

First edition

Indian Banking Ecosystem

A complete guide to the technology behind
Indian banking



Neeraj Prem

Infrastructure Team's Knowledgebase

Indian Banking Ecosystem: A Complete Guide to the Technology Behind Indian Banking

Written by Neeraj Prem. First edition. Facts current as of 29 September 2026.

Published by Infrastructure Team's Knowledgebase.

Text and diagrams © 2026 Neeraj Prem. Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0): <https://creativecommons.org/licenses/by/4.0/>

To credit this work: Indian Banking Ecosystem by Neeraj Prem (<https://ibs.neerajprem.in>), licensed under CC BY 4.0.

Product names, trademarks and the documents cited in this book belong to their owners and are not covered by this licence.

Independence

This is an independent reference. It is a personal project; the views in it are the author's own and do not represent any employer. It is not official documentation of the Reserve Bank of India, the National Payments Corporation of India or any bank or vendor, and it is not legal, compliance or investment advice. Product names appear for reference only; nothing here is a recommendation.

How the facts were checked

Every number, date, limit, named customer and named regulation in this book is drawn from a register of facts, reproduced in Appendix B. Each fact names the source it came from and the date it was true, and each source was opened and read before the fact was recorded. Patterns that describe no particular organisation are labelled illustrative. Figures that change often, such as monthly payment volumes, are dated so that readers can tell how current they are.

The same register drives the companion website, so the book and the site cannot disagree. Where this book and a later edition of the site differ, the site is more recent.

Contents

Part I	Foundations	7
1	How money moves in India	8
2	Core systems	10
3	Payment rails	14
Part II	Architecture	23
4	Core banking system architecture	26
5	Payment system architecture	29
6	API-first and open banking	33
7	Event-driven architecture	37
8	Data architecture	40
9	Legacy modernisation	44
10	Security architecture	47
11	Multi-data-centre and disaster recovery	51
12	Hybrid and multi-cloud deployment	55
Part III	Technologies	59
13	Core banking platforms	62
14	Databases	65
15	Messaging and streaming	68
16	Middleware and integration	71
17	Containers and orchestration	73
18	Cloud platforms	76
19	Security technologies	79
20	Observability	82
21	Machine learning and AI	85
22	Mobile technologies	88
23	Programming languages	91
24	Payment-specific technology	93
Part IV	Scale and decisions	96
25	High-volume systems	97
26	Build versus buy	102

27	Limitations and known problems	106
Part V	Governance	111
28	Regulators and mandates	112
29	RBI ecosystem	116
A	Glossary of short names	133
B	Register of facts	137
C	Bibliography	142
D	Corrections to earlier drafts	145
	Index	146
	About the author	148

Preface

India moves money at a scale few countries match, and it does so on infrastructure that most people who use it never see. A payment that takes seconds on a phone passes through a bank's app, a national switch, another bank's systems and, eventually, the accounts banks hold at the central bank. Behind each of those steps sit decades of decisions about software, networks, rules and institutions.

This book explains that machinery. It was written for engineers joining Indian financial services, for architects and product leads who need to reason about it, for students and analysts who want the whole picture in one place, and for anyone in risk and compliance who needs to know where the rules touch the technology.

It tries to be precise about what is known. Where a public source says how a named organisation works, the book cites it. Where it describes a common industry pattern, it says so. Where a question could not be settled from public sources, the answer is left out rather than guessed. Several claims that circulate widely turned out to be wrong when checked; Appendix D records them.

The chapters were first written as a website, which remains the most current version. This edition gathers them into one sequence, with connecting text, so they can be read from beginning to end.

How to read this book

Reading paths. Part I is the foundation, and everyone should start there. After that the parts stand on their own: Part II explains architecture, Part III surveys technologies, Part IV covers operating at scale and making build-or-buy decisions, and Part V covers regulators and the institutions around the Reserve Bank. Readers new to banking systems will get most from reading Parts I, II and V in order; practitioners can go straight to the chapter they need.

Facts and notes. A small raised number marks a fact taken from a source. The notes at the end of each chapter list those sources in order, with what each one supports and the date it was checked. The full register of facts is in Appendix B, and every source is in Appendix C.

Illustrative material. Diagrams and examples labelled illustrative show common patterns, not the systems of any named organisation. Worked examples use made-up amounts.

Short names. Acronyms are spelled out on first use in each chapter and collected in the glossary in Appendix A.

Questions for a review. Most chapters end with questions to bring to a design or decision review. They are the quickest way to turn a chapter into action.

Part I

Foundations

Three chapters that everything else builds on. The first follows a payment across the institutions that carry it. The second opens the core banking system, the ledger at the centre of every bank. The third walks through the payment rails that connect banks to one another, how they settle and what happens when a payment goes wrong.

Chapter 1

How money moves in India

Every payment in India, whether a tap on a phone, a salary credit or a cheque paid in at a branch, crosses the same basic landscape. There is the bank where the money starts and the bank where it ends. Between them sits a rail: a shared system, with an operator and a rulebook, that carries the instruction from one to the other. Behind every rail sits settlement, the movement of money between the banks themselves in the accounts they hold at the Reserve Bank of India.

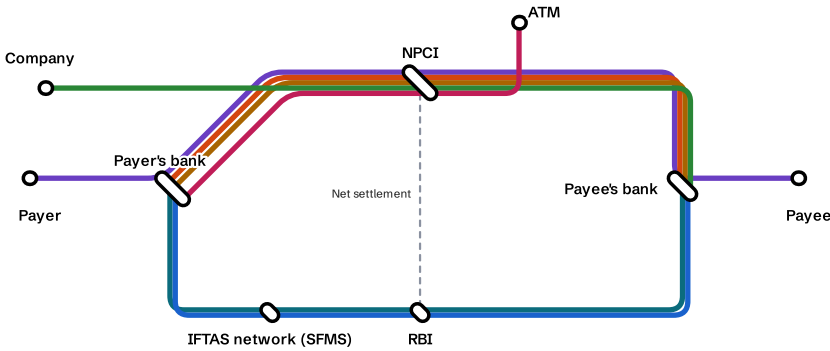
Two operators run most of those rails. The Reserve Bank runs the systems for large and account-to-account transfers. The National Payments Corporation of India runs the systems most customers use every day. Around them is a ring of institutions that built the networks, insure deposits, print notes, run registries and clear securities trades; Part V describes each one.

The map below shows these parts as a transit map: each rail is a line, and each institution or system a payment passes through is a stop. It is simplified on purpose. Its job is to show which parties a payment touches, not the exact path of every message, and the chapters that follow fill in the detail.

In August 2026, UPI handled **24.51 billion transactions**¹, the most in any month so far: about **791 million a day**¹.

Reported from NPCI data, as of 31 August 2026. Latest figures: [RBI payment system indicators](#)².

How a payment travels



Illustrative and simplified. Routes show which institutions a payment touches, not exact message paths. Stop descriptions are awaiting verification.

Notes

1. [UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn](https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html) https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: UPI processed 24.51 billion transactions worth ₹29.82 trillion in August 2026, its highest monthly volume to date (as of 31 August 2026); UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).

2. [Payment System Indicators \(monthly\)](https://rbi.org.in/scripts/TrendsPSIUserView.aspx?Id=56) <https://rbi.org.in/scripts/TrendsPSIUserView.aspx?Id=56>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

1 How money moves in India

Supports: RBI publishes monthly Payment System Indicators with volumes and values for every payment system; the latest edition found covers July 2026 (as of 29 September 2026).

Chapter 2

Core systems

The core banking system is a bank's system of record; apps and payment rails read from it or post to it. This page covers the platforms, the daily cycle and the systems around the core.

The previous chapter followed a payment between banks. This one looks inside a bank, at the system that holds every account and balance.

What a core banking system is

A core banking system (CBS) holds a bank's customers, accounts and balances, and posts every debit and credit to the general ledger. It is the system of record: when two systems disagree about a balance, the core is right by definition.

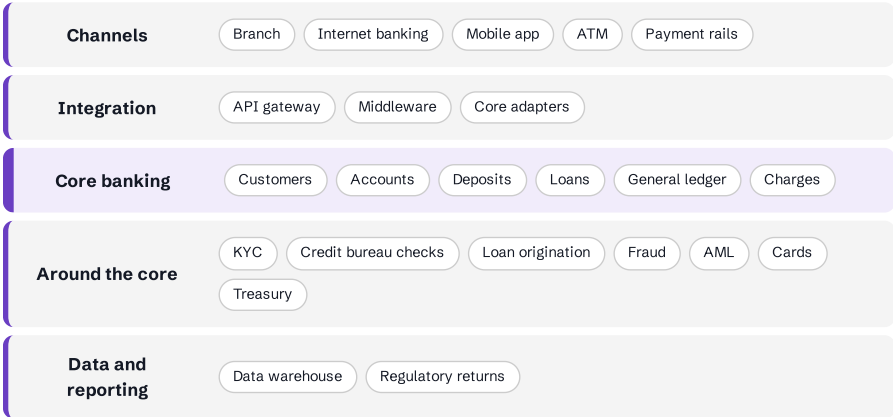
“Core” also means centralised. Before core banking, each branch kept its own books, and a customer could only be served at the branch that held the account. A central core lets every branch, ATM and app see the same account at the same moment. That shift is what made anywhere banking and, later, instant payments possible.

Instant rails such as UPI assume that any bank can debit or credit any account in seconds, at any hour. That is only possible because each bank's accounts sit in one central system.

The layers around the core

A core rarely talks to customers directly. Channels reach it through an integration layer, and a ring of specialist systems sits around it.

The layers of a bank's systems



Illustrative. Real estates contain many more systems, but this layering is typical.

Systems around the core

The main systems that surround a core

System	What it does	How it relates to the core
Channels	Branch, internet banking, mobile apps, ATMs	Send requests through the integration layer; rarely call the core directly
Integration layer	API gateway and middleware that translate and route requests	Protects the core from load and hides its interfaces
KYC and identity	Verifies customers, including Aadhaar-based and video KYC	Creates or updates the customer record in the core
Credit bureau checks	Pulls credit histories from credit information companies	Feeds lending decisions before an account is opened
Loan origination	Takes a loan from application to approval	Books the approved loan into the core
Fraud monitoring	Scores payments and logins for fraud, often in real time	Can hold or block a transaction before the core posts it
AML	Monitors for money laundering and files reports to FIU-IND	Reads transactions from the core, usually after posting
Cards and treasury	Card management; the bank's own money-market and investment desk	Separate systems that post summaries to the general ledger
Data warehouse and regulatory reporting	Stores history and produces returns for RBI	Loaded from the core, often overnight

KYC records increasingly come from a shared source rather than each bank's own files. The Government of India authorised CERSAI to act as the Central KYC Records Registry by notification S.O. 3183(E) of 26 November 2015; the registry went live on 15 July 2016.⁶

The platform landscape

Several commercial platforms are used by Indian banks. Customer names appear on this site only where a public source confirms them.

Core banking platforms

Platform	Maker	Indian users named in public sources
TCS BaNCS	Tata Consultancy Services	State Bank of India (see sources)
Finacle	EdgeVerve Systems, a wholly owned Infosys subsidiary	None confirmed yet on this site
Oracle FLEXCUBE	Oracle	None confirmed yet on this site
Temenos Transact	Temenos	None confirmed yet on this site
Cloud-native cores, such as Mambu and Thought Machine	Various	None confirmed yet on this site
Cooperative-sector and legacy systems	Various, including shared community platforms	See the note on shared platforms below

Product names are for reference only. The site does not recommend vendors. Sources^{1 2}

SBI's core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years.¹ Finacle is developed by EdgeVerve Systems, a wholly owned subsidiary of Infosys, and marketed as Infosys Finacle.² The vendor states that banks in over 100 countries use Finacle to serve more than a billion consumers and 1.3 billion accounts.²

How to read vendor claims

Customer counts, market shares and “largest” claims usually come from the vendor. This site labels them as the vendor’s claim and does not repeat them as fact. Which bank runs which platform changes over time, so every named customer carries the date of its source.

The daily cycle: end of day and beginning of day

A core does two kinds of work. Online processing handles each transaction as it happens: a withdrawal, a transfer, a balance enquiry. Batch processing handles work that is easier to do for every account at once, such as accruing interest, applying charges and producing statements.

The batch run that closes a business day is called end of day (EOD). The run that opens the next day is beginning of day (BOD).

A typical end-of-day cycle



Illustrative. The exact stages and their order vary by platform and by bank.

Why round-the-clock payments strain the core

Many cores were designed around a quiet night. Instant rails never have one: UPI alone now averages 791 million a day³. So a bank cannot simply stop posting while its end-of-day batch runs.

Banks bridge the gap in a few ways. A stand-in layer keeps a shadow balance and approves or declines payments while the core is busy, then replays them afterwards. Batch jobs are split into smaller pieces that run while the core stays online. Some banks move payment processing into separate systems that post to the core in bulk. Each approach adds reconciliation work: two systems now hold a version of the balance, and they must agree.

How cores are deployed

A common pattern is for a large bank to run its core in its own data centres, with a second site for disaster recovery (see multi-data-centre and disaster recovery (chapter 11)). Smaller banks, especially in the cooperative sector, often use a shared platform instead of running their own. IFTAS’s Indian Banking

Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.⁴

Running a core on a vendor's or a public cloud is possible, but it counts as outsourcing and brings RBI's rules for outsourced IT with it (see hybrid and multi-cloud deployment (chapter 12)). RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023.⁵

Why cores are hard to change

A core accumulates decades of products, interest rules and integrations. Replacing it means moving every account, every balance and every open loan without losing a rupee, while the bank keeps trading. That is why core replacements are rare, run for years, and are usually done in stages rather than all at once. The architecture section covers the patterns banks use: core banking system architecture (chapter 4) explains the model, and legacy modernisation (chapter 9) explains how banks change it in stages.

Notes

1. **SBI deepens partnership with TCS to drive innovation and enhance customer experience** <https://tcs.com/who-we-are/newsroom/press-release/sbi-deepens-partnership-with-tcs-drive-innovation-enhance-customer-experience>. Tata Consultancy Services. **Vendor**, accessed 29 September 2026.
Supports: SBI's core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years (as of 6 October 2021).
2. **EdgeVerve Systems Positioned a Leader by Gartner for the Finacle Core Banking Solution** <https://www.edgeverve.com/finacle/news/edgeverve-positioned-gartner-for-finacle-solution/>. EdgeVerve Systems. **Vendor**, accessed 29 September 2026.
Supports: Finacle is developed by EdgeVerve Systems, a wholly owned subsidiary of Infosys, and marketed as Infosys Finacle (as of 31 August 2020); The vendor states that banks in over 100 countries use Finacle to serve more than a billion consumers and 1.3 billion accounts (as of 31 August 2020).
3. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-ncpi-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.
Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).
4. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services (as of 20 September 2022).
5. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023 (as of 10 April 2023).
6. **Amendment to Master Direction on KYC: Operationalisation of Central KYC Registry (RBI/2016-17/11)** <https://www.rbi.org.in/Scripts/NotificationUser.aspx?id=10498>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: The Government of India authorised CERSAI to act as the Central KYC Records Registry by notification S.O. 3183(E) of 26 November 2015; the registry went live on 15 July 2016 (as of 8 July 2016).

Chapter 3

Payment rails

A payment rail is the system that carries money between banks. India runs several, each built for a different job. This page explains how they differ and how they settle.

With the core in view, this chapter turns to the rails that connect banks to one another: what each one is for, how it settles and how failures are put right.

What a payment rail is

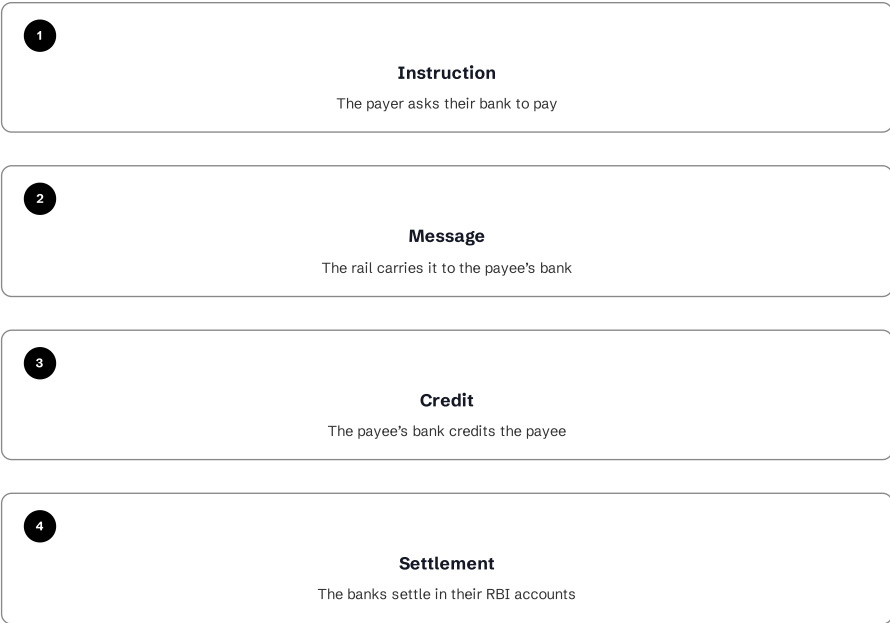
A payment rail is a shared system that banks use to move money for their customers. Each rail has an operator, a rulebook, a message format and a way of settling between banks. In India the main operators are the Reserve Bank of India (RBI), which runs RTGS and NEFT, and the National Payments Corporation of India (NPCI), which runs UPI, IMPS, NACH, the card and ATM network, and cheque clearing.

Every payment has two parts. The message tells the banks what to do. Settlement then moves the money between the banks themselves, in the accounts they hold at RBI.

Banks hold current accounts with RBI. Moving money between those accounts is what settlement means on this page.

This is why a customer can see a credit within seconds while the banks settle later.

The two halves of a payment



Illustrative and simplified. The order is the same on every rail; the timing of the last step differs.

The rails at a glance

The main rails at a glance

Rail	Run by	How it settles	Typical use
 RTGS Real Time Gross Settlement	RBI	Gross, one payment at a time, in real time, 24x7	Large-value transfers, from ₹2 lakh with no upper limit ^{1 2 3}
 NEFT National Electronic Funds Transfer	RBI	Net, in half-hourly batches, 24x7	Everyday account-to-account transfers ^{2 4 3} Awaiting verification
 IMPS Immediate Payment Service	NPCI	Customer credited instantly; banks settle net later	Instant transfers by account number ⁶ Awaiting verification
 UPI Unified Payments Interface	NPCI	Customer credited instantly; banks settle net later	Person-to-person and shop payments by UPI ID or QR code ⁶ Awaiting verification
 NACH National Automated Clearing House	NPCI	Batch, net	Salaries, loan instalments and other recurring bulk payments Awaiting verification
 CTS Cheque Truncation System	NPCI	Continuous clearing; settles hourly (since October 2025)	Cheques, cleared by image instead of paper ^{7 8 9} Awaiting verification
 Cards and NFS RuPay card network and National Financial Switch	NPCI	Card network clearing; banks settle net later	Card payments in shops and online; ATM withdrawals at other banks ¹⁰ Awaiting verification
 BBPS Bharat Bill Payment System	NPCI group	Net, through participating banks	Utility and other recurring bill payments Awaiting verification
 AA Account Aggregator framework	RBI-registered NBFCs	Not a payment rail: moves data, not money	Consent-based sharing of financial data, such as for a loan application ^{11 12} Awaiting verification

Rows marked “awaiting verification” are still being checked against the operator’s own documentation.

The table below sets the rails side by side.

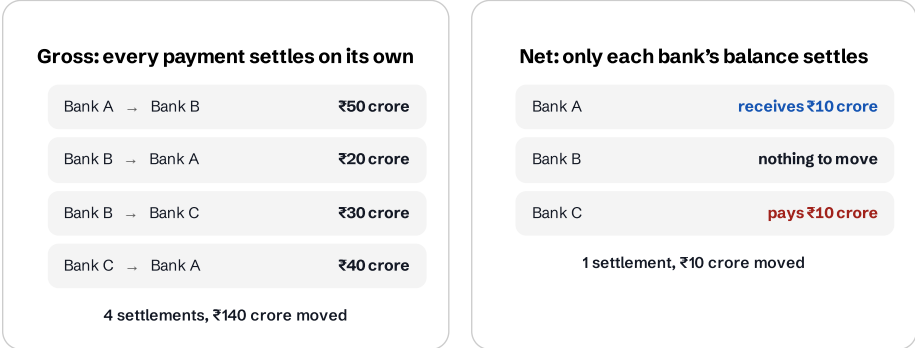
Compare payment rails

Attribute	 RTGS	 NEFT	 IMPS	 UPI	 NACH	 CTS	 Cards and NFS	 BBPS	 AA
Full name	Real Time Gross Settlement	National Electronic Funds Transfer	Immediate Payment Service	Unified Payments Interface	National Automated Clearing House	Cheque Truncation System	RuPay card network and National Financial Switch	Bharat Bill Payment System	Account Aggregator framework
Run by	RBI	RBI	NPCI	NPCI	NPCI	NPCI	NPCI	NPCI group	RBI-registered NBFCs
How it settles	Gross, one payment at a time, in real time, 24x7	Net, in half-hourly batches, 24x7	Customer credited instantly; banks settle net later	Customer credited instantly; banks settle net later	Batch, net	Continuous clearing; settles hourly (since October 2025)	Card network clearing; banks settle net later	Net, through participating banks	Not a payment rail: moves data, not money
Typical use	Large-value transfers, from ₹2 lakh with no upper limit	Everyday account-to-account transfers	Instant transfers by account number	Person-to-person and shop payments by UPI ID or QR code	Salaries, loan instalments and other recurring bulk payments	Cheques, cleared by image instead of paper	Card payments in shops and online; ATM withdrawals at other banks	Utility and other recurring bill payments	Consent-based sharing of financial data, such as for a loan application

Gross and net settlement

Gross settlement moves each payment on its own, at once. It removes the risk that one bank's failure strands everyone else's money, but each bank needs enough money in its RBI account to cover every payment as it goes. Net settlement adds up what each bank owes and is owed over a period, then moves only the difference. That needs far less cash, but money stays in flight until the cycle closes, and a bank that cannot pay its net amount affects everyone in that cycle.

The same four payments, settled two ways



Illustrative amounts. The payments are identical; only the settlement method changes.

RTGS and NEFT

RBI runs both of the main account-to-account rails. The difference between them is the difference between gross and net settlement, described in payment system architecture (chapter 5). RTGS settles each transaction in real time on a one-to-one gross basis.¹ RTGS is meant mainly for large-value transfers: the minimum is ₹2 lakh, with no upper ceiling.² RTGS has been available 24x7x365 since 14 December 2020.² Because each payment settles individually in RBI's books, an RTGS payment is final once it is processed.

NEFT processes transactions received up to a set time in batches, while RTGS processes them continuously, one at a time.² NEFT has been available 24x7, on all days of the year including holidays, since 16 December 2019.⁴ When NEFT moved to 24x7 in December 2019, RBI set 48 half-hourly settlement batches a day.⁴ A beneficiary bank must credit or return an NEFT transaction within 2 hours of the batch settling.⁴

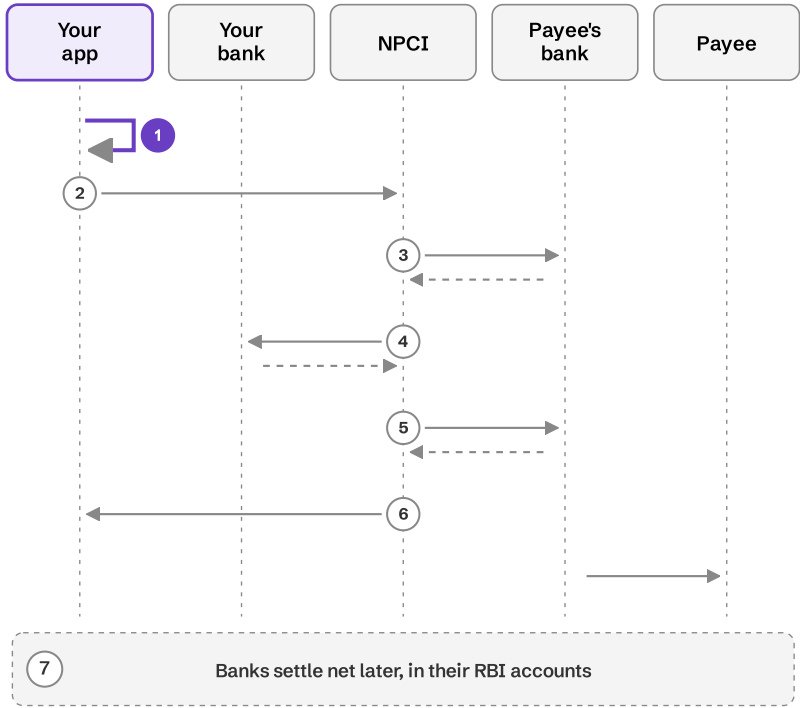
IMPS and UPI

IMPS and UPI both credit the customer within seconds, at any hour, and both settle between banks later, on a net basis. IMPS came first and is used from bank apps and branches with an account number and IFSC. UPI added a simpler address, the UPI ID, and opened payments to apps that are not banks. In August 2026, IMPS handled 360 million transactions⁶ and UPI 24.51 billion transactions⁶, about 791 million a day⁶.

Who takes part in a UPI payment

- **The payer's bank** holds the account that is debited. It checks the UPI PIN and the balance.
- **The app** is where the customer starts the payment. It is either the bank's own app or a third-party app provider (TPAP) that works through one or more partner banks, called payment service providers (PSPs).
- **NPCI** runs the switch that routes the request between banks and works out what each bank owes the others.
- **The payee's bank** credits the person or merchant being paid.

When a customer first sets up an app, UPI ties the app to that phone and its SIM, a step called device binding. Each payment is then approved with the UPI PIN. The PIN proves the customer; the binding proves the phone.



Simplified and illustrative. Real flows also involve the app's partner bank, and the order of the debit and credit messages can vary.

- 1 You start the payment**
You enter the payee's UPI ID or scan their QR code, type the amount and confirm with your UPI PIN.
- 2 Your app sends the request**
The app passes the request, through the bank it works with, to NPCI.
- 3 NPCI finds the payee's bank**
NPCI works out which bank holds the account behind the payee's UPI ID.
- 4 Your bank debits you**
Your bank checks your UPI PIN and balance, debits your account and replies.
- 5 The payee's bank credits them**
NPCI asks the payee's bank to credit the payee, and the bank confirms.
- 6 Everyone is told**

3 Payment rails

NPCI confirms to your app, and the payee's bank notifies the payee.

7

The banks settle later

The banks settle what they owe each other, net, in their accounts at RBI.

UPI limits

NPCI sets ceilings on how much can move through UPI. Your bank and your app may set lower limits of their own.

UPI ceilings from 15 September 2025

Payment type	Per transaction	Per day
Person to person	₹1 lakh	₹1 lakh
Capital markets and insurance (verified merchants)	₹5 lakh	₹10 lakh
Government e-Marketplace, including taxes and deposits	₹5 lakh	Not stated in sources checked
Credit card bill payments	₹5 lakh	₹6 lakh

Other merchant categories have their own ceilings; check NPCI for the full list. Sources ¹⁵ ¹⁴

Ways to pay with UPI

UPI has grown several variants on the same rails. AutoPay lets a customer approve a recurring payment, such as a subscription, once. UPI Lite keeps a small balance on the phone for quick, low-value payments without entering the PIN each time. UPI I23PAY brings UPI to feature phones through voice calls, missed calls and simple apps. NPCI publishes the current limits for each.

UPI is no longer only about bank balances. RBI announced on 8 June 2022 that credit cards, starting with RuPay, could be linked to UPI. ¹⁷ Since RBI's circular of 4 September 2023, pre-sanctioned credit lines at scheduled commercial banks can fund UPI payments, with the customer's prior consent. ¹⁶

When a payment fails

A payment can end in three ways. It succeeds; it fails before any money moves; or it gets stuck, with the payer debited but the payee not credited. The third case is the one customers notice, and RBI sets rules for fixing it. A failed transaction is one not fully completed for a reason not attributable to the customer, such as a link failure, an ATM without cash or a session time-out. ⁵ RBI's framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint. ⁵

Outer time limits for fixing a stuck payment

What went wrong	Must be reversed by	After that
UPI transfer: payer debited, beneficiary not credited	T+1 day	₹100 a day to the customer
UPI payment to a merchant: payer debited, merchant not confirmed	T+5 days	₹100 a day to the customer
IMPS transfer: payer debited, beneficiary not credited	T+1 day	₹100 a day to the customer
ATM: account debited, cash not dispensed	T+5 days	₹100 a day to the customer

T is the day of the transaction. These are outer limits; banks are expected to fix failures sooner. Sources ⁵

Why pending states are hard

A payment that times out is not necessarily a failure: the money may have moved, and only the confirmation was lost. Systems must be able to ask “what happened to this payment?” and get one consistent answer, which is why every payment carries a unique reference and every retry reuses it. Payment system architecture (chapter 5) explains the state machine behind this.

Bulk and recurring payments: NACH

NACH moves many payments in one go, such as a company's salaries, dividends, or the monthly instalments a lender collects. Collections run under a mandate: the customer authorises a lender or biller once, and the bank then debits the account on each due date. Files are processed in batches, so NACH suits planned, scheduled money rather than urgent payments.

Cards, tokens and ATMs

Card payments run over card networks, including NPCI's domestic network, RuPay. Online card payments changed in 2022. Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead.¹⁸ A token stands in for the card number and works only for the merchant it was issued for, so a breached merchant database no longer exposes usable card numbers.

ATM withdrawals at another bank's machine travel over the National Financial Switch. NPCI took over operation of the National Financial Switch from IDRBT with effect from 14 December 2009, under an RBI authorisation.¹⁰ The National Financial Switch connected 2.61 lakh ATMs of 1,317 member banks as of 31 July 2024.¹

Card networks must also keep payment data in India. RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad.¹⁹ RBI had earlier restricted American Express and Diners Club from onboarding new domestic customers from 1 May 2021 on the same grounds.²⁰ RBI barred Mastercard from onboarding new domestic card customers from 22 July 2021 for not complying with the payment data storage directions.²¹ RBI lifted the restriction on Mastercard in June 2022 after satisfactory compliance with the data storage directions.²²

Cheques now clear within the day

The Cheque Truncation System (CTS) clears cheques by image, so the paper never travels between banks. RBI asked NPCI to build the Positive Pay facility into CTS and make it available to participant banks, and refers to the CTS grids that NPCI runs.⁹

Changed recently

RBI moved the Cheque Truncation System from batch processing to continuous clearing with settlement on realisation; Phase 1 took effect on 4 October 2025.⁷

Under continuous clearing, CTS settles every hour from 11:00, based on positive confirmations and deemed approvals from drawee banks.⁸

RBI postponed Phase 2 of continuous cheque clearing, which had been planned for 3 January 2026, until further notice.⁷ RBI set the CTS presentation session at 09:00 to 15:00 and the confirmation session at 09:00 to 19:00.⁷

Large cheques get an extra check. Since 1 January 2021, banks must offer Positive Pay for cheques of ₹50,000 and above; using it is the account holder's choice, and banks may make it mandatory from ₹5 lakh.⁹ The issuer tells their bank the date, payee and amount in advance, and CTS flags any cheque that does not match.

Bill payments: BBPS

The Bharat Bill Payment System (BBPS) lets customers pay electricity, water, telecom and many other bills through any participating bank, app or agent, with a common confirmation. Its value is interoperability: a biller connects once and can be paid through every channel on the system.

Messaging networks: SFMS, INFINET and SWIFT

Behind RTGS and NEFT sit a private network and a messaging layer. IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS.¹ SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities.¹ IDRBT transferred INFINET, SFMS, the RTGS and NEFT systems and its banking community cloud to its subsidiary IFTAS in February 2015; IFTAS was transferred to RBI in 2019.¹ For cross-border payments, banks use SWIFT, the global cooperative network for financial messages.

Account Aggregators: moving data, not money

An Account Aggregator (AA) is not a payment rail, but lenders now use it alongside the rails, for example to check a borrower's bank statements with consent. RBI issued its Master Direction for Account Aggregators on 2 September 2016; an Account Aggregator must be a non-bank financial company registered with RBI.¹¹ No financial information is retrieved, shared or transferred through an Account Aggregator without the customer's explicit consent, and joining is voluntary.¹²

Three roles make it work. A financial information provider (FIP), such as a bank, holds the data. A financial information user (FIU), such as a lender, asks for it. The aggregator carries the request and the encrypted data between them. Customer data passing through an Account Aggregator is not visible to, and does not reside with, the aggregator.¹³ Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT.¹³

Which rail for which job

Choosing a rail

Job	Usual rail	Why
Paying a friend or a shop	UPI	Instant, works from a phone number, UPI ID or QR code
A large transfer that must be final at once	RTGS	Settles gross and immediately; minimum ₹2 lakh
An ordinary transfer between accounts	NEFT or IMPS	NEFT settles in batches through the day; IMPS credits instantly
Salaries, dividends or loan instalments	NACH	Built for bulk files and mandates
A cheque	CTS	Cleared by image, continuously through the day
A card payment in a shop or online	Card networks	Accepted widely; online payments use tokens
Paying a utility bill	BBPS	One connection for the biller, many channels for the customer
Sharing bank statements with a lender	Account Aggregator	Consent-based data sharing, not a payment

Guidance, not rules: banks and apps may route a payment differently. Sources²

Live volumes for every system are published each month: [see RBI's payment system indicators](#)³.

Notes

1. [About IDRBT](https://www.idrbt.ac.in/about-idrbt) <https://www.idrbt.ac.in/about-idrbt>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.

3 Payment rails

Supports: RTGS settles each transaction in real time on a one-to-one gross basis (as of 1 January 2025); The National Financial Switch connected 2.61 lakh ATMs of 1,317 member banks as of 31 July 2024 (as of 31 July 2024); SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities (as of 1 January 2025); IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS (as of 1 January 2025); IDRBT transferred INFINET, SFMS, the RTGS and NEFT systems and its banking community cloud to its subsidiary IFTAS in February 2015; IFTAS was transferred to RBI in 2019 (as of 1 January 2025).

2. **Real Time Gross Settlement (RTGS) System: FAQs** <https://rbi.org.in/Scripts/FAQView.aspx?Id=65>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RTGS is meant mainly for large-value transfers: the minimum is ₹2 lakh, with no upper ceiling (as of 29 September 2026); RTGS has been available 24x7x365 since 14 December 2020 (as of 29 September 2026); NEFT processes transactions received up to a set time in batches, while RTGS processes them continuously, one at a time (as of 29 September 2026).

3. **Payment System Indicators (monthly)** <https://rbi.org.in/scripts/TrendsPSIUserView.aspx?Id=56>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI's Payment System Indicators list RTGS and NEFT under RBI-operated payment systems (as of 29 September 2026); RBI publishes monthly Payment System Indicators with volumes and values for every payment system; the latest edition found covers July 2026 (as of 29 September 2026).

4. **Availability of National Electronic Funds Transfer (NEFT) System on 24x7 basis (RBI/2019-20/111)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11750>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: NEFT has been available 24x7, on all days of the year including holidays, since 16 December 2019 (as of 6 December 2019); When NEFT moved to 24x7 in December 2019, RBI set 48 half-hourly settlement batches a day (as of 6 December 2019); A beneficiary bank must credit or return an NEFT transaction within 2 hours of the batch settling (as of 6 December 2019).

5. **Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems (RBI/2019-20/67)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11693>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: If an IMPS transfer debits the payer but does not credit the beneficiary, it must be reversed by T+1 day; after that, ₹100 a day is payable (as of 20 September 2019); RBI's framework for failed transactions, in force since 15 October 2019, sets out time limits for reversal and requires compensation to be paid automatically, without a complaint (as of 20 September 2019); A failed transaction is one not fully completed for a reason not attributable to the customer, such as a link failure, an ATM without cash or a session time-out (as of 20 September 2019); If a UPI transfer debits the payer but does not credit the beneficiary, the beneficiary bank must reverse it by T+1 day; after that, ₹100 a day is payable (as of 20 September 2019); If a UPI payment to a merchant debits the payer but the merchant gets no confirmation, it must be reversed within T+5 days; after that, ₹100 a day is payable (as of 20 September 2019); If an ATM debits the account but does not dispense cash, the bank must reverse it within T+5 days; after that, ₹100 a day is payable (as of 20 September 2019).

6. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: UPI processed 24.51 billion transactions worth ₹29.82 trillion in August 2026, its highest monthly volume to date (as of 31 August 2026); UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026); IMPS processed 360 million transactions worth ₹7.04 trillion in August 2026 (as of 31 August 2026).

7. **Continuous Clearing and Settlement on Realisation in Cheque Truncation System: Phase 2 (RBI/2025-26/156)** <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12323&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI moved the Cheque Truncation System from batch processing to continuous clearing with settlement on realisation; Phase 1 took effect on 4 October 2025 (as of 24 December 2025); RBI postponed Phase 2 of continuous cheque clearing, which had been planned for 3 January 2026, until further notice (as of 24 December 2025); RBI set the CTS presentation session at 09:00 to 15:00 and the confirmation session at 09:00 to 19:00 (as of 24 December 2025).

8. **Introduction of Continuous Clearing and Settlement on Realisation in Cheque Truncation System (RBI/2025-26/73)** <https://website.rbi.org.in/documents/d/rbi/circulardatedaugust132025cts>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Under continuous clearing, CTS settles every hour from 11:00, based on positive confirmations and deemed approvals from drawee banks (as of 13 August 2025).

9. **Positive Pay System for Cheque Truncation System (RBI/2020-21/41)** <https://website.rbi.org.in/web/rbi/-/notifications/positive-pay-system-for-cheque-truncation-system-11969>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI asked NPCI to build the Positive Pay facility into CTS and make it available to participant banks, and refers to the CTS grids that NPCI runs (as of 25 September 2020); Since 1 January 2021, banks must offer Positive Pay for cheques of ₹50,000 and above; using it is the account holder's choice, and banks may make it mandatory from ₹5 lakh (as of 25 September 2020).

10. **Takeover of NFS by NPCI from IDRBT (NPCI/NFS/OC No.1)** <https://www.npci.org.in/PDF/nfs/circular/2009-10/NFS-OC-1-Takeover-of-NFS-by-NPCI-from-IDRBT.pdf>. National Payments Corporation of India. **Primary source**, accessed 29 September 2026.

Supports: NPCI took over operation of the National Financial Switch from IDRBT with effect from 14 December 2009, under an RBI authorisation (as of 18 December 2009).

11. **Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 (updated 6 September 2024)** http://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?Id=10598. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI issued its Master Direction for Account Aggregators on 2 September 2016; an Account Aggregator must be a non-bank financial company registered with RBI (as of 6 September 2024).

3 Payment rails

12. **Account Aggregator Framework** <https://financialservices.gov.in/account-aggregator-framework>. Department of Financial Services, Ministry of Finance. **Primary source**, accessed 29 September 2026.
Supports: No financial information is retrieved, shared or transferred through an Account Aggregator without the customer's explicit consent, and joining is voluntary (as of 29 September 2026).
13. **Consultation paper on Financial Information Users in the securities markets under the Account Aggregator framework** https://www.sebi.gov.in/sebi_data/attachdocs/aug-2023/1690887848711.pdf. Securities and Exchange Board of India. **Primary source**, accessed 29 September 2026.
Supports: Customer data passing through an Account Aggregator is not visible to, and does not reside with, the aggregator (as of 1 August 2023); Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT (as of 1 August 2023).
14. **NPCI raises daily UPI payment limit on P2M transactions to ₹10 lakh** <https://ddnews.gov.in/en/npci-raises-daily-upi-payment-limit-on-p2m-transactions-to-%E2%82%B910-lakh/>. DD News (Prasar Bharati). **Reported**, accessed 29 September 2026.
Supports: From 15 September 2025, NPCI raised UPI limits for verified merchants in capital markets and insurance to ₹5 lakh per transaction and ₹10 lakh a day (as of 15 September 2025); From 15 September 2025, UPI payments on the Government e-Marketplace, including taxes and earnest money deposits, can be up to ₹5 lakh per transaction (as of 15 September 2025).
15. **UPI raises daily P2M payment limit to Rs 10 lakh** <https://www.newsonair.gov.in/npci-raises-upi-person-to-merchant-transaction-limit-to-%E2%82%B95-lakh>. All India Radio News (Prasar Bharati). **Reported**, accessed 29 September 2026.
Supports: From 15 September 2025, credit card bills can be paid by UPI up to ₹5 lakh per transaction and ₹6 lakh a day (as of 15 September 2025); The UPI limit for person-to-person transfers stayed at ₹1 lakh a day (as of 15 September 2025).
16. **Credit lines on UPI: the next step towards digital financial inclusion** https://khaitanco.com/thought-leaderships/Credit_lines_on_UPI_the_next_step_towards_Digital_Financial_Inclusion. Khaitan & Co. **Analyst**, accessed 29 September 2026.
Supports: Since RBI's circular of 4 September 2023, pre-sanctioned credit lines at scheduled commercial banks can fund UPI payments, with the customer's prior consent (as of 4 September 2023).
17. **Credit cards, starting with RuPay, can now be linked to UPI: RBI** <https://businesstoday.in/amp/latest/economy/story/credit-cards-starting-with-ruPAY-can-now-be-linked-to-upi-rbi-336757-2022-06-08>. Business Today. **Reported**, accessed 29 September 2026.
Supports: RBI announced on 8 June 2022 that credit cards, starting with RuPay, could be linked to UPI (as of 8 June 2022).
18. **Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)] (RBI/2022-2023/95)** <https://website.rbi.org.in/web/rbi/-/notifications/restriction-on-storage-of-actual-card-data-i.e.-card-on-file-cof-12363>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead (as of 28 July 2022).
19. **Storage of Payment System Data (RBI/2017-18/153)** <https://rbi.org.in/scripts/NotificationUser.aspx?Id=11244>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad (as of 6 April 2018).
20. **RBI bars Mastercard from adding new clients in India** <https://www.tribuneindia.com/news/business/rbi-bars-mastercard-from-adding-new-clients-in-india-283510>. The Tribune. **Reported**, accessed 29 September 2026.
Supports: RBI had earlier restricted American Express and Diners Club from onboarding new domestic customers from 1 May 2021 on the same grounds (as of 14 July 2021).
21. **RBI restricts Mastercard from onboarding new domestic customers** https://www.business-standard.com/article/finance/rbi-restricts-mastercard-from-onboarding-new-domestic-customers-121071400974_1.html. Business Standard. **Reported**, accessed 29 September 2026.
Supports: RBI barred Mastercard from onboarding new domestic card customers from 22 July 2021 for not complying with the payment data storage directions (as of 14 July 2021).
22. **Restrictions on Mastercard lifted (press release)** https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53877. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI lifted the restriction on Mastercard in June 2022 after satisfactory compliance with the data storage directions (as of 16 June 2022).

Part II

Architecture

Nine models that shape how banks build and run their systems. Each chapter explains the model, how it plays out in Indian banking, its trade-offs and the ways it fails, and ends with questions for a design review.

Start here introductory

Core banking system architectureThe system of record for accounts, deposits and loans, and why its end-of-day cycle shapes everything around it.4 min read (chapter 4)

Payment system architectureSwitches, participants and settlement accounts, and the state machine that stops a payment being lost or made twice.5 min read (chapter 5)

API-first and open bankingLayered APIs from channel to core, what a gateway does, and how consented data sharing works through Account Aggregators.5 min read (chapter 6)

Next intermediate

Event-driven architectureEvents versus requests, logs and consumers, and the outbox pattern that stops events and data drifting apart.5 min read (chapter 7)

Data architectureTransaction and analytical stores, warehouses and lakes, streaming, and the lineage that regulatory reporting depends on.4 min read (chapter 8)

Legacy modernisationThe strangler fig, anti-corruption layers, data migration, parallel runs and why cutover is where projects fail.4 min read (chapter 9)

Security architectureDefence in depth: network zones, hardware security modules, just-in-time privileged access, detection and reporting duties.5 min read (chapter 10)

Deeper advanced

Multi-data-centre and disaster recoveryActive-passive and active-active, RPO and RTO, replication trade-offs, split-brain and what RBI expects from DR drills.4 min read (chapter 11)

Hybrid and multi-cloud deploymentWhere each workload runs, data localisation, outsourcing and exit planning, connectivity, identity and cost control.4 min read (chapter 12)

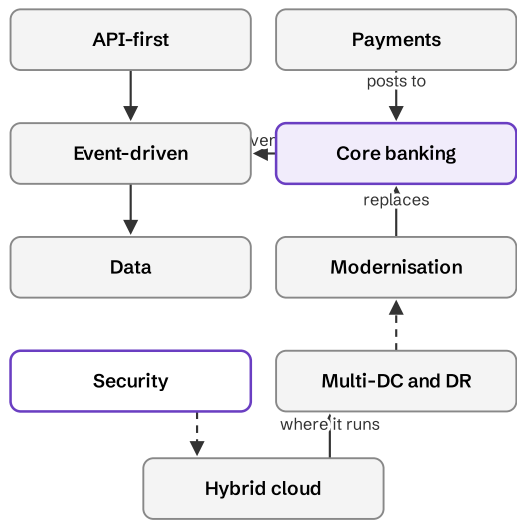
How to read this section

Topics are grouped by how much background they assume. If you are new to banking systems, start with core banking system architecture, then payment system architecture. The advanced topics assume you know both.

Patterns described here are common across the industry. Where a page describes how a named organisation works, it cites a public source; everything else is labelled illustrative.

How the topics connect

How the architecture topics relate



Each box is a topic in this section. Arrows show which topic builds on which.

Chapter 4

Core banking system architecture

A core banking system keeps a bank's accounts and general ledger. It mixes online posting with a nightly batch cycle. Its modules and that cycle explain most constraints elsewhere in a bank.

Part I described what a core banking system does. This chapter explains how one is built, and why its daily cycle shapes the rest of a bank.

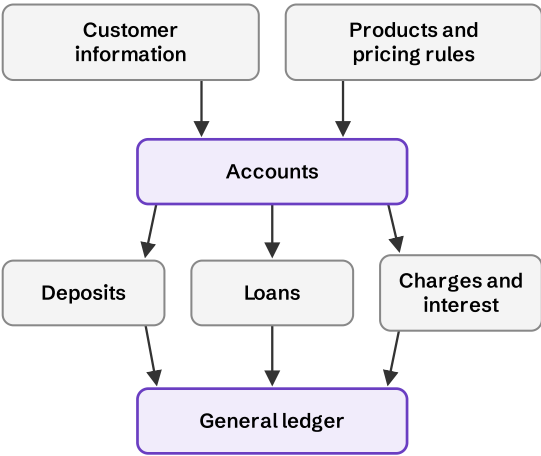
Why it matters

Every other system in a bank either reads from the core or posts to it. When a payment rail credits a customer, a mobile app shows a balance or a regulator asks for a return, the answer ultimately comes from the core. Its design decides how fast a bank can launch products, how it copes with round-the-clock payments and how risky it is to change anything.

The model explained

A core is a set of modules around one ledger. The customer module holds who the bank's customers are. The product module holds the rules: interest rates, fees, limits and statement cycles, set up as parameters rather than code, so a new savings product is usually configuration, not a software release. Accounts are instances of those products. Deposits and loans hold the balances and schedules. Every change of money ends as balanced debits and credits in the general ledger.

The modules of a core banking system



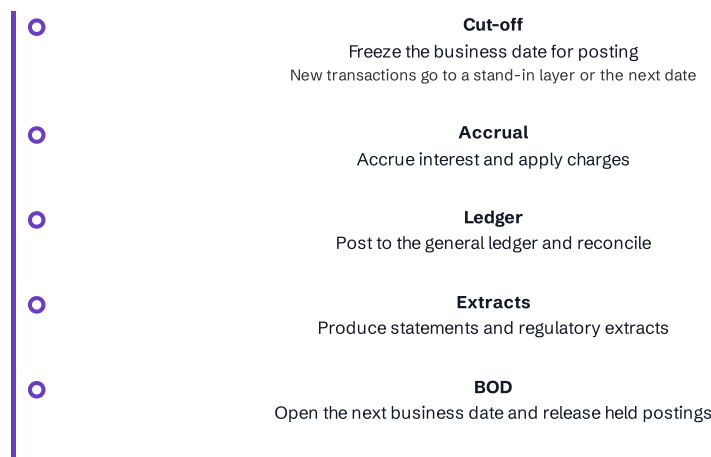
Illustrative. Platforms name and split these modules differently.

Online and batch

Online processing posts each transaction as it happens and must be fast and correct. Batch processing handles work done for every account at once: accruing interest, applying charges, ageing loans, producing statements and regulatory extracts. The run that closes the business day is end of day (EOD); the run that

opens the next is beginning of day (BOD).

End-of-day and beginning-of-day stages



Illustrative. Stage names and order vary by platform and bank.

Why a core is hard to scale out

Money needs strong consistency: two withdrawals must never both succeed against a balance that covers only one. Most cores achieve this with a large relational database and transactions, which works well on one very big machine and less well across many. Some accounts are also hot spots. A merchant’s settlement account or a bank’s own clearing account may receive thousands of postings a minute, and each posting must lock the same balance. Adding servers does not help if every request queues behind one row.

Stand-in processing and shadow balances

When the core is busy with batch work, or briefly unavailable, a stand-in layer can keep approving transactions against a shadow copy of each balance, within safe limits. Once the core is back, the stand-in replays what it approved. This keeps payments flowing but means two systems hold a version of the truth for a while, and they must be reconciled afterwards.

How it plays out in Indian banking

Large Indian banks run large commercial platforms. SBI’s core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years.¹ Smaller banks often share one. IFTAS’s Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.³

The pressure today comes from instant payments. UPI alone averages 791 million a day², and none of that stops for end of day. Banks answer with stand-in layers, shorter batch windows and payment hubs that shield the core. RBI’s resilience rules also reach the batch cycle. A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day.⁴

Trade-offs

Core design choices

Choice	You gain	You give up
One central core	One version of every balance; simpler audit	A single, very important system to protect and scale
Parameterised products	New products without code changes	Complex configuration that itself needs testing and control
Nightly batch	Efficient bulk processing	A window when the core is not fully available
Stand-in processing	Payments keep flowing during batch and outages	Reconciliation work and the risk of approving against a stale balance

Failure modes

- **End of day overruns.** Volumes grow until the batch no longer fits its window, delaying the next business day.
- **Stand-in drift.** The shadow balance and the core disagree, and a customer is allowed to overdraw or is wrongly declined.
- **Hot-account contention.** A few very busy accounts slow every posting that touches them.
- **Configuration errors.** A wrongly set product parameter charges or pays interest incorrectly across thousands of accounts at once.

When to use it, and when to avoid it

Every bank needs a system of record, so the question is not whether to have a core but how much to put in it. Keep the core to what only it can do: accounts, balances, the ledger and product rules. Move customer journeys, payment orchestration and analytics outside it, where they can change faster. Avoid putting logic in the core simply because it is the one system that already has the data.

Questions for a design review

- Which work must stay in the core, and which could move to a system that changes faster?
- Does end of day still fit its window at next year's expected volumes, with margin?
- What happens to payments while the core is in its batch window, and how are stand-in approvals reconciled?
- Which accounts are hot spots, and how is contention on them handled?
- How are product parameter changes reviewed and tested before they reach live accounts?

Notes

1. **SBI deepens partnership with TCS to drive innovation and enhance customer experience** <https://tcs.com/who-we-are/newsroom/press-release/sbi-deepens-partnership-with-tcs-to-drive-innovation-enhance-customer-experience>, Tata Consultancy Services. **Vendor**, accessed 29 September 2026.
Supports: SBI's core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years (as of 6 October 2021).
2. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html, Business Standard. **Reported**, accessed 29 September 2026.
Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).
3. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>, Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services (as of 20 September 2022).
4. **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text)** <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0>, Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day (as of 7 November 2023).

Chapter 5

Payment system architecture

A payment system moves messages between banks, then settles money between them. Each payment is a state machine with exactly one outcome. Idempotency and reversals keep it that way.

Next, the architecture of payment systems themselves: switches, settlement and the state machine that stops a payment being lost or made twice.

Why it matters

Payments are where banking meets the outside world in real time. A customer who taps “pay” expects an answer in seconds, and a merchant expects the money to be there. Behind that answer, several independently run systems must agree on what happened, even when a network link drops halfway through. Getting that agreement right, every time, is the core problem of payment architecture.

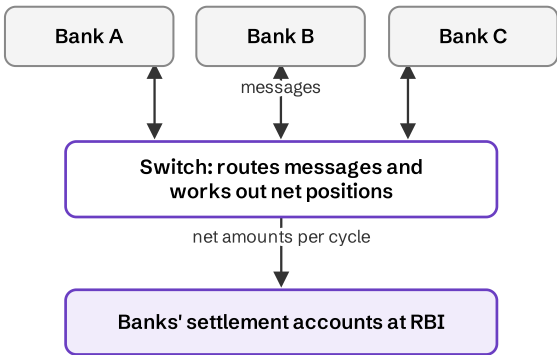
The model explained

Participants, switch and settlement

A payment system has **participants**, usually banks, and an **operator** that runs a central **switch**. The switch receives a payment message from the payer’s bank, routes it to the payee’s bank, collects the answer and passes it back. Smaller banks and non-bank firms often join through a **sponsor bank** that is a direct member and settles on their behalf.

Moving the message is only half the job. **Settlement** moves the money between banks, in the accounts they hold at the central bank. Some systems settle each payment on its own; others settle the net amount each bank owes at intervals.

From payment messages to settlement



Illustrative. Gross systems skip the netting step and settle each payment directly.

Message standards

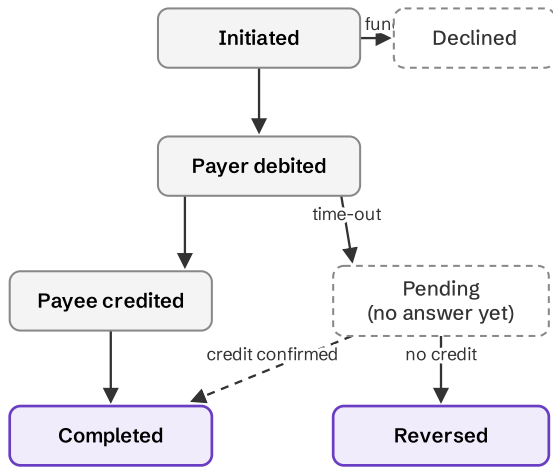
Messages follow published formats so that every participant can read them. Card and ATM networks have long used ISO 8583, a compact format built for authorisations. ISO 20022 is a richer, structured format increasingly used for high-value and cross-border payments, because it carries more information about the

payer, the payee and the purpose. UPI defines its own interface specifications, which banks and apps must implement and certify against.

Every payment is a state machine

A payment moves through a small number of states and must end in exactly one final state. The difficult cases are the ones in the middle: the payer has been debited but no answer has come back from the payee's bank.

States of a push payment



Illustrative. Real systems use more states and different names, but the shape is the same.

Idempotency: the same request twice must do nothing new

Networks fail, so senders retry. If a retry is processed as a new payment, the customer pays twice. Every payment therefore carries a unique reference created by the sender, and every system in the chain records references it has already handled. A repeat with a known reference returns the original answer instead of moving money again. The same reference lets any party ask later, “what happened to this payment?”, and get one consistent answer.

Reversals, disputes and reconciliation

A pending payment is resolved either by confirming the credit or by reversing the debit. At the end of each cycle, every bank compares its own records with the operator’s settlement report. Any mismatch becomes an exception to investigate. Disputes, such as a customer saying goods never arrived, follow a separate, slower process with its own rules and deadlines.

How it plays out in Indian banking

India runs both kinds of settlement side by side. RTGS settles each transaction in real time on a one-to-one gross basis.¹ When NEFT moved to 24x7 in December 2019, RBI set 48 half-hourly settlement batches a day.² Cheques now settle on a fixed hourly rhythm: Under continuous clearing, CTS settles every hour from 11:00, based on positive confirmations and deemed approvals from drawee banks.⁵

Scale turns rare edge cases into daily events. At about 791 million a day⁴, even a tiny share of time-outs means many stuck payments every day, so the rules for resolving them matter. RBI's framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint.³ If a UPI transfer debits the payer but does not credit the beneficiary, the beneficiary bank must reverse it by T+1 day; after that, ₹100 a day is payable.³ If a UPI payment to a merchant debits the payer but the merchant gets no confirmation, it must be reversed within T+5 days; after that, ₹100 a day is payable.³

These deadlines shape system design. A bank needs automated status checks, reversal jobs that run well inside the limit and records that prove when each step happened.

Trade-offs

Payment design choices

Choice	You gain	You give up
Gross settlement	No settlement risk between banks	Banks need more money on hand in their settlement accounts
Net settlement	Far less money needs to move	Exposure between banks until the cycle settles
Credit the customer before settlement	An instant experience	The bank carries the risk until settlement completes
Strict time-outs	Fast answers for customers	More payments land in the pending state and need resolving

Failure modes

- **Duplicate payments** when a retry is treated as new because references are missing or not checked.
- **Stuck payments** that stay pending because no job asks for their status or reverses them in time.
- **Reconciliation breaks** when a bank's records and the operator's report disagree and no one owns the difference.
- **Sponsor-bank bottlenecks** when many smaller participants depend on one direct member's systems.

When to use it, and when to avoid it

Use this model, a central switch with a state machine per payment, for any system where many independent parties must agree on money. Avoid building a private payment network where a public rail already does the job; joining the existing rail is usually cheaper and safer. Inside a bank, avoid letting each channel talk to each rail directly. A single payment hub that owns references, states and reconciliation is easier to control.

Questions for a design review

- Where is the unique reference created, and does every retry reuse it?
- Which component owns each payment's state, and can it answer a status query at any time?
- How are pending payments found and resolved inside the regulator's time limits?
- What does reconciliation compare, how often, and who owns each exception?
- What happens to in-flight payments if the switch connection drops?

Notes

1. **About IDRBT** <https://www.idrbt.ac.in/about-idrbt>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.

Supports: RTGS settles each transaction in real time on a one-to-one gross basis (as of 1 January 2025).

2. **Availability of National Electronic Funds Transfer (NEFT) System on 24x7 basis (RBI/2019-20/111)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11750>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: When NEFT moved to 24x7 in December 2019, RBI set 48 half-hourly settlement batches a day (as of 6 December 2019).

3. **Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems (RBI/2019-20/67)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11693>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: If a UPI transfer debits the payer but does not credit the beneficiary, the beneficiary bank must reverse it by T+1 day; after that, ₹100 a day is payable (as of 20 September 2019); If a UPI payment to a merchant debits the payer but the merchant gets no confirmation, it must be reversed within T+5 days; after that, ₹100 a day is payable (as of 20 September 2019); RBI's framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint (as of 20 September 2019).

4. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-ncpi-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).

5. **Introduction of Continuous Clearing and Settlement on Realisation in Cheque Truncation System (RBI/2025-26/73)** <https://website.rbi.org.in/documents/d/rbi/circulardatedaugust132025cts>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Under continuous clearing, CTS settles every hour from 11:00, based on positive confirmations and deemed approvals from drawee banks (as of 13 August 2025).

Chapter 6

API-first and open banking

API-first design exposes a bank’s capabilities through stable, versioned interfaces. A gateway and orchestration layer protect the core. Account Aggregators apply the idea to consented data sharing.

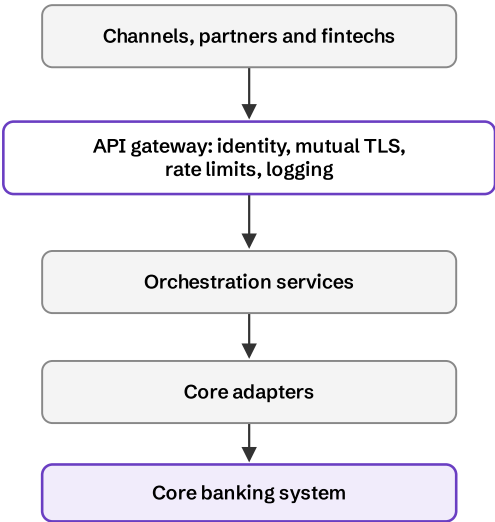
Payments and the core both need a safe front door. This chapter covers the API layers that provide one, and India’s framework for consented data sharing.

Why it matters

A modern bank serves customers through its own apps, partners’ apps, branches and payment rails at the same time. If each of these connects to the core in its own way, every change becomes a project and every new partner a risk. API-first design says: decide the interface first, publish it, version it and put controls in front of it. Channels and partners then build against a stable contract rather than against the core’s internals.

The model explained

Layers of an API-first bank



Illustrative. Layer names vary; the separation of concerns is what matters.

Channels are the callers: the bank’s apps, partner apps, internal tools. **The gateway** is the front door. It checks who is calling, enforces quotas, rejects malformed requests and records every call. **Orchestration services** combine steps into a business action, such as “open an account” or “make a payment”, calling several systems in the right order. **Core adapters** translate between clean API models and the core’s own interfaces, so the core can change, or be replaced, without breaking every caller.

What the gateway is responsible for

- **Identity:** every call carries credentials; partners are identified by certificates or tokens.
- **Mutual TLS:** for machine-to-machine traffic, both sides present certificates, so each proves who it is.
- **Rate limits and quotas:** a misbehaving partner cannot exhaust capacity meant for everyone.
- **Validation:** requests that do not match the published schema are rejected before they reach anything valuable.
- **Observability:** every request is logged and traced, which is how incidents are investigated later.

Designing good bank APIs

Good bank APIs share a few habits. They name business resources, such as accounts, payments and mandates, rather than exposing internal tables. Every request that moves money accepts an idempotency key, so a retried call cannot pay twice. Lists are paged, so one call cannot pull a million transactions. Errors use stable, documented codes that tell the caller whether to retry, correct the request or give up. Timestamps carry time zones, and amounts carry currencies. These details sound small, but they decide whether partners can build reliable products on top.

Versioning, sandboxes and certification

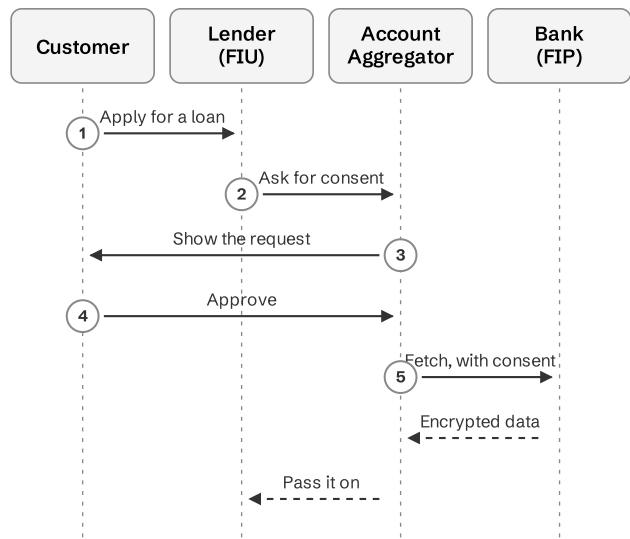
Published APIs change slowly and carefully. A new version runs alongside the old one for a notice period, and callers move across on their own schedule. Partners build first against a sandbox with test data, then pass a certification step before they get production access. For shared public infrastructure, the operator usually publishes the specification and runs the certification.

Onboarding a partner is as much a governance process as a technical one. Before production access, the bank checks who the partner is, what data the use case genuinely needs and how the partner will protect it. Access is then scoped to exactly that use case, reviewed periodically and withdrawn when the relationship ends. A register of every partner, credential and permitted operation makes those reviews possible.

How it plays out in Indian banking

India's Account Aggregator (AA) framework is API-first thinking applied to data sharing across the whole financial system. RBI issued its Master Direction for Account Aggregators on 2 September 2016; an Account Aggregator must be a non-bank financial company registered with RBI.¹ No financial information is retrieved, shared or transferred through an Account Aggregator without the customer's explicit consent, and joining is voluntary.² Customer data passing through an Account Aggregator is not visible to, and does not reside with, the aggregator.³ Everyone builds to one published specification: Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT.³

A consented data request through an Account Aggregator



Simplified and illustrative. Real flows include consent artefacts, encryption keys and notifications.

The same pattern extends to lending. The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai.⁴

Trade-offs

API design choices

Choice	You gain	You give up
One gateway for all traffic	Consistent security and visibility	A critical component that must scale and stay available
Thin core adapters	The core can be replaced behind a stable interface	Another layer to build and run
Long version overlaps	Partners are not forced to change at once	More versions to support and test
Shared public specifications	One integration works with every participant	Less freedom to add bank-specific features

Failure modes

- **The gateway becomes the bottleneck** because it was sized for normal traffic, not for a salary day or a festival sale.
- **Orchestration leaks into the gateway**, turning it into a hard-to-test tangle of business rules.
- **Breaking changes** reach callers because a version was changed in place instead of added alongside.
- **Over-broad access**, where a partner token can do more than its use case needs.

When to use it, and when to avoid it

Use API-first design wherever more than one caller needs the same capability, and certainly wherever partners are involved. Avoid publishing an API for something only one internal system will ever use; a direct, well-tested link may be simpler. Avoid exposing the core's own data model as the public API, because it ties every caller to the core forever.

Questions for a design review

- Is this interface designed for its callers, or does it mirror the core's own data model?
- How are partners identified, and what exactly can each partner's credentials do?
- What are the rate limits for a salary day or a festival sale, not just a normal day?
- How will a breaking change be introduced without forcing every caller to move at once?
- Can every request be traced from the gateway to the core and back?

Notes

1. **Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 (updated 6 September 2024)** http://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI issued its Master Direction for Account Aggregators on 2 September 2016; an Account Aggregator must be a non-bank financial company registered with RBI (as of 6 September 2024).
2. **Account Aggregator Framework** <https://financialservices.gov.in/account-aggregator-framework>. Department of Financial Services, Ministry of Finance. **Primary source**, accessed 29 September 2026.
Supports: No financial information is retrieved, shared or transferred through an Account Aggregator without the customer's explicit consent, and joining is voluntary (as of 29 September 2026).
3. **Consultation paper on Financial Information Users in the securities markets under the Account Aggregator framework** https://www.sebi.gov.in/sebi_data/attachdocs/aug-2023/1690887848711.pdf. Securities and Exchange Board of India. **Primary source**, accessed 29 September 2026.
Supports: Customer data passing through an Account Aggregator is not visible to, and does not reside with, the aggregator (as of 1 August 2023); Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT (as of 1 August 2023).
4. **Reserve Bank Innovation Hub** <https://rbihub.in/>. Reserve Bank Innovation Hub. **Primary source**, accessed 29 September 2026.
Supports: The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai (as of 29 September 2026).

Chapter 7

Event-driven architecture

Event-driven systems announce what happened instead of asking others to act. A durable log lets consumers react at their own pace. The outbox pattern keeps events and data in step.

APIs answer requests. Many systems also need to react to what has happened; this chapter covers events, logs and the outbox pattern.

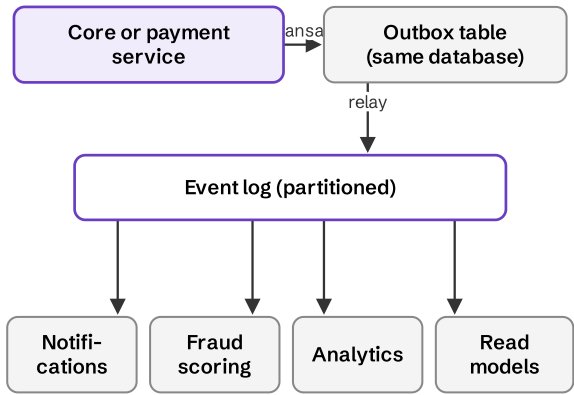
Why it matters

In a request-driven design, the system that records a payment must also call the notification service, the fraud system, the analytics store and anyone else who cares, and wait for each. Every new consumer means changing the payment system. In an event-driven design, the payment system publishes one fact, “payment 123 completed”, and anyone interested subscribes. The producer does not need to know who is listening, and a slow consumer cannot slow down the payment.

The model explained

An **event** records something that has already happened, with the details needed to act on it. A **request** asks for something to happen and expects an answer. Events are published to a **log**: an ordered, durable sequence that consumers read at their own pace and can replay from any point.

One event, many consumers



Illustrative. Consumers are examples; each keeps its own position in the log.

Designing events

A good event describes a business fact in the past tense, such as payment completed or mandate cancelled, and carries enough detail that most consumers need not call back for more. Its structure is registered in a shared schema registry, so producers and consumers agree on the format. Changes are additive where possible: new fields can be added, but existing ones are not removed or renamed without a new event version. Each event carries a unique identifier, the time it happened and the identifier of the thing it describes, which together make idempotent processing and tracing possible.

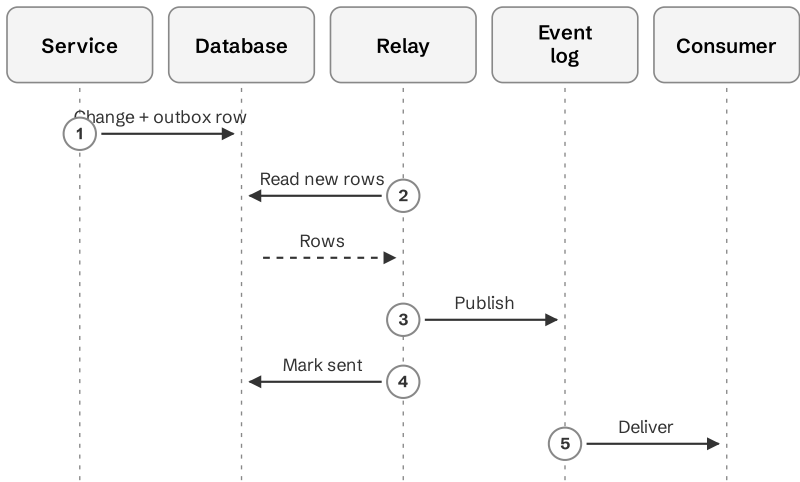
Event sourcing and CQRS

Event sourcing goes further: the events themselves are the record, and the current balance is calculated by replaying them. Banking has always worked a little like this, since a ledger is a list of postings. **CQRS** (command query responsibility segregation) separates the model that accepts changes from the models that answer questions. A mobile app's "recent transactions" screen can read from a fast read model built from events, instead of querying the core.

The outbox pattern and change data capture

The hardest practical problem is keeping the database and the event log in step. If a service updates its database and then publishes an event, a crash between the two leaves them disagreeing. The **outbox pattern** writes the change and a record of the event in the same database transaction; a separate relay then publishes outbox records to the log and marks them sent. **Change data capture** (CDC) achieves a similar result by reading the database's own change log.

The outbox pattern



Illustrative. The relay may deliver an event more than once, so consumers must handle repeats.

Exactly once, ordering and partitions

Some products promise exactly-once delivery. That promise holds inside the product; once an event causes a change in another system, such as a ledger, the consumer still needs its own idempotency check, usually by recording each event's identifier. Ordering is guaranteed only within a **partition**, so events that must stay in order, such as every event for one account, are sent to the same partition by using the account number as the key.

How it plays out in Indian banking

Events suit the work that surrounds a payment rather than the payment itself: alerts to customers, fraud features, analytics, audit trails and read models for apps. The core posting stays a request with a definite answer. The scale makes the decoupling valuable. At about 791 million a day¹ across the UPI system, a bank cannot afford for a slow analytics job to hold up payments. The events also form an audit trail: an ordered, time-stamped record of what each system saw and when.

Trade-offs

Event-driven design choices

Choice	You gain	You give up
Publish events instead of calling consumers	New consumers without changing the producer	No immediate confirmation that a consumer acted
Durable, replayable log	Consumers can rebuild state and recover from bugs	Storage, retention rules and a platform to run
Read models built from events	Fast screens that do not load the core	Read models lag behind by seconds or more
Event sourcing	Full history and easy audit	Complex queries and careful handling of changes to event formats

Failure modes

- **Lost events** when a service writes to its database and publishes separately, without an outbox or CDC.
- **Duplicate effects** when consumers assume each event arrives exactly once.
- **Out-of-order processing** when related events land in different partitions.
- **Silent lag**, where a consumer falls hours behind and no alert fires because nothing has technically failed.
- **Format breakage** when a producer changes an event’s structure and old consumers cannot read it.

When to use it, and when to avoid it

Use events when several systems need to react to the same fact, when consumers can tolerate a short delay, or when an ordered history is valuable in itself. Avoid them for the step that must give the customer a definite yes or no, such as authorising a debit. That step is better as a request with a clear answer, followed by an event that tells everyone else.

Questions for a design review

- Which step must give a definite answer, and which steps can react later to an event?
- How does the producer guarantee that a database change and its event never disagree?
- How does each consumer detect and ignore an event it has already processed?
- Which events must stay in order, and what partition key keeps them together?
- How far behind can each consumer fall before someone is alerted?

Notes

1. [UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn](https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html) https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.
Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).

Chapter 8

Data architecture

Banks keep transaction and analytical systems apart. Data flows between them through batch and streaming pipelines. Regulatory reporting depends on that flow being complete and traceable.

Events and transactions become data. This chapter follows it from transaction systems to the reports regulators rely on.

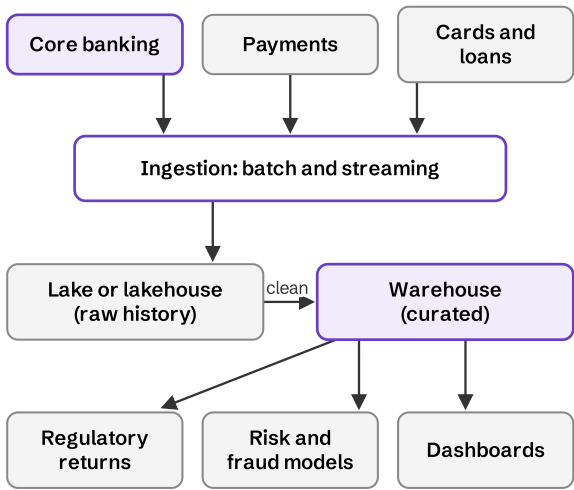
Why it matters

Every balance, payment and loan in a bank is data, and so is every report to the regulator. A bank that cannot trace a figure in a regulatory return back to the transactions behind it cannot prove the figure is right. Good data architecture makes that tracing routine. It also lets risk models, fraud systems and management reports use the same trusted numbers instead of each building its own.

The model explained

Transaction systems (OLTP) record individual events quickly and safely: a core ledger, a payment switch, a card system. They are optimised for many small writes. **Analytical systems** (OLAP) answer questions across millions of records: how many loans are overdue, which merchants are growing. They are optimised for large reads. Running heavy analysis on a transaction system slows it down for customers, so data is copied from one to the other.

How data flows from transactions to reports



Illustrative. Many banks run several of each store.

Warehouses, lakes and lakehouses

A **data warehouse** holds cleaned, structured data with agreed definitions: one meaning of “active customer”, one meaning of “overdue”. A **data lake** holds raw data of every kind, cheaply, before anyone has decided how to use it. A **lakehouse** combines the two, adding warehouse-style tables and controls on top of lake storage. Most banks end up with some of each.

Batch and streaming

Batch pipelines move data in bulk, often overnight after end of day, and suit reports that need a complete, balanced day. Streaming pipelines move each change within seconds and suit fraud detection, alerts and live dashboards. The two often feed the same stores.

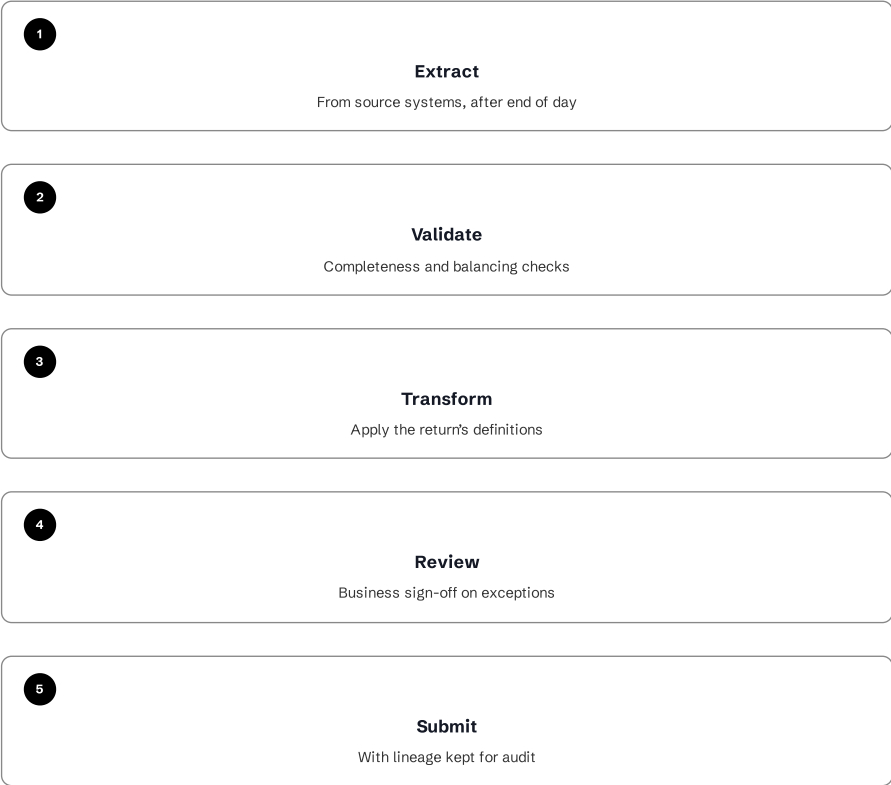
Feature stores for models

Risk and fraud models need the same inputs, called features, at training time and at the moment of a decision: “number of payments in the last hour”, “average balance over 90 days”. A **feature store** calculates these once and serves them consistently to both, so a model is not trained on one definition and run on another.

Lineage and quality

Lineage records where each figure came from and every step that changed it. **Data quality controls** check completeness, validity and consistency at each step: did every branch's data arrive, do debits equal credits, do totals match the source. For regulatory reporting, these are not extras. They are how a bank shows that a return is right.

A regulatory reporting pipeline



Illustrative. Each step records lineage and quality results.

Retention and deletion

Keeping data forever is neither cheap nor safe. Each class of data needs a retention period, set by legal and regulatory requirements and by business need, and a process that deletes or anonymises it when that period ends. Deletion must reach every copy, including backups, analytics stores and test environments, and be recorded so it can be proved. Personal data protection law adds purpose limits: data collected for one use should not quietly be reused for another.

How it plays out in Indian banking

Where data may live is a design constraint, not only a policy. RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad.¹ Any pipeline, copy or backup of payment data must respect that, including test and analytics copies. When data moves to a cloud platform, RBI expects the whole lifecycle to be governed: When using cloud services, a regulated entity's outsourcing policy must cover the whole lifecycle of data, from creation and entry into the cloud until it is permanently deleted.³ Backups count only if they work: Regulated entities must back up data and periodically restore it to check that it is usable.²

Trade-offs

Data design choices

Choice	You gain	You give up
One central warehouse	One agreed definition of every figure	A central team that can become a bottleneck
Raw data in a lake	Cheap storage and freedom to explore	Risk of a swamp of undocumented, untrusted data
Streaming pipelines	Fresh data for fraud and alerts	More moving parts and harder reconciliation
Strict lineage	Figures that can be proved	Engineering effort on every pipeline

Failure modes

- **Two versions of the truth**, when different teams define the same measure differently.
- **Silent gaps**, when one source’s feed fails and the report runs anyway on partial data.
- **Copies nobody governs**, such as test databases full of real customer data.
- **Lineage that stops at the warehouse**, so a figure can be traced back to a table but not to the transactions behind it.

When to use it, and when to avoid it

Invest in a governed warehouse, lineage and quality checks for anything that feeds a regulator, a board or a model that decides credit. For exploratory work, a lake with light controls is fine, as long as nothing leaves it for a decision or a report without passing through the governed path. Avoid copying production data into lower environments at all, unless it is masked.

Questions for a design review

- Can every figure in a regulatory return be traced to the transactions behind it?
- Which quality checks stop a report running on partial data?
- Is there one agreed definition of each key measure, and who owns it?
- Where do copies of payment data live, including backups, logs and test environments?
- When is data deleted, and how is deletion proved?

Notes

1. **Storage of Payment System Data (RBI/2017-18/153)** <https://rbi.org.in/scripts/NotificationUser.aspx?Id=11244>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI’s circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad (as of 6 April 2018).

2. **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text)** <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: Regulated entities must back up data and periodically restore it to check that it is usable (as of 7 November 2023).

3. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: When using cloud services, a regulated entity’s outsourcing policy must cover the whole lifecycle of data, from creation and entry into the cloud until it is permanently deleted (as of 10 April 2023).

Chapter 9

Legacy modernisation

Replacing a core in one move is among the riskiest things a bank can do. Most succeed by changing it in stages. The strangler fig moves one capability at a time until the old system retires.

The earlier chapters describe systems as they are. This one covers how banks change them without stopping the business.

Why it matters

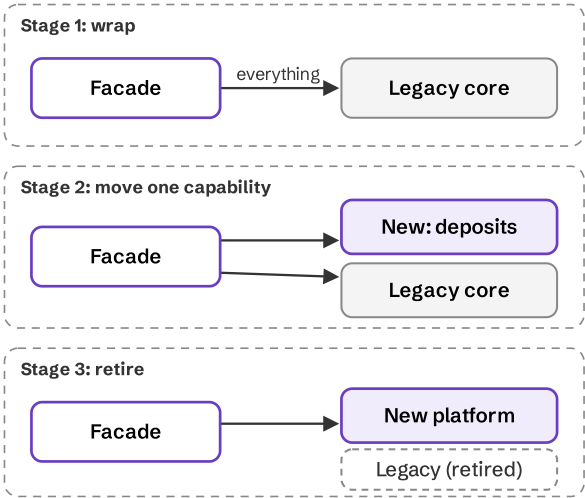
A bank’s core holds decades of products, rules and integrations. Replacing it means moving every account and open loan without losing a rupee, while the bank keeps trading. A “big bang” replacement, where everything switches on one weekend, concentrates all of that risk into one moment. Incremental approaches spread it out, so each step is small enough to test, reverse and learn from.

The model explained

The strangler fig

Named after a vine that grows around a tree until it can stand on its own, the **strangler fig** pattern puts a facade in front of the old system. At first the facade simply passes every request through. Then, one capability at a time, requests are routed to new services instead. When nothing is left routed to the old system, it can be switched off.

The strangler fig, in three stages



Illustrative. Real programmes move many capabilities, often over several years.

Supporting patterns

- **Anti-corruption layer.** New services talk to the old system only through a translator, so the old system’s data model and quirks do not leak into the new design.

- **Wrapping the core.** Before replacing anything, put APIs in front of the core. Channels then depend on the APIs, not the core, which makes every later step easier.
- **Branch by abstraction.** Inside a codebase, introduce an interface over the thing being replaced, move callers to the interface, then swap what sits behind it.
- **Hollowing out.** Move functions such as payments, customer data or lending out of the core one by one, leaving it as a thinner ledger.

Sequencing the moves

Order matters. Many programmes start with capabilities that are valuable but loosely coupled to the ledger, such as customer onboarding, notifications or a new digital product, because they can move without touching balances. Deposits and loans move later, product by product, once migration tooling and reconciliation have been proven on smaller waves. The general ledger and end-of-day processing usually move last, because everything depends on them.

Data migration and parallel runs

Data is usually the hardest part. Migration moves accounts in waves, by product, region or customer segment, with automated checks that every balance, rate and schedule arrived intact. A **parallel run** processes real transactions through both old and new systems and compares the results before customers depend on the new one. Differences found in a parallel run are cheap; differences found by customers are not.

Cutover

Cutover is the moment a wave of customers starts being served by the new system. It needs a rehearsed plan, a clear decision point, a tested way back and enough people on hand to resolve problems quickly. Most failed migrations fail here, usually because the rollback was never really tested.

How it plays out in Indian banking

Core changes at large Indian banks are multi-year programmes. SBI's core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years.¹ Most are carried out with vendors and system integrators, which brings RBI's outsourcing rules into scope: RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023.² A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement.² A new core must also meet the same resilience tests as the old one before it goes live. A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day.³

Trade-offs

Modernisation approaches

Approach	You gain	You give up
Big-bang replacement	One short transition; no long period of two systems	All risk concentrated in one event
Strangler fig	Small, reversible steps; value delivered early	Years of running old and new side by side
Wrap first, replace later	Immediate agility for channels	The old core lives on, and the wrapper can become permanent
Hollow out the core	Fast-changing functions move to modern systems	More integration points to keep consistent

Failure modes

- **The permanent middle**, where the old and new systems both keep running indefinitely because the last capabilities are never moved.
- **Untested rollback**, discovered only when a cutover goes wrong.
- **Migration defects** that surface weeks later as wrong interest or charges.
- **Scope creep**, where the migration becomes a chance to redesign every product at once.
- **Knowledge loss**, when the people who understood the old system leave before its rules are documented.

When to use it, and when to avoid it

Prefer incremental change whenever the old system can be wrapped and the business can tolerate running two systems for a while, which is most of the time. Consider a big-bang switch only for small, self-contained systems, or when the old one is failing so badly that running it longer is the greater risk. In every case, test the rollback as seriously as the rollout.

Questions for a design review

- What will be wrapped first, so that channels stop depending on the old system directly?
- In what order will capabilities move, and what is the first small move that proves the approach?
- How will migrated balances, rates and schedules be checked, account by account?
- What will the parallel run compare, and for how long?
- Has the rollback been rehearsed end to end, with real data volumes?

Notes

1. **SBI deepens partnership with TCS to drive innovation and enhance customer experience** <https://tcs.com/who-we-are/newsroom/press-release/sbi-deepens-partnership-with-tcs-drive-innovation-enhance-customer-experience>. Tata Consultancy Services. **Vendor**, accessed 29 September 2026.
Supports: SBI's core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years (as of 6 October 2021).
2. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?Id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023 (as of 10 April 2023); A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement (as of 10 April 2023).
3. **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text)** <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day (as of 7 November 2023).

Chapter 10

Security architecture

Bank security relies on layers, so no single failure exposes money or data. Networks are zoned, keys live in hardware and admin access is granted only when needed. Incidents are reported in hours.

Every layer described so far needs protecting. This chapter explains defence in depth as banks apply it, conceptually and without describing any organisation's controls.

Why it matters

Banks are attractive targets because they hold money and personal data, and because their systems connect to thousands of others. Security architecture decides how far an attacker can get after the first mistake: a phished password, an unpatched server, a misconfigured cloud bucket. The goal is not a system that can never be breached, but one where a breach is contained, detected quickly and reported properly.

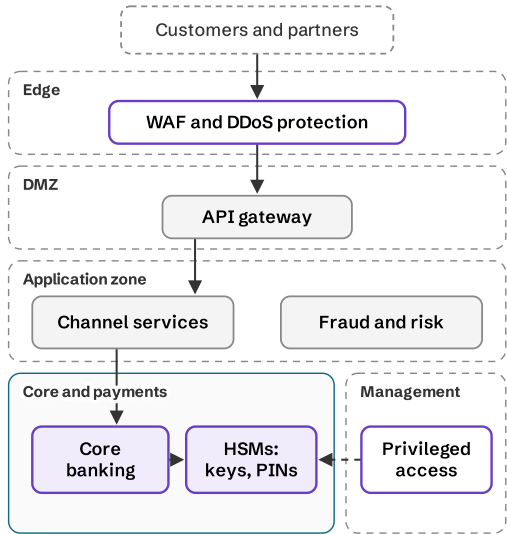
This page describes principles and common patterns only. It does not describe any organisation's actual controls.

The model explained

Defence in depth and zones

Defence in depth stacks independent controls so that each failure is caught by the next layer. The network is split into **zones** by trust level, and traffic between zones passes through controlled points. The most sensitive systems, such as the core ledger and the systems that handle keys and PINs, sit in the innermost zone and accept connections only from specific systems in the zone next to them.

Security zones in a typical bank



Illustrative and conceptual. The dashed line is administrative access only. Real networks have more zones and many controls not shown.

Card data scope

Systems that store, process or transmit card numbers fall under strict card-industry security rules. Architects shrink that **scope** by keeping card data in as few systems as possible and replacing it with tokens everywhere else, so most of the estate never sees a real card number.

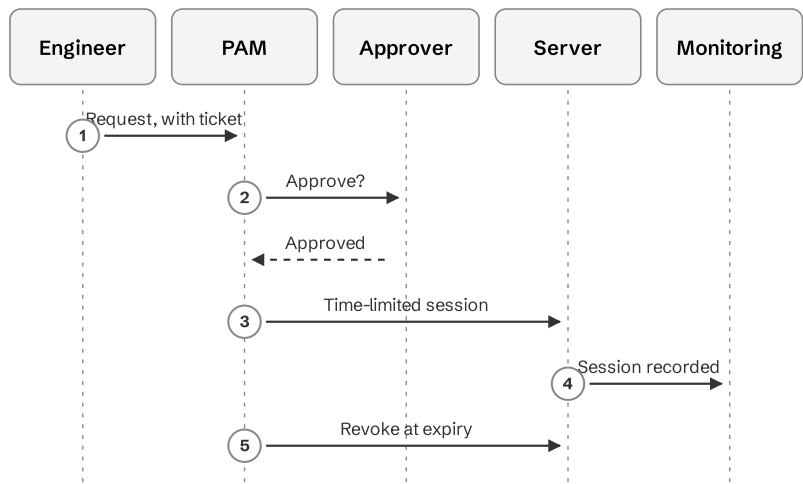
Hardware security modules

A **hardware security module** (HSM) is a tamper-resistant device that stores cryptographic keys and performs operations with them, such as verifying a PIN or signing a message, without ever revealing the key. Payment PINs are checked inside HSMs, so no application server ever holds a PIN in clear text.

Privileged access, just in time

Administrator accounts can change anything, so they are the most valuable thing an attacker can steal. **Privileged access management** (PAM) keeps those credentials in a vault, grants access through a controlled gateway and records every session. **Just-in-time access** goes further: nobody holds standing administrator rights, and access is granted for a specific task, approved, time-limited and revoked automatically.

Just-in-time privileged access



Illustrative and conceptual.

Secrets, zero trust and detection

Applications need passwords, keys and certificates to talk to each other. A **secrets vault** issues them at run time and rotates them, so they are never written into code or configuration files. **Zero trust** means no request is trusted just because it comes from inside the network; every call is authenticated and authorised. A **SIEM** collects logs from across the estate and raises alerts on suspicious patterns, and a security operations team investigates them.

How it plays out in Indian banking

RBI sets the governance frame for IT and cyber security: RBI issued the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on 7 November 2023 (RBI/2023-24/107).⁵ Reporting deadlines are short, and they apply even when the incident happens at a supplier. CERT-In's directions of 28 April 2022 under section 70B(6) of the IT Act require reportable cyber incidents to be reported to CERT-In within 6 hours of noticing them; they took effect 60 days after issue.¹ A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them.² Detection and escalation therefore have to be fast enough to meet those clocks.

Card data rules have shrunk the attack surface for online payments. Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead.³ Digital certificates for the banking sector have their own certifying authority: IDRBT is the certifying authority for digital certificates in the Indian banking and financial sector under the IT Act, 2000.⁴

Trade-offs

Security design choices

Choice	You gain	You give up
Many small zones	A breach stays contained	More rules to manage and more paths to test

Choice	You gain	You give up
Just-in-time admin access	No standing credentials to steal	Slower emergency fixes unless break-glass access is designed well
Tokens instead of card numbers	Most systems leave card-data scope	A tokenisation service that must itself be highly available
Central log collection	Incidents can be seen across the estate	Large volumes of data to store, protect and analyse

Failure modes

- **Flat networks**, where one compromised server can reach the core directly.
- **Standing administrator accounts** shared by teams, with no record of who did what.
- **Secrets in code** or configuration files that end up in a repository or a backup.
- **Alerts no one reads**, where monitoring exists but is not staffed or tuned.
- **Supplier blind spots**, where an incident at a service provider is not passed on quickly enough to meet reporting deadlines.

When to use it, and when to avoid it

Every principle here applies to every bank; the question is depth. Put the strongest controls around what would hurt most: money movement, keys, customer data and administrator access. Avoid security measures that people work around, such as approval steps so slow that teams share credentials to meet a deadline. A control that is bypassed in practice gives false comfort.

Questions for a design review

- If one application server is compromised, which systems can it reach?
- Who holds standing administrator rights today, and could that be replaced with just-in-time access?
- Where are keys and PINs handled, and does any application ever see them in clear?
- Where are application secrets stored, and how often are they rotated?
- Can an incident at a supplier be detected and reported to the regulator within the deadline?

Notes

1. **Directions under sub-section (6) of section 70B of the IT Act, 2000 (28 April 2022)** https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf. CERT-In, Ministry of Electronics and Information Technology. **Primary source**, accessed 29 September 2026.
Supports: CERT-In's directions of 28 April 2022 under section 70B(6) of the IT Act require reportable cyber incidents to be reported to CERT-In within 6 hours of noticing them; they took effect 60 days after issue (as of 28 April 2022).

2. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them (as of 10 April 2023).

3. **Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)] (RBI/2022-2023/95)** <https://website.rbi.org.in/web/rbi/-/notifications/restriction-on-storage-of-actual-card-data-i.e.-card-on-file-cof-12363>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead (as of 28 July 2022).

4. **About IDRBT** <https://www.idrbt.ac.in/about-idrbt>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.
Supports: IDRBT is the certifying authority for digital certificates in the Indian banking and financial sector under the IT Act, 2000 (as of 1 January 2025).

5. **Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI/2023-24/107)** <https://website.rbi.org.in/web/rbi/-/notifications/master-direction-on-information-technology-governance-risk-controls-and-assurance-practices>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI issued the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on 7 November 2023 (RBI/2023-24/107) (as of 7 November 2023).

Chapter 11

Multi-data-centre and disaster recovery

Banks run critical systems in two or more data centres. Replication decides how much data can be lost and how fast service returns. RBI expects both to be defined, tested and proven.

Security protects against attack; resilience protects against failure. This chapter covers running across data centres, and what the regulator expects from recovery.

Why it matters

A data centre can be lost to a power failure, a flood, a fire or a network cut. For a bank, losing its only site means no payments, no ATMs and no access to money until it is fixed. A second site, kept ready to take over, turns that disaster into an interruption. How ready the second site is, and how much recent data it holds, are design decisions with real costs.

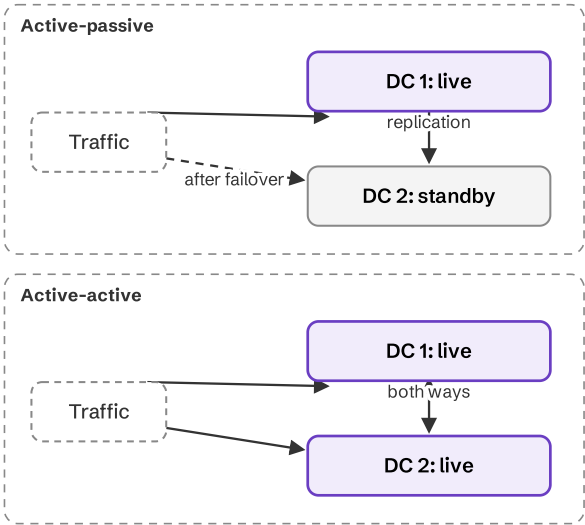
The model explained

Two measures: RPO and RTO

The **recovery point objective** (RPO) is how much data, measured in time, the bank can afford to lose. An RPO of zero means no confirmed transaction may be lost. The **recovery time objective** (RTO) is how quickly service must be back. Both are business decisions first and technical designs second: a lower RPO or RTO costs more.

Active-passive and active-active

Two common topologies



Illustrative. Many banks mix both, choosing per system.

In **active-passive**, one site serves all traffic and the other waits, receiving a copy of the data. Failover means promoting the standby. It is simpler, but the standby sits idle, and a failover is a rare, stressful event. In **active-active**, both sites serve traffic at the same time. Losing one halves capacity instead of stopping service, but keeping one set of balances consistent across two live sites is hard.

Synchronous and asynchronous replication

With **synchronous replication**, a transaction is confirmed only after both sites have it. That gives an RPO of zero but adds the network round trip to every transaction, which limits how far apart the sites can be. With **asynchronous replication**, the primary confirms first and the copy follows a moment later. It is faster and allows distant sites, but the last few transactions can be lost in a failure and must be reconciled.

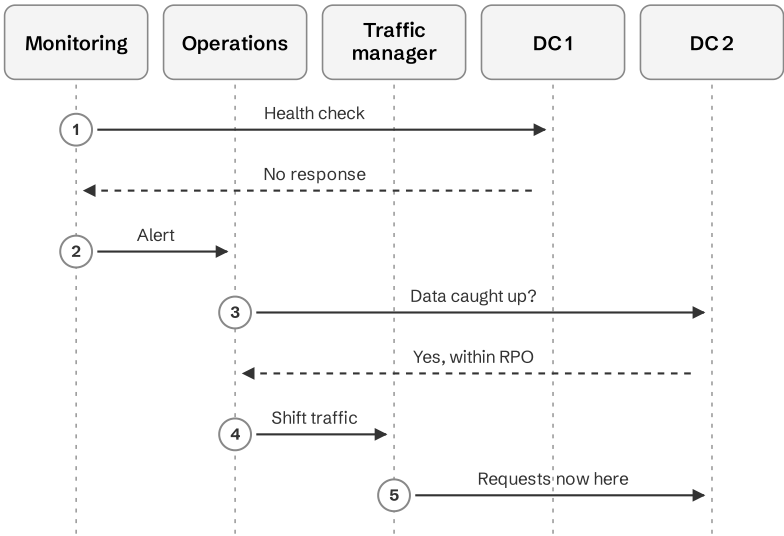
Split-brain

If the link between two sites fails, each may think the other is down and start acting as the primary. Two sites then accept conflicting updates to the same accounts: a **split-brain**. Designs prevent it with a third, independent witness that decides which site may act, and with rules that a site which cannot reach the witness stops accepting writes.

Traffic shifting and drills

Moving traffic from one site to another uses DNS, global load balancers or routing changes, each with its own delay. A failover that has never been practised is a hope, not a plan, so banks run **drills**: planned switches to the second site under real load.

A controlled failover



Illustrative. Real runbooks include many more checks and approvals.

What RBI expects

RBI’s IT governance Direction does not set a single number for every bank. It requires banks to define their own targets, aim high for critical systems and prove them in practice:

- RBI requires regulated entities to define recovery metrics, including a recovery point objective (RPO) and recovery time objective (RTO), for all critical information systems.¹
- For critical information systems, regulated entities should prioritise a minimal RTO, approved by their IT Strategy Committee, and a near-zero RPO; with a non-zero RPO they need a documented method for reconciling data when resuming from the alternate site.¹
- DR drills for critical information systems must be held at least every six months, and major issues found in a drill must be fixed and tested again before the next cycle.¹
- A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day.¹
- Configurations and security patches must be identical at the primary data centre and the DR site.¹
- Regulated entities must back up data and periodically restore it to check that it is usable.¹

No fixed RPO or RTO in the Direction

Earlier drafts of this site claimed RBI mandates specific RPO and RTO values. The Direction read for this page sets no such figures; it requires each bank to define them and to prioritise a near-zero RPO for critical systems.

Trade-offs

Resilience design choices

Choice	You gain	You give up
Active-passive	Simpler consistency; clear primary	Idle capacity and rare, risky failovers
Active-active	Loss of a site reduces capacity instead of stopping service	Hard consistency problems and higher cost
Synchronous replication	No confirmed transaction lost	Slower transactions; sites must be close
Asynchronous replication	Speed and distant sites	Recent transactions can be lost and must be reconciled

Failure modes

- **Drift between sites**, where configuration or patches differ and the standby fails when it is needed.
- **Split-brain** after a network partition, leaving two conflicting sets of balances.
- **Failover that was never really tested** under full load.
- **Shared dependencies**, such as both sites relying on the same identity service, key store or network provider.
- **Backups that cannot be restored**, discovered during the incident.

When to use it, and when to avoid it

Every system that moves money or holds balances needs a tested second site. Choose active-active for the systems where even a short outage is unacceptable and the consistency problem can be solved, for example by partitioning customers between sites. Choose active-passive where simplicity matters more than instant recovery. Avoid claiming an RPO or RTO that the design cannot demonstrate in a drill.

Questions for a design review

- What RPO and RTO has the business approved for each critical system, and can the design meet them?
- Is replication synchronous or asynchronous, and how are any lost transactions reconciled?
- What stops both sites acting as the primary after a network partition?
- When was the last full switch-over drill, and did it run a complete business day at the second site?

- Which dependencies, such as identity, keys or network, are shared by both sites?

Notes

1. Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text) <https://rbio.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0>, Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI requires regulated entities to define recovery metrics, including a recovery point objective (RPO) and recovery time objective (RTO), for all critical information systems (as of 7 November 2023); For critical information systems, regulated entities should prioritise a minimal RTO, approved by their IT Strategy Committee, and a near-zero RPO; with a non-zero RPO they need a documented method for reconciling data when resuming from the alternate site (as of 7 November 2023); DR drills for critical information systems must be held at least every six months, and major issues found in a drill must be fixed and tested again before the next cycle (as of 7 November 2023); A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day (as of 7 November 2023); Configurations and security patches must be identical at the primary data centre and the DR site (as of 7 November 2023); Regulated entities must back up data and periodically restore it to check that it is usable (as of 7 November 2023).

Chapter 12

Hybrid and multi-cloud deployment

Banks split workloads between their own data centres and the cloud. Cloud use counts as outsourcing, with rules on data, security and exit. Multi-cloud adds resilience and cost.

The last architecture chapter asks where each system should run: in the bank's own data centres or in the cloud, and under what rules.

Why it matters

Cloud platforms offer capacity on demand, managed services and fast environments for development. Banks also carry obligations that do not move to the provider: data residency, security, resilience and the ability to leave. Most banks therefore run a **hybrid** estate, keeping some systems in their own data centres and putting others in the cloud. The architecture question is which workload goes where, and how the pieces connect safely.

This page describes general patterns. It does not describe any organisation's actual estate.

The model explained

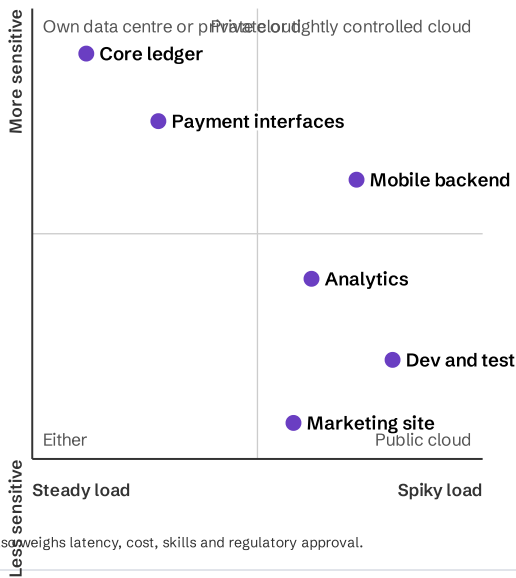
Three kinds of place

On-premises means the bank's own data centres and hardware. **Private cloud** means cloud-style automation on infrastructure dedicated to the bank, in its own premises or a provider's. **Public cloud** means shared infrastructure from a provider, rented by the hour. A **community cloud** is shared among a defined group, such as banks of one type.

Placing workloads

A useful first sort uses two questions: how sensitive is the workload, and how much does it benefit from elastic scale?

A first cut at workload placement

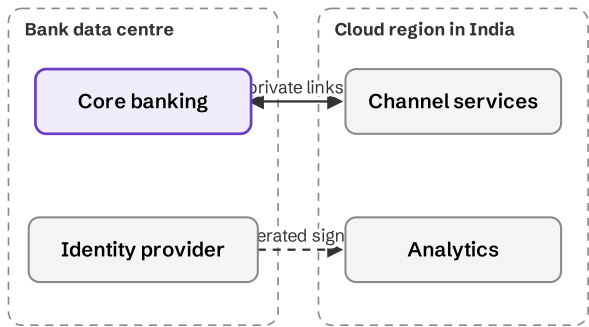


Illustrative. Real placement also weighs latency, cost, skills and regulatory approval.

Connectivity and identity

Workloads in different places must talk to each other securely and predictably. Private, dedicated links between the bank's data centres and the cloud region carry traffic that should never cross the public internet, usually over two separate paths. **Identity federation** lets staff and services use one identity across both environments, so access is granted and removed in one place.

Connecting a data centre to a cloud region



Illustrative and generic.

Making the exit plan real

An exit plan is only useful if it can be carried out. That means knowing, for each workload, which provider-specific services it depends on and what would replace them; keeping data in formats that can be exported; and holding enough skills in-house to run the workload elsewhere. Some banks rehearse exit by periodically restoring a workload's backups into another environment and running it there. The cost of exit is lowest when it is considered at design time, before the workload has grown around one provider's features.

Multi-cloud

Using more than one cloud provider can reduce dependence on one supplier and give a way out if a relationship ends. It also multiplies skills, tooling, security configurations and network links. Many banks use multiple providers for different workloads rather than running the same workload across several.

Cost governance

Cloud costs grow quietly: idle environments, oversized instances, data moving between regions. Tagging every resource to an owner, setting budgets with alerts and reviewing spend regularly keep the bill tied to value.

How it plays out in Indian banking

For a regulated entity, cloud is a form of outsourcing. RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud.¹ When using cloud services, a regulated entity's outsourcing policy must cover the whole lifecycle of data, from creation and entry into the cloud until it is permanently deleted.¹ RBI's Direction describes cloud security as a shared responsibility between the regulated entity and the cloud service provider.¹

Where payment data may be stored limits where some workloads can run: RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad.² And every arrangement needs a way out: A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement.¹

Shared platforms are not new in Indian banking. IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.³

Trade-offs

Deployment choices

Choice	You gain	You give up
Keep a workload on-premises	Full control and simple residency	Slower capacity changes and hardware to own
Move it to public cloud	Elastic capacity and managed services	Outsourcing obligations and dependence on a provider
Single cloud provider	One set of skills and tools	Concentration risk and harder exit
Several providers	Less dependence on any one	More complexity, cost and security surface

Failure modes

- **Accidental exposure** through a misconfigured storage bucket or network rule in the cloud.
- **Data outside approved locations**, for example backups or logs replicated to another region.
- **An exit plan that exists only on paper**, never tested and dependent on provider-specific services.
- **Hidden coupling**, where an on-premises core cannot work without a cloud service, or the reverse, making both a single point of failure.
- **Cost overruns** from resources nobody owns.

When to use it, and when to avoid it

Use public cloud for workloads that benefit from elastic scale, such as channels, analytics and development environments, once the outsourcing, security and residency requirements are met. Keep the systems of record where the bank has the strongest control and the clearest exit path, unless a considered risk assessment says otherwise. Avoid moving a workload only because it is fashionable; move it because the gain is clear and the obligations are covered.

Questions for a design review

- Why does this workload belong where it is placed, in one sentence a regulator would accept?
- Where will its data, backups and logs physically reside?
- Which controls are the bank's responsibility and which are the provider's?
- How would the workload leave this provider, how long would it take, and has that been tested?
- Who owns each cloud resource and its cost?

Notes

1. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud (as of 10 April 2023); When using cloud services, a regulated entity's outsourcing policy must cover the whole lifecycle of data, from creation and entry into the cloud until it is permanently deleted (as of 10 April 2023); RBI's Direction describes cloud security as a shared responsibility between the regulated entity and the cloud service provider (as of 10 April 2023); A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement (as of 10 April 2023).

2. **Storage of Payment System Data (RBI/2017-18/153)** <https://rbi.org.in/scripts/NotificationUser.aspx?id=11244>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad (as of 6 April 2018).

3. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services (as of 20 September 2022).

Part III

Technologies

Twelve families of technology found in Indian banking. Each chapter surveys the main options in a landscape table, explains how to choose between them and lists the pitfalls that catch teams out.

Start here introductory

Core banking platformsThe main commercial and cloud-native cores, how they are deployed, what they depend on, and how banks choose.3 min read (chapter 13)

DatabasesRelational engines for ledgers, clustering, caches, document and key-value stores, and what money needs from each.3 min read (chapter 14)

Mobile technologiesNative Android and iOS, Flutter and Kotlin Multiplatform, design systems, device binding and app security, SDKs and updates.3 min read (chapter 22)

Programming languagesJava, Go, Python, TypeScript, Kotlin, Swift, Dart and legacy COBOL: where each fits in banking, and why.3 min read (chapter 23)

Next intermediate

Messaging and streamingQueues versus logs, the main products, stream processing, and the patterns that keep money safe when messages repeat.3 min read (chapter 15)

Middleware and integrationESB versus API gateway versus service mesh, the main products, and translating between SOAP, REST, gRPC and ISO messages.4 min read (chapter 16)

Containers and orchestrationKubernetes, Helm, GitOps with Argo CD or Flux, Terraform, workflow engines, and what regulated workloads need on top.3 min read (chapter 17)

Cloud platformsAWS, Azure, Google Cloud and Oracle Cloud in Indian banking: regions in India, regulatory constraints and community cloud.3 min read (chapter 18)

Security technologiesFirewalls, WAFs, HSMs, secrets vaults, privileged access, SIEM and SOAR, cloud posture management and DLP, conceptually.3 min read (chapter 19)

ObservabilityMetrics, logs and traces; Prometheus, Grafana and OpenTelemetry; alerting, SLOs, on-call and incident review.3 min read (chapter 20)

Deeper advanced

Machine learning and AIFraud scoring, credit models, assistants and document AI; feature stores, serving, drift, explainability and RBI's emerging expectations.4 min read (chapter 21)

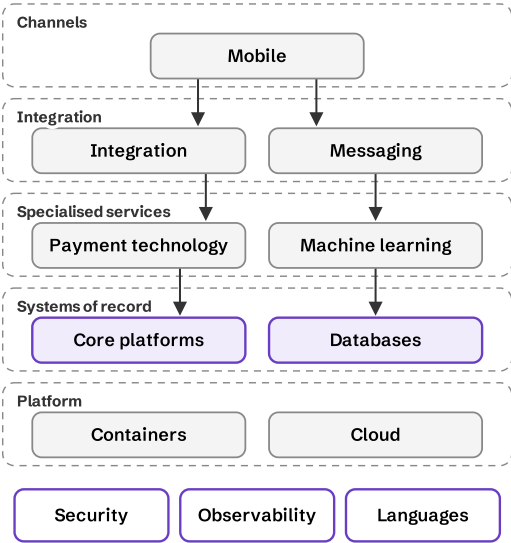
Payment-specific technologyISO 8583 and ISO 20022, SFMS and INFINET, UPI integration, HSMs and PINs, tokenisation, QR codes and card authentication.4 min read (chapter 24)

How to read this section

Each topic starts with a landscape table of the main options and what they are good at, then explains how to choose, the trade-offs and the common pitfalls, and ends with questions for a design review. Product names appear as plain text for reference only; the site does not recommend vendors. Indian users of a product are named only where a public source confirms it.

How the topics fit together

Where each technology sits



Each box is a topic in this section, placed by the layer it mostly serves. Languages and security run through every layer.

Chapter 13

Core banking platforms

Bank ledgers run on established commercial platforms and newer cloud-native cores. They differ in architecture, deployment and database. Choosing one is a decade-long commitment.

Part III begins with the products behind the ledger: the commercial and cloud-native core platforms banks choose between.

Why it matters

The core platform is usually a bank’s largest single technology decision. It sets the product catalogue the bank can offer, how quickly it can change, which skills it needs and which vendor it depends on for the next decade or more. Core banking system architecture (chapter 4) explains what a core does; this page covers the products.

The landscape

Core banking platforms

Platform	Maker	Architecture	Indian users named in public sources
TCS BaNCS	Tata Consultancy Services	Established commercial suite; deposits, lending, payments and more	State Bank of India (see sources)
Finacle	EdgeVerve Systems, a wholly owned Infosys subsidiary	Established commercial suite, now offered in modular, componentised form	None confirmed yet on this site
Oracle FLEXCUBE	Oracle	Established commercial suite, closely tied to the Oracle database	None confirmed yet on this site
Temenos Transact	Temenos	Established commercial suite, widely used outside India	None confirmed yet on this site
Mambu	Mambu	Cloud-native, delivered as software as a service	None confirmed yet on this site
Thought Machine Vault	Thought Machine	Cloud-native core where products are defined as code	None confirmed yet on this site
Shared community platforms	Various	One hosted core serving many smaller banks	See the note on shared platforms below

Product names are for reference only. The site does not recommend vendors. Customers are named only where a public source confirms them. Sources^{1 2}

SBI’s core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years.¹ Finacle is developed by EdgeVerve Systems, a wholly owned subsidiary of Infosys, and marketed as Infosys Finacle.² The vendor states that banks in over 100 countries use Finacle to serve more than a billion consumers and 1.3 billion accounts.²

Deployment models

A common pattern is for a large bank to run its core on-premises, in its own data centres, with a disaster-recovery site. Some platforms are also offered hosted by the vendor or a partner, or as software as a service. Smaller banks often share a platform. IFTAS’s Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.⁴ Any arrangement where a third party runs the core brings RBI’s outsourcing rules into play: RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023.⁵

Database dependence

Established cores were built on large commercial relational databases, and their performance, licensing and skills needs follow from that choice. Some vendors now support open-source databases for parts of the platform. EDB stated in 2019 that multiple Finacle modules had been migrated to EDB Postgres and implemented at financial institutions in Asia.³

How to choose

Banks usually weigh six things:

- **Functional fit:** the products the bank sells today and expects to sell, including Indian requirements such as priority-sector tagging, regulatory returns and connections to Indian payment rails.
- **Architecture:** whether the platform can run modules independently, expose APIs and cope with round-the-clock payments without long batch windows.
- **Proven scale:** reference customers of a similar size, checked directly rather than taken from brochures.
- **Total cost:** licences, hardware, database, implementation partner, upgrades and the in-house team, over ten years rather than one.
- **Skills and partners:** how many people in the Indian market know the platform, and how many implementation partners support it.
- **Exit:** how data would be extracted and moved if the relationship ended.

Trade-offs

Platform choices

Choice	You gain	You give up
Established commercial suite	Breadth of products, reference customers, local skills	Heavy customisation, long upgrade cycles, vendor dependence
Cloud-native core	Faster product change, modern APIs, elastic scale	Fewer large local references; cloud and outsourcing obligations
Shared community platform	Low cost and managed operations for a small bank	Little control over roadmap and change timing
Heavy customisation	An exact fit to current products	Every future upgrade becomes a project

Pitfalls

- **Customising instead of configuring.** Code changes to the vendor's product make every later upgrade slower and riskier.
- **Buying for the demo.** A platform chosen on user-interface screens rather than on batch performance, APIs and data model disappoints later.
- **Underestimating data migration,** which is usually the longest and riskiest part of the programme.
- **Ignoring the database bill.** Database licences and specialist skills can rival the platform's own cost.
- **No exit plan,** leaving the bank unable to leave even when the relationship is failing.

Questions to ask a vendor

- Which banks of our size run this version today, and can we speak to them without you present?
- How long does end of day take at our projected volumes, and what runs during it?
- Which functions are exposed as APIs, and which only through screens or files?
- How is a new product launched: configuration, scripting or code change?
- How do we extract all our data, in what format, if we leave?

Notes

1. **SBI deepens partnership with TCS to drive innovation and enhance customer experience** <https://tcs.com/who-we-are/newsroom/press-release/sbi-deepens-partnership-with-tcs-drive-innovation-enhance-customer-experience>. Tata Consultancy Services. **Vendor**, accessed 29 September 2026.
Supports: SBI's core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years (as of 6 October 2021).
2. **EdgeVerve Systems Positioned a Leader by Gartner for the Finacle Core Banking Solution** <https://www.edgeverve.com/finacle/news/edgeverve-positioned-gartner-for-finacle-solution/>. EdgeVerve Systems. **Vendor**, accessed 29 September 2026.
Supports: Finacle is developed by EdgeVerve Systems, a wholly owned subsidiary of Infosys, and marketed as Infosys Finacle (as of 31 August 2020); The vendor states that banks in over 100 countries use Finacle to serve more than a billion consumers and 1.3 billion accounts (as of 31 August 2020).
3. **Infosys Finacle Names EnterpriseDB Open Source DB Partner of the Year** <https://www.enterprisedb.com/blog/infosys-finacle-names-enterprisedb-open-source-db-partner-year>. EDB. **Vendor**, accessed 29 September 2026.
Supports: EDB stated in 2019 that multiple Finacle modules had been migrated to EDB Postgres and implemented at financial institutions in Asia (as of 11 April 2019).
4. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services (as of 20 September 2022).
5. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023 (as of 10 April 2023).

Chapter 14

Databases

Money needs databases that never lose a confirmed write and never let two transactions spend the same balance. Relational engines hold the ledgers. Caches and other stores take load off them.

Every core and payment system rests on a database. This chapter covers what money needs from one.

Why it matters

A bank's database is where money actually lives. If it loses a confirmed transaction, or lets two withdrawals both succeed against a balance that covers only one, the error is real money. Most other design choices in a bank can be revisited. The database behind the ledger rarely can.

What money needs from a database

The four properties known as **ACID** matter most:

- **Atomicity:** a transfer's debit and credit both happen or neither does.
- **Consistency:** rules such as "balance may not go below the overdraft limit" always hold.
- **Isolation:** concurrent transactions do not see each other's half-finished work.
- **Durability:** once confirmed, a transaction survives a crash.

Relational databases were built for exactly this, which is why ledgers run on them.

The landscape

Database types in banking

Technology	Role	Typical use in Indian banking	Notes
Commercial relational (for example Oracle Database, IBM Db2, Microsoft SQL Server)	System of record	Core ledgers, payment systems, loan systems	Mature clustering and tooling; significant licence cost
Open-source relational (PostgreSQL and its enterprise distributions)	System of record or supporting system	Newer applications, channel back ends, some core modules	Lower licence cost; enterprise support available
Distributed SQL (for example CockroachDB, YugabyteDB)	Relational data spread across nodes	New systems that need scale across sites	Strong consistency across nodes, at the cost of write latency
In-memory cache (Redis and similar)	Fast reads of data held elsewhere	Session data, reference data, rate limiting, balance snapshots for display	Not a system of record; data can be lost
Document stores (for example MongoDB)	Flexible, nested records	Customer profiles, onboarding journeys, content	Check the transaction guarantees before using for money
Key-value and wide-column stores	Very high write and read volumes	Event histories, logs, device and fraud features	Usually eventual consistency

Typical uses are general industry patterns, not claims about named banks. Product names are examples only.

Vendors have also moved established banking software onto open-source relational databases. EDB stated in 2019 that multiple Finacle modules had been migrated to EDB Postgres and implemented at financial institutions in Asia.¹

Clustering and replication

A single database server is a single point of failure. **Clustering** runs several servers so that one can take over from another. **Replication** copies data to other servers or sites, synchronously (no loss, slower writes) or asynchronously (faster, small possible loss). RBI expects critical systems to aim for no loss at all: For critical information systems, regulated entities should prioritise a minimal RTO, approved by their IT Strategy Committee, and a near-zero RPO; with a non-zero RPO they need a documented method for reconciling data when resuming from the alternate site.² Replication is not a backup, though: a deleted table is deleted everywhere. Regulated entities must back up data and periodically restore it to check that it is usable.²

How to choose

Start from the consistency the data needs, not from the technology. Balances, postings and anything else that must never be wrong belong in a relational database with full transactions. Data that is read far more than written, such as reference data or a customer's recent transactions for an app screen, can be cached. Data whose shape changes often and which does not move money, such as onboarding forms, can suit a document store. High-volume append-only data, such as events and logs, suits stores built for writes.

Trade-offs

Database choices

Choice	You gain	You give up
One large relational database	Simple strong consistency	Scale limited to the biggest machine; costly failover
Distributed SQL	Scale and resilience across nodes	Higher write latency; newer operational skills
Cache in front of the database	Fast reads and less load on the core	Stale data risk; another system to keep consistent
Open-source engine	Lower licence cost, no single vendor	Support contracts and in-house skills still needed

Pitfalls

- **Treating a cache as the truth**, for example approving a payment against a cached balance.
- **Assuming replication is a backup**. Mistakes replicate too.
- **Choosing a store for its speed** and discovering later that it cannot run a multi-record transaction.
- **Migrating engines without checking behaviour**, such as differences in how dates, rounding or locking work.
- **Long-running reports on the ledger database**, slowing customer transactions.

Questions for a design review

- Which data here must never be wrong, and which store holds it?
- What isolation level do money-moving transactions run at?
- If the primary database fails now, how much data is lost and who reconciles it?
- When was a backup last restored and checked?
- Which reads could move to a cache or replica, and how stale may they be?

Notes

1. **Infosys Finacle Names EnterpriseDB Open Source DB Partner of the Year** <https://www.enterprisedb.com/blog/infosys-fincle-names-enterprisedb-open-source-db-partner-year>. EDB. **Vendor**, accessed 29 September 2026.
Supports: EDB stated in 2019 that multiple Finacle modules had been migrated to EDB Postgres and implemented at financial institutions in Asia (as of 11 April 2019).
2. **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text)** <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: For critical information systems, regulated entities should prioritise a minimal RTO, approved by their IT Strategy Committee, and a near-zero RPO; with a non-zero RPO they need a documented method for reconciling data when resuming from the alternate site (as of 7 November 2023); Regulated entities must back up data and periodically restore it to check that it is usable (as of 7 November 2023).

Chapter 15

Messaging and streaming

Messaging moves work between systems without making them wait for each other. Queues hand each message to one consumer; logs keep an ordered record many can replay. Banks use both.

Between databases and services, messages move the work. This chapter compares queues and logs.

Why it matters

Banks connect hundreds of systems. Calling each one directly and waiting for an answer makes every system as slow and as fragile as the slowest one it calls. Messaging lets a system hand off work and carry on, while another system picks it up when it can. It is how banks absorb peaks, decouple teams and feed real-time fraud and analytics.

Queues and logs

A **queue** holds messages until a consumer takes them, and each message goes to one consumer. It suits distributing work: “send this SMS”, “generate this statement”. A **log** keeps messages in order for a set time, and any number of consumers read it at their own pace, each keeping its own position. It suits event streams, audit trails and feeding several systems from one source. Event-driven architecture (chapter 7) covers the design patterns.

The landscape

Messaging and streaming technologies

Technology	Model	Typical use in Indian banking	Watch out for
Apache Kafka (and managed or compatible services)	Partitioned, replicated log	Event streams, change data capture, feeding fraud and analytics	Operational complexity; ordering holds only within a partition
RabbitMQ	Broker with queues and flexible routing	Task distribution between services	Throughput ceilings at very high volumes
IBM MQ	Enterprise queue manager with transactions	Messaging with mainframes and older cores	Licence cost and specialist skills
Cloud messaging services	Managed queues and streams	Cloud-hosted channels and analytics	Data residency and outsourcing obligations
Apache Flink	Stateful stream processing	Real-time fraud features, running totals, alerts	State management and upgrades need care
Spark Structured Streaming	Micro-batch stream processing	Near-real-time analytics and data pipelines	Latency of seconds rather than milliseconds

Typical uses are general industry patterns, not claims about named banks. Product names are for reference only.

How to choose

Ask three questions. **Does more than one system need the same message?** If so, a log. **Must messages stay in order?** If so, which ones: usually all messages for one account or one payment, which a partitioned log can keep together. **How long must messages be kept?** A queue deletes a message once handled; a log can keep days or weeks, so a new consumer or a fixed bug can replay history.

Scale matters too. The UPI system alone averages 791 million a day¹, so a bank’s messaging layer must absorb peaks without back-pressure reaching customers.

Handling repeats safely

Almost every messaging system can deliver a message more than once, for example after a timeout and retry. For money, a repeated message must never move money twice. The usual answer is an idempotent consumer: it records each message’s unique key and ignores keys it has already processed.

An idempotent consumer (illustrative)

```
async function handle(msg: PaymentMessage) {
  // The key comes from the sender and is the same on every retry.
  const seen = await db.processed.find(msg.idempotencyKey);
  if (seen) return seen.result; // already done: return the same answer

  return db.transaction(async (tx) => {
    const result = await postToLedger(tx, msg);
    await tx.processed.insert({ key: msg.idempotencyKey, result });
    return result;
  });
}
```

Exactly-once has limits

Products that promise exactly-once delivery keep that promise inside their own boundary. The moment a message causes a change in another system, such as a core ledger, the application still needs its own idempotency check.

Trade-offs

Messaging choices

Choice	You gain	You give up
Queue	Simple work distribution; message gone once handled	No replay; one consumer per message
Log	Many consumers, replay and history	Retention to manage; ordering only per partition
Managed cloud service	No cluster to run	Provider dependence, residency and outsourcing rules
Self-run cluster	Full control on-premises	Specialist operations team

Pitfalls

- **Assuming exactly-once delivery** and skipping idempotency checks.
- **Hot partitions**, where one busy key, such as a large merchant, overloads a single partition.
- **Unbounded retries** that hammer a failing system; use back-off and a dead-letter queue for messages that keep failing.
- **Silent consumer lag** with no alert.
- **Changing message formats** without versioning, breaking consumers.

Questions for a design review

- What is the key for each message, and does every consumer check it?
- Which messages must stay in order, and what partition key guarantees that?
- Where do messages go after repeated failure, and who looks at them?
- How far can each consumer fall behind before an alert fires?
- How long are messages kept, and does that respect data retention rules?

Notes

- 1. UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.
Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).

Chapter 16

Middleware and integration

Integration technology connects a bank's systems and translates between their formats. Service buses, API gateways and service meshes overlap. Using each where it fits avoids a tangle.

Messaging is one way to connect systems. This chapter covers the others: service buses, gateways and service meshes.

Why it matters

A bank runs a core, card systems, loan systems, payment hubs, channels, fraud engines, data platforms and dozens of third-party connections. Each speaks its own language: fixed-width files, SOAP web services, REST APIs, ISO payment messages. Integration technology is what lets them work together. Done well, it hides that variety. Done badly, it becomes the least-understood and most fragile part of the estate.

Three families

An **enterprise service bus (ESB)** is central middleware that routes, transforms and orchestrates messages between applications. Many banks introduced one to replace point-to-point links with a hub. Its risk is that business logic accumulates inside it.

An **API gateway** is a front door for APIs. It handles identity, rate limits, validation and logging, and passes requests to the services behind it. It should route and protect, not hold business logic. See API-first and open banking (chapter 6).

A **service mesh** manages traffic between services inside a platform, usually containers. It adds mutual TLS, retries, time-outs and telemetry to every service-to-service call without changing the services' code.

The landscape

Integration technologies

Technology	Family	Typical use in Indian banking	Notes
IBM App Connect, TIBCO, Oracle SOA Suite	Enterprise service bus and integration suites	Connecting cores, card systems and older applications	Mature; often the oldest integration layer in a bank
MuleSoft Anypoint	API-led integration platform	Exposing core functions as APIs; partner integration	Commercial licensing
WSO2	Open-source API management and integration	API gateways and integration, on-premises or cloud	Open-source core with commercial support
Kong, Apigee, cloud API gateways	API gateway	Channel and partner APIs	Choose by where APIs run and how they are governed
Envoy, Istio, Linkerd	Proxy and service mesh	Traffic between microservices on container platforms	Operational complexity; best on mature platforms
File transfer (managed SFTP and similar)	Batch integration	Bulk files such as NACH, statements and regulatory extracts	Still essential; secure and monitor it like any interface

Typical uses are general industry patterns, not claims about named banks. Product names are for reference only.

Protocols and formats

- **SOAP and XML** are common in older enterprise systems, with strict contracts.
- **REST and JSON** are the default for new APIs: simple, widely understood, easy to test.
- **gRPC** uses compact binary messages and suits fast internal service-to-service calls.

- **ISO payment messages**, ISO 8583 for cards and ISO 20022 for richer payment data, need specialist parsers and validation.
- **Flat files** remain the backbone of batch processing.

Much of an integration layer's work is **protocol translation**: accepting a REST call from an app and turning it into the SOAP call or file the core understands, then translating the answer back. Shared specifications reduce this work. For example, in the Account Aggregator framework Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT.¹

How to choose

Use a gateway for anything exposed to channels or partners. Use a service mesh only when many services on one platform need consistent security and traffic control, and the team can run it. Keep an ESB or integration suite for connecting systems that cannot speak modern APIs, and resist adding new business logic to it. For every interface, decide whether it must be synchronous (the caller waits) or can be asynchronous (a message on a queue or log); many can be asynchronous, which makes them more resilient.

Trade-offs

Integration choices

Choice	You gain	You give up
Central ESB	One place to connect and monitor	A bottleneck and a single point of failure; logic hides inside it
API gateway plus services	Clear contracts; logic stays in services	More services to build and run
Service mesh	Uniform security and telemetry between services	A complex platform component to operate
Point-to-point links	Quick for one connection	Unmanageable as connections multiply

Pitfalls

- **The smart pipe**. Business rules added to the ESB or gateway, where nobody can test them properly.
- **Chained synchronous calls**, where one request waits on five others and fails if any of them is slow.
- **No time-outs**, so a slow downstream system ties up every thread upstream.
- **Unmonitored file transfers** that fail quietly at night.
- **Undocumented transformations**, so nobody knows how a field in one system maps to another.

Questions for a design review

- Where does each business rule live, and is any of it in the integration layer?
- Which calls could be asynchronous instead of waiting for an answer?
- What are the time-out and retry settings for each downstream call?
- How is a failed file transfer detected, and by whom?
- Is every field mapping documented and tested?

Notes

1. Consultation paper on Financial Information Users in the securities markets under the Account Aggregator framework https://www.sebi.gov.in/sebi_data/attachdocs/aug-2023/1690887848711.pdf. Securities and Exchange Board of India. **Primary source**, accessed 29 September 2026. Supports: Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT (as of 1 August 2023).

Chapter 17

Containers and orchestration

Containers package an application with everything it needs to run. Kubernetes runs them at scale; GitOps and infrastructure as code keep them reproducible. Regulated workloads add controls.

The services described so far increasingly run in containers. This chapter covers the platforms that run them, and what regulated workloads add.

Why it matters

Banks now build many of their channel, payment and integration services as small applications that change often. Containers let each one be packaged once and run the same way on a laptop, in testing and in production. An orchestration platform then runs hundreds of them, restarts failures, scales with load and rolls out changes gradually. For a bank, the prize is faster, safer change; the cost is a platform that must itself be run to a very high standard.

The landscape

Container and platform technologies

Technology	Role	Typical use in Indian banking	Notes
Kubernetes (upstream, or distributions such as OpenShift and Rancher)	Container orchestration	Running microservices for channels, payments and APIs	The standard; distributions add support and security defaults
Managed Kubernetes (EKS, AKS, GKE, OKE)	Kubernetes run by a cloud provider	Cloud-hosted channel and analytics services	Cloud outsourcing and residency rules apply
Helm	Packaging for Kubernetes applications	Versioned, repeatable deployments	Keep charts simple and reviewed
Argo CD, Flux	GitOps delivery	Keeping clusters matched to what is in Git	Every change becomes a reviewed commit
Terraform, OpenTofu	Infrastructure as code	Networks, clusters and cloud resources defined in code	Protect the state file; review plans before applying
Temporal, Camunda	Workflow and orchestration engines	Long-running processes such as onboarding or loan origination	Durable state for multi-step processes

Typical uses are general industry patterns, not claims about named banks. Product names are for reference only.

GitOps and infrastructure as code

Infrastructure as code defines servers, networks and clusters in files kept in version control, so an environment can be rebuilt exactly. **GitOps** extends that to applications: the Git repository holds the desired state of every cluster, and an agent keeps the live cluster matched to it. Every change is a reviewed commit with an author and a timestamp, which is also an audit trail.

This matters for resilience. RBI expects the primary and DR sites to match: Configurations and security patches must be identical at the primary data centre and the DR site.¹ Defining both sites from the same code is the most reliable way to keep them identical.

What regulated workloads add

- **Separation:** production isolated from development and testing, with separate clusters or strictly controlled namespaces.

- **Image control:** only images built by the bank's pipeline, scanned for vulnerabilities and signed, may run in production.
- **Policy enforcement:** admission rules that block privileged containers, missing resource limits or unapproved registries.
- **Secrets:** credentials supplied at run time from a vault, never baked into images.
- **Evidence:** logs of who deployed what, when, and with which approval.
- **Outsourcing:** where a provider runs the platform, RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023.²

How to choose

Start with a supported distribution or a managed service rather than assembling upstream Kubernetes by hand, unless the bank has a strong platform team. Standardise on one deployment method, usually GitOps, across all teams. Move stateless services first; keep databases and other stateful systems on proven infrastructure until the platform has shown it can run them reliably.

Trade-offs

Platform choices

Choice	You gain	You give up
Self-run Kubernetes	Full control, on-premises	A skilled platform team, and upgrades every few months
Managed Kubernetes in the cloud	The provider runs the control plane	Outsourcing and residency obligations
GitOps for every change	Reproducible environments and an audit trail	Discipline: no manual fixes in production
Workflow engine	Reliable long-running processes	Another stateful system to operate

Pitfalls

- **Treating the platform as a project**, not a product that needs a permanent team.
- **Manual changes in production** that drift from what Git says.
- **Stateful systems moved too early**, before backup, failover and upgrades are proven.
- **Missing resource limits**, so one service starves others on the same nodes.
- **Unpatched base images** carrying known vulnerabilities into production.

Questions for a design review

- Can this environment be rebuilt from code alone, and when was that last done?
- Which images may run in production, and how is that enforced?
- Where do this service's secrets come from?
- Are the primary and DR clusters defined from the same code?
- Who owns the platform, and how are its upgrades scheduled and tested?

Notes

1. **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text)** <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Configurations and security patches must be identical at the primary data centre and the DR site (as of 7 November 2023).

2. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023 (as of 10 April 2023).

Chapter 18

Cloud platforms

The main cloud providers all run regions in India, so banks can keep data in the country. For a bank, cloud use is outsourcing, with rules on data, security and exit. Providers differ mostly in fit.

Container platforms often run in the cloud. This chapter covers the providers and the rules that shape their use in Indian banking.

Why it matters

Cloud platforms give banks capacity on demand, managed databases and analytics, and environments that can be created in minutes. Whether and how a bank uses them is shaped less by technology than by rules: where data may live, what counts as outsourcing and how the bank would leave. Hybrid and multi-cloud deployment (chapter 12) covers the architecture; this page covers the providers and constraints.

The landscape

Major cloud providers

Provider	Regions in India (see sources)	Typical use in Indian banking	Notes
Amazon Web Services	Mumbai, Hyderabad	Channel back ends, analytics, development and testing	Broadest service catalogue
Microsoft Azure	Pune, Chennai, Mumbai	Workloads tied to Microsoft software and identity	Strong hybrid and identity tooling
Google Cloud	Mumbai, Delhi NCR	Data analytics and machine learning	Strong data and analytics services
Oracle Cloud Infrastructure	Mumbai, Hyderabad	Oracle database and application workloads	Natural home for Oracle-based systems
Indian data-centre and cloud operators	Various Indian cities	Private and community cloud, colocation	Local contracts and support

Typical uses are general patterns, not claims about named banks. Region lists change; confirm on each provider's region page. Sources ¹

As of 2026, AWS runs cloud regions in Mumbai and Hyderabad, Microsoft Azure in Pune, Chennai and Mumbai, Google Cloud in Mumbai and Delhi NCR, and Oracle Cloud in Mumbai and Hyderabad. ¹ Having more than one region in the country lets a bank run a primary and a disaster-recovery site without moving data abroad.

The regulatory frame

Three rules shape almost every cloud decision:

- **Data residency.** RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad. ²
- **Outsourcing.** RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud. ³ RBI's Direction describes cloud security as a shared responsibility between the regulated entity and the cloud service provider. ³
- **Exit.** A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement. ³

Sovereign and community cloud

Some workloads are better served by cloud infrastructure dedicated to a sector or a country. A **community cloud** is shared among a defined group, such as banks of one type. IFTAS’s Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.⁴ A **sovereign cloud** is operated so that data, operations and control stay within one jurisdiction. Both trade some of the public cloud’s breadth for tighter control.

How to choose

Most banks choose a provider per workload rather than for the whole estate. The deciding factors are usually:

- the software the workload already depends on;
- the services it needs, such as a managed database, analytics or AI;
- the availability of two regions in India for resilience;
- the bank’s existing skills and contracts;
- how easily the workload could move elsewhere.

Start with workloads that benefit most and carry least risk, such as development environments, analytics on masked data and customer-facing channels. Build the controls, contracts and evidence once, then reuse them.

Trade-offs

Cloud choices

Choice	You gain	You give up
Public cloud region in India	Elastic capacity and managed services, data in India	Outsourcing obligations and provider dependence
Provider-specific managed services	Speed and less to operate	Harder exit
Portable, open technologies on cloud	Easier exit	More to run yourself
Community or sovereign cloud	Tighter control and sector fit	Fewer services and less scale

Pitfalls

- **Assuming the provider handles security.** Configuration, identity and data protection remain the bank’s job.
- **Data leaving India unnoticed,** through backups, logs, support access or a global service.
- **Lock-in by convenience,** when a workload uses so many provider-specific services that it cannot move.
- **Cost surprises** from idle resources and data transfer.
- **An exit plan written only for the auditor.**

Questions for a design review

- In which regions will this workload’s data, backups and logs reside?
- Which controls does the bank own, and which does the provider?
- What provider-specific services does this workload use, and what would replace them on exit?
- Has the outsourcing assessment been completed and approved?
- Who owns the running cost, and how is it reviewed?

Notes

1. **Cloud Infrastructure Map** <https://www.cloudinfrastructuremap.com/>. Cloud Infrastructure Map. **Analyst**, accessed 29 September 2026.
Supports: As of 2026, AWS runs cloud regions in Mumbai and Hyderabad, Microsoft Azure in Pune, Chennai and Mumbai, Google Cloud in Mumbai and Delhi NCR, and Oracle Cloud in Mumbai and Hyderabad (as of 29 September 2026).
2. **Storage of Payment System Data (RBI/2017-18/153)** <https://rbi.org.in/scripts/NotificationUser.aspx?Id=11244>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad (as of 6 April 2018).
3. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?Id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud (as of 10 April 2023); RBI's Direction describes cloud security as a shared responsibility between the regulated entity and the cloud service provider (as of 10 April 2023); A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement (as of 10 April 2023).
4. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services (as of 20 September 2022).

Chapter 19

Security technologies

Bank security uses a stack of tools, each covering a different way in. Firewalls filter traffic, HSMs guard keys, vaults and PAM guard credentials, SIEM watches it all. Tools help only if run well.

The architecture of security was covered in Part II. This chapter surveys the tools that implement it.

Why it matters

No single product makes a bank secure. Each tool covers a different way an attacker could get in or a different stage of an attack: preventing, detecting or responding. Security architecture (chapter 10) explains how the layers fit together; this page describes the technology families.

This page is conceptual. It does not describe any organisation’s tools or configuration.

The landscape

Security technology families

Technology	What it does	Where it sits	Notes
Next-generation firewall	Filters network traffic by application, user and threat, not just address and port	Between network zones and at the perimeter	Rules need regular review; old rules pile up
Web application firewall (WAF)	Blocks common attacks on web traffic, such as injection	In front of websites and APIs	Tune it to the application, or it blocks customers
DDoS protection	Absorbs floods of traffic meant to take a service down	At the network edge, often a provider service	Test it before an attack does
Hardware security module (HSM)	Stores keys and performs cryptography without revealing keys	Payment, card and signing systems	Keys never leave the device in clear
Secrets vault	Issues and rotates passwords, keys and certificates at run time	Used by applications and pipelines	Removes secrets from code and configuration
Privileged access management (PAM)	Controls and records administrator access, ideally just in time	Between administrators and systems	Standing admin rights are the thing to eliminate
SIEM	Collects logs and raises alerts on suspicious patterns	Central, fed by every system	Only as good as the logs and the people reading alerts
SOAR	Automates responses to alerts	Alongside the SIEM	Automate the routine; keep people for judgement
Cloud security posture management (CSPM)	Finds risky settings in cloud accounts	Across cloud accounts	Catches exposed storage and open network rules
Data loss prevention (DLP)	Detects and blocks sensitive data leaving	Email, web, endpoints and cloud storage	Needs well-labelled data to work

Families, not products. Product choices depend on each bank’s estate.

Where banking adds requirements

- **Cards and keys.** Card numbers are replaced by tokens wherever possible, shrinking what must be protected: Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead.³ PINs and keys are handled inside HSMs.
- **Customer authentication.** RBI’s Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026.⁵

- **Digital certificates.** IDBRT is the certifying authority for digital certificates in the Indian banking and financial sector under the IT Act, 2000.⁴
- **Reporting clocks.** Detection tools must feed a process fast enough to meet deadlines. CERT-In's directions of 28 April 2022 under section 70B(6) of the IT Act require reportable cyber incidents to be reported to CERT-In within 6 hours of noticing them; they took effect 60 days after issue.¹ A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them.²

How to choose

Choose by the risk each tool reduces, in order of what would hurt most: money movement, keys, customer data and administrator access. Prefer fewer tools that are well integrated and fully used over many that are partly deployed. For each tool, decide in advance who owns it, who reads its alerts and what happens when it fires.

Trade-offs

Security technology choices

Choice	You gain	You give up
Best-of-breed tools	The strongest capability in each area	Integration work and more consoles to watch
One platform suite	Integration and a single view	Dependence on one vendor; weaker in some areas
Managed security service	Round-the-clock monitoring without building a team	Outsourcing obligations; less in-house knowledge
Strict blocking by default	Fewer successful attacks	More false positives affecting customers and staff

Pitfalls

- **Shelfware:** tools bought, partly installed and never tuned.
- **Alert fatigue,** where so many alerts fire that real ones are missed.
- **Blind spots,** such as cloud accounts, supplier connections or new services not sending logs.
- **Firewall rule sprawl,** with thousands of rules nobody can explain.
- **Secrets outside the vault,** in scripts, tickets or chat.

Questions for a design review

- Which risk does each security tool here reduce, and who owns it?
- Does every system, including cloud and supplier connections, send logs to the SIEM?
- Who reads alerts at 3 a.m., and how fast can an incident reach the reporting deadline?
- Which administrator accounts have standing access, and why?
- Where are this system's secrets, and when were they last rotated?

Notes

1. Directions under sub-section (6) of section 70B of the IT Act, 2000 (28 April 2022) https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf. CERT-In, Ministry of Electronics and Information Technology. **Primary source**, accessed 29 September 2026.

Supports: CERT-In's directions of 28 April 2022 under section 70B(6) of the IT Act require reportable cyber incidents to be reported to CERT-In within 6 hours of noticing them; they took effect 60 days after issue (as of 28 April 2022).

2. Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102) https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them (as of 10 April 2023).

3. Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)] (RBI/2022-2023/95) <https://website.rbi.org.in/web/rbi/-/notifications/restriction-on-storage-of-actual-card-data-i.e.-card-on-file-cof-12363>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead (as of 28 July 2022).

4. **About IDRBT** <https://www.idrbt.ac.in/about-idrbt>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.

Supports: IDRBT is the certifying authority for digital certificates in the Indian banking and financial sector under the IT Act, 2000 (as of 1 January 2025).

5. **RBI unveils new directions to strengthen digital payment security** <https://www.tribuneindia.com/news/business/rbi-unveils-new-directions-to-strengthen-digital-payment-security>. The Tribune. **Reported**, accessed 29 September 2026.

Supports: RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026 (as of 25 September 2025).

Chapter 20

Observability

Observability lets teams see what their systems are doing and why. Metrics, logs and traces answer different questions. Service level objectives turn that data into decisions about reliability.

Systems that cannot be seen cannot be run. This chapter covers the metrics, logs and traces that make them visible.

Why it matters

A payment passes through an app, a gateway, several services, a payment switch and a core. When customers report failures, the team must find which step is failing, for whom and since when, in minutes. Observability is the ability to answer those questions from the data systems emit, without guessing or adding code during the incident.

Three kinds of signal

Metrics are numbers over time: requests per second, error rate, response time, queue depth. They are cheap to store and ideal for dashboards and alerts. **Logs** are records of individual events, with detail about what happened. They are essential for investigation and audit, but costly at volume. **Traces** follow one request across every service it touches, showing where time was spent and where it failed. Together they answer “is something wrong?”, “what happened?” and “where?”.

The landscape

Observability technologies

Technology	Role	Typical use in Indian banking	Notes
Prometheus	Metrics collection and alerting rules	Metrics from container platforms and services	The standard for Kubernetes metrics
Grafana	Dashboards across many data sources	Operations and business dashboards	Works with metrics, logs and traces
OpenTelemetry	Vendor-neutral standard and libraries for emitting signals	Instrumenting services once, sending anywhere	Avoids lock-in to one monitoring vendor
Elasticsearch or OpenSearch, Loki, Splunk	Log storage and search	Application and security logs	Plan retention and cost carefully
Jaeger, Tempo	Distributed tracing back ends	Following requests across microservices	Needs trace IDs passed through every hop
Commercial observability suites	All signals in one managed product	Teams that prefer a managed service	Check where data is stored and processed

Typical uses are general industry patterns, not claims about named banks. Product names are for reference only.

From data to decisions: SLOs

A **service level indicator** (SLI) is a measure of what users experience, such as the share of payments that succeed within two seconds. A **service level objective** (SLO) is the target for it, such as 99.9% over 30 days. The gap between the target and perfection is the **error budget**: while it lasts, the team can ship changes; when it runs out, reliability work comes first.

Scale makes these measures essential. With UPI alone averaging 791 million a day¹, a success rate that looks excellent as a percentage can still mean many failed payments. Failures also have regulatory clocks attached: RBI’s framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint.²

Alerting, on-call and incident review

Good alerts fire on symptoms users would notice, such as rising payment failures, rather than on every internal blip. Each alert has an owner, a runbook and a clear severity. On-call rotations share the load fairly and include time to recover. After every significant incident, a **blameless review** records what happened, why it made sense to the people involved at the time and what will change. Incident timelines built from good observability data also feed regulatory reporting: A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them.³

How to choose

Instrument once with OpenTelemetry, so the choice of back end can change later. Start with the few SLIs that matter most to customers, such as payment success and response time, and build dashboards and alerts around them before adding more. Decide log retention by need and rule, not by default.

Trade-offs

Observability choices

Choice	You gain	You give up
Open-source stack	Control, no per-host licence	A team to run and scale it
Managed suite	Fast start, less to operate	Cost at volume; data leaves the bank's estate
Log everything	Nothing missing during an investigation	High cost and personal data in logs
Sample traces	Lower cost	The one failing request may not be sampled

Pitfalls

- **Dashboards nobody watches** and alerts nobody owns.
- **Alerting on causes**, such as high CPU, instead of symptoms users feel.
- **Personal data in logs**, such as full account numbers or card details.
- **Broken traces** because one service does not pass the trace ID on.
- **Reviews that assign blame**, which teach people to hide problems.

Questions for a design review

- What are this service's SLIs and SLOs, and who agreed them?
- If payments start failing, which alert fires first, and who receives it?
- Can one payment be traced from the app to the core?
- What personal data could appear in these logs, and how is it masked?
- How long are logs kept, and why that long?

Notes

1. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-ncpi-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.
Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).
2. **Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems (RBI/2019-20/67)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11693>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI's framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint (as of 20 September 2019).
3. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

20 Observability

Supports: A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them (as of 10 April 2023).

Chapter 21

Machine learning and AI

Banks use machine learning for fraud, credit, collections, service and documents. The hard parts are data, monitoring and explaining decisions. RBI's AI and model risk rules are still being settled.

Data and observability feed models. This chapter covers where banks use machine learning, and what the regulator has said so far.

Why it matters

Machine learning now touches many of a bank's most important decisions: whether a payment looks fraudulent, whether a borrower is likely to repay, which customer to call about an overdue loan. Language models add assistants for customers and staff, and tools that read documents. Each can bring speed and consistency. Each can also be wrong at scale, treat groups of customers unfairly or be impossible to explain to a customer or a supervisor.

Where banks use it

Common uses of machine learning in banking

Use	What the model does	Typical technique	Key risk
Fraud scoring	Scores each payment or login for fraud in milliseconds	Gradient-boosted trees, graph features, anomaly detection	Blocking genuine customers; missing new fraud patterns
Credit underwriting	Estimates the chance a borrower repays	Scorecards, gradient-boosted trees	Unfair outcomes; decisions that cannot be explained
Collections	Chooses whom to contact, when and how	Propensity models	Aggressive or unfair treatment of vulnerable customers
Customer and staff assistants	Answers questions and drafts responses	Large language models with retrieval	Wrong answers stated confidently; data leakage
Document AI	Reads forms, statements and identity documents	Optical character recognition plus language models	Extraction errors flowing into decisions

General industry patterns, not claims about named banks.

Some of the data these models use arrives through consent-based channels, such as Account Aggregators: No financial information is retrieved, shared or transferred through an Account Aggregator without the customer's explicit consent, and joining is voluntary.⁵ Shared infrastructure for credit is also emerging: The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai.⁴

The machinery around a model

- **Feature stores** calculate model inputs once and serve the same values for training and for live decisions.
- **Model serving** runs models behind an API with a fixed latency budget. A fraud score that arrives after the payment has completed is useless.
- **Monitoring and drift detection** watch whether live inputs and outcomes still resemble the training data. Fraud patterns and economic conditions change, and models decay.
- **Explainability** produces reasons for a decision, such as the factors that most lowered a credit score. Customers, staff and supervisors can then understand and challenge it.
- **Model inventory and validation** records every model, its owner, purpose, data and last independent review.

RBI's expectations: emerging, not settled

RBI's position on AI and model risk is still developing, and it matters which documents are final:

- An RBI committee's report on responsible AI in finance (FREE-AI), placed on RBI's website on 13 August 2025, sets out 7 guiding principles and 26 recommendations under six pillars.¹
- RBI's draft circular of 5 August 2024 on model risk in credit proposed a board-approved model risk policy, independent validation before deployment, and outcomes that are unbiased, explainable and verifiable.²
- On 24 June 2026 RBI released draft guidance on model risk management across the model lifecycle, including models that use AI and machine learning, for public comment.³

Draft and advisory, as of this page's date

The FREE-AI report is a committee report, and the model risk documents above are drafts released for comment. Treat them as a strong signal of direction, and check for final RBI instruments before treating any recommendation as a rule.

The direction is already clear enough to design for. Keep a model inventory, validate models independently before use and after significant change, monitor them in production, be able to explain decisions that affect customers, and hold the bank accountable for models bought from vendors as well as those built in-house.

Large language models and data protection

Language models raise specific questions: where prompts and outputs are processed and stored, whether customer data could be used to train someone else's model, and how to stop a model revealing information to the wrong user. Common safeguards include hosting models within the bank's controlled environment or an approved region, masking personal data before it reaches the model, retrieving only documents the user is allowed to see, and logging prompts and responses for review.

How to choose

Prefer the simplest model that works, especially where decisions must be explained. Start where errors are cheap to catch, such as staff-facing assistants with human review, before customer-facing or credit decisions. Build the inventory, monitoring and validation process before the second model, not after the tenth.

Pitfalls

- **Training on data the model will not have live**, so it performs well in testing and badly in production.
- **No monitoring after launch**, letting a model decay unnoticed.
- **Proxies for protected characteristics**, such as location standing in for community, producing unfair outcomes.
- **Vendor models treated as black boxes**, although the bank remains accountable for them.
- **Language models given access to data** their users should not see.

Questions for a design review

- Is this model in the inventory, with an owner and a validation date?
- What happens to a customer when the model is wrong, and how can they challenge it?
- How is drift detected, and what triggers retraining or rollback?
- Can the reasons for an individual decision be produced on request?
- Where is data processed when this model runs, and does any of it leave the bank's control?

Notes

1. **Report of the Committee to develop a Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) in the Financial Sector (press release)** <https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR902F828551DA4B54AFDA44180762D51FFCD.PDF>, Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: An RBI committee's report on responsible AI in finance (FREE-AI), placed on RBI's website on 13 August 2025, sets out 7 guiding principles and 26 recommendations under six pillars (as of 13 August 2025).

2. **RBI releases draft circular on model risk management in credit for lenders** <https://www.lexology.com/library/detail.aspx?g=2e3e5197a3ec-4b08-9048-8c70dfd82be4>, Lexology. **Analyst**, accessed 29 September 2026.

Supports: RBI's draft circular of 5 August 2024 on model risk in credit proposed a board-approved model risk policy, independent validation before deployment, and outcomes that are unbiased, explainable and verifiable (as of 5 August 2024).

3. **Reserve Bank issues draft Regulatory Principles for Management of Model Risks** https://www.business-standard.com/markets/capital-market-news/reserve-bank-issues-draft-regulatory-principles-for-management-of-model-risks-in-credit-126062500401_1.html, Business Standard. **Reported**, accessed 29 September 2026.

Supports: On 24 June 2026 RBI released draft guidance on model risk management across the model lifecycle, including models that use AI and machine learning, for public comment (as of 25 June 2026).

4. **Reserve Bank Innovation Hub** <https://rbihub.in/>, Reserve Bank Innovation Hub. **Primary source**, accessed 29 September 2026.

Supports: The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai (as of 29 September 2026).

5. **Account Aggregator Framework** <https://financialservices.gov.in/account-aggregator-framework>, Department of Financial Services, Ministry of Finance. **Primary source**, accessed 29 September 2026.

Supports: No financial information is retrieved, shared or transferred through an Account Aggregator without the customer's explicit consent, and joining is voluntary (as of 29 September 2026).

Chapter 22

Mobile technologies

For most customers, the mobile app is the bank. Banks choose native or cross-platform development and must protect the app on devices they do not control. Payment rules shape authentication.

For most customers the phone is the bank. This chapter covers how banking apps are built and protected.

Why it matters

Mobile is where most retail banking and payments now happen. UPI alone processed 24.51 billion transactions¹ in August 2026, almost all of it started on a phone. The app must be fast and simple for customers, and must also hold up against fraud on a device the bank does not own, may be years old and may be compromised.

The landscape

Mobile development approaches

Approach	What it is	Typical use in Indian banking	Notes
Native Android (Kotlin) and iOS (Swift)	Separate apps written for each platform	Flagship retail banking apps	Best performance and platform features; two codebases
Flutter (Dart)	One codebase drawing its own interface on both platforms	New apps and journeys that must ship fast on both	Consistent look; plugins needed for some device features
React Native (TypeScript)	One codebase using native interface components	Apps built by teams with web skills	Large ecosystem; bridge to native code for sensitive parts
Kotlin Multiplatform	Shared business logic in Kotlin; native interfaces on each platform	Sharing rules and networking code while keeping native screens	Growing; interface still built twice
Mobile web and progressive web apps	Browser-based experiences	Low-friction journeys and onboarding	Limited device security features

Typical uses are general patterns, not claims about named banks.

Design systems

A **design system** is a shared library of interface components, patterns and rules: buttons, amount fields, confirmation screens, error messages. For a bank it keeps every journey consistent and accessible, and it makes the security-critical screens, such as payment confirmation, the same everywhere so customers learn to trust them.

Device binding and app security

Device binding ties a customer’s registration to one phone, usually by verifying the SIM and registering the device, so that stolen credentials alone are not enough elsewhere. Common app protections include:

- detecting rooted or jailbroken devices and emulators;
- keeping keys in the phone’s hardware-backed keystore;
- certificate pinning, so the app talks only to the bank’s servers;
- obfuscation and runtime checks against tampering;
- blocking screen capture on sensitive screens;
- detecting overlay attacks, where malware draws a fake screen over the real one.

Authentication rules have recently changed. RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026.² For digital payments other than card-present transactions, at least one authentication factor must be dynamic, that is, unique to the transaction.³ The 2025 authentication framework encourages new authentication factors but does not require banks to stop using SMS-based OTP.⁴ For apps, this opens the way to stronger factors such as device-bound keys and biometrics, used together with a PIN.

SDKs and third-party code

Banking apps embed third-party software development kits (SDKs): payment libraries, identity verification, analytics, crash reporting. Each SDK runs with the app's permissions and can see what the app sees. Banks therefore keep an inventory of every SDK, review what data each collects and where it sends it, and keep them updated.

App stores and updates

Banks do not control when customers update. A security fix can take weeks to reach most users unless the bank sets a **minimum supported version** and asks older apps to update. Changes are usually released in stages, to a small share of users first, with the ability to switch features off remotely if problems appear.

How to choose

Choose native where the app is the bank's primary channel and needs the best performance and device security. Choose a cross-platform framework where speed across both platforms matters more and the team can still write native code for the sensitive parts. Whatever the choice, put the security-critical pieces, such as key storage, device binding and PIN entry, in well-reviewed native code.

Pitfalls

- **Trusting the device.** Treat every check done on the phone as advisory; confirm on the server.
- **Secrets in the app package**, such as API keys, which attackers extract easily.
- **Unreviewed SDKs** collecting customer data.
- **No forced-update path**, leaving old, vulnerable versions in use for years.
- **Inconsistent confirmation screens**, which make fake ones easier to pass off.

Questions for a design review

- What stops stolen credentials being used on another phone?
- Which checks run on the device, and which are confirmed on the server?
- Which SDKs are in the app, and what data does each collect?
- How quickly can a security fix reach 90% of active users?
- Which authentication factors does each payment journey use, and is one of them dynamic?

Notes

1. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: UPI processed 24.51 billion transactions worth ₹29.82 trillion in August 2026, its highest monthly volume to date (as of 31 August 2026).

2. **RBI unveils new directions to strengthen digital payment security** <https://www.tribuneindia.com/news/business/rbi-unveils-new-directions-to-strengthen-digital-payment-security>. The Tribune. **Reported**, accessed 29 September 2026.

Supports: RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026 (as of 25

September 2025).

3. **RBI Authentication Mechanisms for Digital Payment Transactions Directions, 2025** <https://kpmg.com/in/en/insights/2025/12/reserve-bank-of-india-rbi-authentication-mechanisms-for-digital-payment-transactions-directions-2025.html>. KPMG in India. **Analyst**, accessed 29 September 2026.

Supports: For digital payments other than card-present transactions, at least one authentication factor must be dynamic, that is, unique to the transaction (as of 1 December 2025).

4. **RBI issues Directions on Framework on Authentication Mechanisms for Digital Payment Transactions** https://www.business-standard.com/markets/capital-market-news/rbi-issues-directions-on-framework-on-authentication-mechanisms-for-digital-payment-transactions-125092501090_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: The 2025 authentication framework encourages new authentication factors but does not require banks to stop using SMS-based OTP (as of 25 September 2025).

Chapter 23

Programming languages

Banks run on many languages at once, from COBOL on mainframes to Kotlin and Swift in mobile apps. Each fits some jobs better than others. Skills and long-term support matter as much as features.

Behind every system above is code. This chapter looks at the languages banks use, and why.

Why it matters

A bank’s software outlives most of the people who write it. A language chosen today will need to be read, patched and extended in ten or twenty years. The right choice balances what the language is good at with how many people can work in it, how stable its ecosystem is and how well its tools support security and correctness.

The landscape

Languages in banking

Language	Where it fits	Why	Watch out for
Java	Core platforms, payment systems, back-end services	Mature, fast, huge ecosystem and talent pool; strong for long-lived systems	Framework complexity and slow start-up in some styles
Kotlin	Android apps; increasingly back-end services	Runs on the Java platform with safer, more concise code	Smaller back-end talent pool than Java
Go	Infrastructure, gateways, high-concurrency services	Simple, fast, small binaries, good for network services	Fewer libraries for complex business domains
Python	Data engineering, analytics, machine learning	The standard for data science and ML libraries	Slower for heavy transaction processing; dependency management
TypeScript	Web front ends, backend-for-frontend services	Type safety on top of JavaScript; one language across web and server	Fast-moving ecosystem; supply-chain risk in packages
Swift	iOS apps	The platform language for Apple devices	Apple platforms only
Dart	Cross-platform apps with Flutter	One codebase for Android and iOS	Tied closely to Flutter
C and C++	Low-level components, HSM integrations, performance-critical code	Speed and control	Memory-safety bugs; needs expert review
COBOL	Legacy mainframe cores and batch jobs	Decades of proven business logic still running	Shrinking skills pool; hard to change
SQL and stored procedure languages	Logic inside databases, especially in older cores	Close to the data and fast	Business rules hidden in the database, hard to test

General patterns across the industry, not claims about named banks.

Choosing a language for a new system

Four questions settle most choices:

- **What does the system do?** Transaction processing favours Java or Kotlin; in infrastructure favours Go; data and models favour Python; interfaces favour TypeScript, Swift, Kotlin or Dart.
- **Who will maintain it?** A language the bank can hire for, train in and support internally beats a better language nobody knows.

- **How long must it live?** Long-lived systems favour languages with long-term-support releases and stable ecosystems.
- **How safe is it?** Memory-safe languages remove whole classes of security bugs; strong typing catches mistakes before production.

Legacy languages

COBOL and database procedure languages still run important parts of many banks' estates, often reliably for decades. The risk is not the language itself but the shrinking number of people who understand the code and the rules buried in it. Banks manage this by documenting business rules, wrapping legacy code behind APIs and moving logic out in stages, as described in legacy modernisation (chapter 9).

Trade-offs

Language strategy choices

Choice	You gain	You give up
A few standard languages across the bank	Shared tooling, skills and security review	Some teams use a less ideal tool for their job
Free choice per team	Best fit per system	Fragmented skills, tooling and maintenance
Rewrite legacy code in a modern language	Easier hiring and change	Risk of losing rules the old code encoded
Keep legacy code and wrap it	Low risk now	The skills problem grows

Pitfalls

- **Choosing by fashion** rather than by fit and long-term support.
- **Unreviewed dependencies** pulled in from public package registries.
- **Business rules in stored procedures** that no test covers.
- **One expert** who alone understands a critical codebase.
- **Floating-point numbers for money**, instead of decimal types or integer minor units.

Questions for a design review

- Why this language for this system, and who will maintain it in five years?
- How are third-party dependencies approved, scanned and updated?
- How are monetary amounts represented and rounded?
- Where do business rules live, and are they covered by tests?
- What happens if the one person who knows this codebase leaves?

Chapter 24

Payment-specific technology

Payments need specialised technology: message standards, secure networks, hardware for keys and PINs, tokens instead of card numbers, and strong authentication. Networks and regulators set much of it.

Part III ends where payments demand the most: message standards, keys and PINs, tokens and authentication.

Why it matters

Payments are where precision and security matter most, and where much of the technology is not the bank's choice. Networks and regulators set message formats, security rules and authentication requirements, and every participant must implement them exactly. Payment system architecture (chapter 5) explains the model; this page covers the technology that implements it.

The landscape

Payment technologies

Technology	Role	Where it is used	Notes
ISO 8583	Compact message format for card and ATM authorisations	Card networks, ATM switches, card processing	Each network adds its own field conventions
ISO 20022	Rich, structured XML or JSON payment messages	High-value and cross-border payments worldwide	Carries more data about payer, payee and purpose
SFMS	Secure messaging for RTGS, NEFT and related systems	Banks connecting to RBI-run payment systems	Launched 2001; run by IFTAS
INFINET	The banking sector's closed network	Connectivity for RBI-run payment systems	Launched 1999; run by IFTAS
UPI interfaces	Specifications, libraries and certification for UPI participants	Banks and apps joining UPI	Published and certified by the operator
Hardware security modules	Key storage, PIN verification and message signing	Card issuing, acquiring and payment switches	Payment HSMs are a specialised class
Tokenisation services	Replace card numbers with merchant-specific tokens	Online card payments and wallets	Required for stored cards
Interoperable QR codes	Carry payee details for scan-to-pay	Shops and merchants	One code accepted by many apps
3-D Secure and additional authentication	Authenticate the cardholder for card-not-present payments	Online card payments	Now governed by the 2025 authentication Directions

Families and standards, not recommendations. Network-specific details are in each operator's own documentation. Sources ^{1 2}

Message standards

ISO 8583 is the long-standing format for card authorisations: compact, fast and built around numbered fields such as amount, merchant type and response code. **ISO 20022** is a richer standard with structured data about the parties and the purpose of a payment. That structure helps screening, reconciliation and fraud detection. Payment engineers spend much of their time translating between formats and validating every field.

Networks and messaging in India

Banks reach RBI-run payment systems over a dedicated network and messaging layer. IDBRT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS.¹ SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities.¹ IFTAS is a wholly owned subsidiary of RBI, registered under the Companies Act, 2013; it runs INFINET, SFMS, the Indian Banking Community Cloud and GIFT.²

Keys, PINs and HSMs

Payment security rests on keys. PINs are encrypted at the point of entry and verified inside hardware security modules, so no application ever sees a clear PIN. Keys are organised in hierarchies: a small number of master keys protect the keys that protect data. They are changed on schedules, and handling them needs several people present, so no one person can misuse them.

Tokens instead of card numbers

Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead.³ A token works only for the merchant or device it was issued for, so a breach at one merchant does not expose usable card numbers. Tokenisation services, run by card networks and issuers, create tokens, map them back to cards for authorisation and manage their lifecycle when cards expire or are replaced.

Authentication

RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026.⁴ For digital payments other than card-present transactions, at least one authentication factor must be dynamic, that is, unique to the transaction.⁵ The 2025 authentication framework encourages new authentication factors but does not require banks to stop using SMS-based OTP.⁶ For cards used abroad online, Card issuers must be able to validate an additional authentication factor for non-recurring cross-border card-not-present transactions, when the overseas merchant asks, by 1 October 2026.⁴

In practice, banks are adding device-bound keys, biometrics and in-app approvals alongside OTPs. They are also using risk-based checks that ask for more when a payment looks unusual.

Scale and timing

Payment technology must work at national scale: UPI alone averages 791 million a day⁷. Every component in the path, such as message parsing, fraud scoring, HSM operations and the core posting, has a share of a tight time budget. A slow HSM or an overloaded fraud engine shows up to customers as failed payments.

How to choose

Most choices here are about implementation quality rather than technology selection: follow each network's specification exactly, certify early, size HSMs and tokenisation services for peak rather than average load, and keep payment components separate from the rest of the estate to limit what falls under card-security rules.

Pitfalls

- **Loose message validation**, letting malformed fields through to downstream systems.
- **HSM capacity sized for average load**, failing on festival or salary days.
- **Card numbers surviving in logs**, test data or analytics copies.

- **Authentication added as an afterthought**, creating extra steps that customers abandon.
- **Specification drift**, when a network updates its rules and one component is not upgraded.

Questions for a design review

- Which message standards does this system parse, and how strictly is each field validated?
- Where are keys and PINs handled, and does any system see them in clear?
- Could a card number appear in any log, file or database outside the tokenisation service?
- Which authentication factors does each journey use, and which is dynamic?
- What is the time budget for each step in the payment path, and what happens when one is exceeded?

Notes

1. **About IDRBT** <https://www.idrbt.ac.in/about-idrbt>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.

Supports: SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities (as of 1 January 2025); IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS (as of 1 January 2025).

2. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: IFTAS is a wholly owned subsidiary of RBI, registered under the Companies Act, 2013; it runs INFINET, SFMS, the Indian Banking Community Cloud and GIFT (as of 20 September 2022).

3. **Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)] (RBI/2022-2023/95)** <https://website.rbi.org.in/web/rbi/-/notifications/restriction-on-storage-of-actual-card-data-i.e.-card-on-file-cof-12363>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead (as of 28 July 2022).

4. **RBI unveils new directions to strengthen digital payment security** <https://www.tribuneindia.com/news/business/rbi-unveils-new-directions-to-strengthen-digital-payment-security>. The Tribune. **Reported**, accessed 29 September 2026.

Supports: RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026 (as of 25 September 2025); Card issuers must be able to validate an additional authentication factor for non-recurring cross-border card-not-present transactions, when the overseas merchant asks, by 1 October 2026 (as of 25 September 2025).

5. **RBI Authentication Mechanisms for Digital Payment Transactions Directions, 2025** <https://kpmg.com/in/en/insights/2025/12/reserve-bank-of-india-rbi-authentication-mechanisms-for-digital-payment-transactions-directions-2025.html>. KPMG in India. **Analyst**, accessed 29 September 2026.

Supports: For digital payments other than card-present transactions, at least one authentication factor must be dynamic, that is, unique to the transaction (as of 1 December 2025).

6. **RBI issues Directions on Framework on Authentication Mechanisms for Digital Payment Transactions** https://www.business-standard.com/markets/capital-market-news/rbi-issues-directions-on-framework-on-authentication-mechanisms-for-digital-payment-transactions-125092501090_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: The 2025 authentication framework encourages new authentication factors but does not require banks to stop using SMS-based OTP (as of 25 September 2025).

7. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-ncpi-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).

Part IV

Scale and decisions

Three chapters on the hard parts of running banking technology: keeping systems up when volumes peak, deciding what to build and what to buy, and facing the known weaknesses honestly.

Chapter 25

High-volume systems

Indian payment volumes are among the highest in the world, and they peak on predictable days. Banks shield their cores with layers that absorb, queue and shed load. Idempotency makes retries safe.

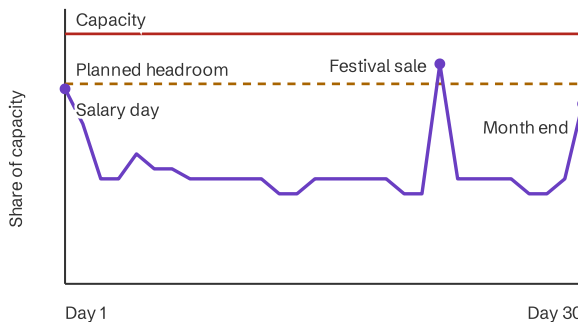
Part IV begins with scale: what peak volume means in India, and the patterns that keep the core standing.

What “high volume” means here

In August 2026, UPI processed 24.51 billion transactions¹, about 791 million a day¹, and IMPS another 360 million transactions¹. Every one of those payments touches at least two banks' systems, and demand is not spread evenly. It climbs on predictable days:

- **Salary days**, at the start of the month, when credits arrive and spending follows.
- **Loan instalment and bill dates**, in the first week, when mandates debit millions of accounts.
- **Month end and financial-year end**, when businesses settle and reporting runs.
- **Festive sales**, when card and UPI payments to merchants spike for hours.
- **Deadline days**, such as tax due dates or popular share offers, when many people pay in the same window.

A month of load against capacity



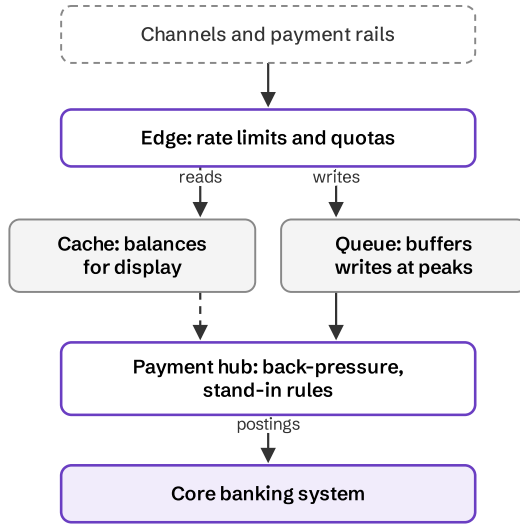
Illustrative. The shape, not the numbers, is the point: peaks are predictable, and capacity is planned for them.

The consequence of getting this wrong is public and regulatory, not just technical. RBI said the bank's core banking system and online channels had suffered frequent and significant outages over the previous two years, and that rapid growth in digital transactions was adding load on its IT systems.⁴ On 24 April 2024 RBI directed Kotak Mahindra Bank to stop onboarding new customers through online and mobile channels and to stop issuing new credit cards, citing concerns from its IT examinations of the bank for 2022 and 2023.⁵

Shielding the core

The core banking system is usually the hardest component to scale, so high-volume design is largely about protecting it. Requests pass through layers that each absorb part of the load before anything reaches the ledger.

Layers that shield the core



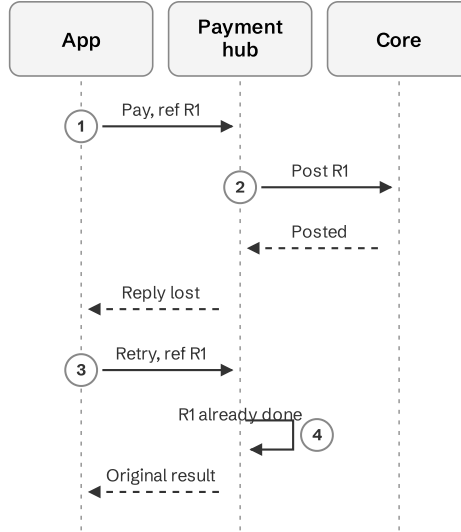
Illustrative. Not every bank has every layer, and the order varies.

- **Caching** serves reads, such as a balance shown on an app's home screen, without asking the core each time.
- **Queues** buffer writes, so a peak becomes a slightly longer line rather than a failure.
- **Back-pressure** slows or rejects new work when the systems behind are saturated, instead of letting everything time out together.
- **Rate limits** protect shared capacity from any one channel, partner or runaway client.

Idempotency and safe retries

At high volume, time-outs are not rare events but a steady stream. A client that times out will retry, and a retry must never move money twice. Each payment therefore carries a unique reference from its sender, and every system records references it has already processed. A repeated request returns the original result.

A retry that does not pay twice



Illustrative. The same reference makes the second request harmless.

Retries themselves need discipline: wait longer between each attempt, add a little randomness so thousands of clients do not retry in step, and stop after a limit. Payments that end up stuck must still be resolved within regulatory limits. If a UPI transfer debits the payer but does not credit the beneficiary, the beneficiary bank must reverse it by T+1 day; after that, ₹100 a day is payable.²

Circuit breakers, bulkheads and graceful degradation

A **circuit breaker** stops calling a failing dependency for a short time, returning a fast failure instead of waiting on time-outs, then tests it again. A **bulkhead** gives each channel or function its own pool of threads and connections, so a problem in one cannot exhaust capacity for all. **Graceful degradation** keeps the most important functions working when something fails. Payments may continue while statements and analytics pause. The app may show a balance marked “as of” a few minutes ago, rather than an error.

Stand-in processing is the payment-specific form. When the core is unavailable or busy with its batch cycle, a stand-in layer approves low-risk transactions against a shadow balance within limits, and replays them to the core afterwards. It keeps payments flowing, at the cost of reconciliation work.

Asynchronous processing and the outbox

Work that does not need to finish before the customer gets an answer, such as notifications, loyalty points or analytics, is done asynchronously. The service records the change and an event in one database transaction, the outbox, and a separate process publishes the event. That keeps the customer path short and the event reliable. See event-driven architecture (chapter 7).

Capacity planning, load testing and warm capacity

Capacity is planned for the peak, not the average, with headroom on top. Load tests replay realistic peak traffic, including the mix of payment types and the slow dependencies, not just a simple script. Autoscaling helps for stateless services, but new capacity takes time to start and warm up. Banks therefore scale up

before known peaks rather than waiting for load to rise. Databases and cores usually cannot autoscale at all, which is why the shielding layers matter.

Batch windows

Not all volume is real time. Mandate collections, salary files and statement runs arrive as large batches, often at the same times each month. Batch jobs are scheduled so they do not collide with real-time peaks, split into pieces that can run in parallel, and checkpointed so a failure resumes rather than restarts.

Latency budgets for fraud scoring

Real-time fraud scoring sits inside the payment path, so it gets a fixed slice of the time available. An illustrative budget might give the fraud engine a few tens of milliseconds. If it cannot answer in time, the payment proceeds or stops by a pre-agreed rule, rather than waiting. Any such figure here is illustrative; each bank sets its own from its end-to-end limits.

Measuring success: SLOs and resilience drills

The measure that matters is the share of payments that succeed, and how fast, broken down by channel, partner and type. Service level objectives turn that into targets, and error budgets decide when reliability work takes priority. Resilience is proven by drills, not by design documents. DR drills for critical information systems must be held at least every six months, and major issues found in a drill must be fixed and tested again before the next cycle.³ A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day.³

Questions for a design review

- What is the expected peak for this system, on which day, and what headroom does it have above that?
- Which layer absorbs the peak before it reaches the core?
- How does every client retry, and does every retry reuse its reference?
- What does this system do when a dependency is slow: wait, fail fast or degrade?
- When was it last load-tested at peak volume, with realistic traffic?

Notes

1. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-ncpi-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: UPI processed 24.51 billion transactions worth ₹29.82 trillion in August 2026, its highest monthly volume to date (as of 31 August 2026); UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026); IMPS processed 360 million transactions worth ₹7.04 trillion in August 2026 (as of 31 August 2026).

2. **Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems (RBI/2019-20/67)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?id=11693>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: If a UPI transfer debits the payer but does not credit the beneficiary, the beneficiary bank must reverse it by T+1 day; after that, ₹100 a day is payable (as of 20 September 2019).

3. **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text)** <https://rbi.org.in/Scripts/NotificationUser.aspx?id=12562&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: DR drills for critical information systems must be held at least every six months, and major issues found in a drill must be fixed and tested again before the next cycle (as of 7 November 2023); A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day (as of 7 November 2023).

4. **RBI bars Kotak Mahindra Bank from onboarding new customers via online, mobile banking channels** <https://inc42.com/buzz/rbi-bars-kotak-mahindra-bank-from-onboarding-new-customers-via-online-mobile-banking-channels/>. Inc42. **Reported**, accessed 29 September 2026.

Supports: RBI said the bank's core banking system and online channels had suffered frequent and significant outages over the previous two years, and that rapid growth in digital transactions was adding load on its IT systems (as of 24 April 2024).

5. **RBI directs Kotak Mahindra Bank to cease issue of fresh credit cards, bars onboarding of new online customers** <https://newsonair.gov.in/rbi-directs-kotak-mahindra-bank-to-cease-issue-of-fresh-credit-cards-bars-onboarding-of-new-online-customers>. All India Radio News (Prasar Bharati).

25 High-volume systems

Reported, accessed 29 September 2026.

Supports: On 24 April 2024 RBI directed Kotak Mahindra Bank to stop onboarding new customers through online and mobile channels and to stop issuing new credit cards, citing concerns from its IT examinations of the bank for 2022 and 2023 (as of 24 April 2024).

Chapter 26

Build versus buy

Banks buy most of their technology and build the parts that set them apart. Six factors decide which is which. RBI's outsourcing rules apply whenever a third party runs part of the service.

Every system in this book was either built or bought. This chapter offers a framework for choosing.

Why it is rarely all one or the other

Almost every bank buys its core banking platform, card systems and much of its infrastructure, and builds at least some of its customer experience and decisioning. The real questions are which capabilities belong in each group, how much to customise what is bought, and how to keep the ability to change course. This page gives a framework, not a verdict. The right answer differs by bank and changes over time.

Six factors

The six factors in a build-versus-buy decision

Factor	Points towards building	Points towards buying
Differentiation	The capability is how you win customers	Every competitor needs the same thing
Regulatory complexity	Rules are simple, or you want control over how you meet them	Rules are complex and change often, and a vendor tracks them for many clients
Total cost of ownership	Large, long-lived use where build costs are spread thinly	Small or short-lived use, or costs that are mostly shared R&D
Speed to market	There is time to build well	You need it working soon
Talent	You can hire and keep the people to build and run it	The skills are scarce or not core to your organisation
Sovereignty and lock-in	You need full control of roadmap, data and exit	A vendor's roadmap is acceptable and exit is manageable

A worksheet

Rate one capability against the six factors using the worksheet below. The scorer treats differentiation, urgency and in-house talent as the strongest influences, and control, scale and regulatory complexity as moderate ones. The result is a starting point for discussion.

Worksheet: rate one capability

Question	1 means	Your rating	5 means
How much does this capability set you apart from competitors?	Commodity	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐	Core differentiator
How complex and fast-changing are the rules it must follow?	Simple and stable	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐	Complex and changing
How large and long-lived will your use of it be?	Small or short-lived	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐	Large and long-lived
How urgently do you need it in production?	No rush	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐	Very urgent
How strong is your own team for building and running it?	Weak	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐	Strong
How much do you need to control its roadmap, data and exit?	Little	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐	A great deal

Differentiation, urgency and in-house talent carry the most weight. High ratings on differentiation, scale, talent and control point towards building; high ratings on regulatory complexity and urgency point towards buying. A mix usually means a hybrid.

System by system

Common patterns, system by system

System	Common pattern	Why
Core banking	Buy	Huge, regulated, slow-changing functionality that vendors spread across many banks
Mobile app	Build, on bought components	The main customer experience and a key differentiator
Credit underwriting models	Build or hybrid	Models encode the bank's own risk appetite and data
Anti-money laundering	Buy, then tune	Complex, rule-heavy and audited; tuning to the bank's customers is the in-house part
KYC and onboarding	Hybrid	Buy identity and document checks; build the journey
API gateway	Buy	Commodity infrastructure; configuration is the work
Data platform	Hybrid	Buy storage and processing; build data models, pipelines and reports
Fraud detection	Hybrid	Buy the engine; build rules, features and models from the bank's own data
Cloud infrastructure	Buy	Nobody builds their own cloud; the decisions are which and how
Conversational AI	Hybrid	Buy the models and platform; build the knowledge, guardrails and journeys
Payment orchestration	Build or hybrid	Routing, retries and reconciliation are tightly tied to the bank's own systems

Illustrative patterns across the industry, not a description of any named bank.

Patterns by type of institution

- **Public-sector banks** tend to buy large, proven platforms and run long programmes with system integrators. Scale, procurement rules and the need for stability shape those choices. SBI's core banking has run on TCS BaNCs since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years.⁴
- **Large private banks** usually buy the core and build more around it: apps, decisioning and data, with sizeable in-house engineering teams.
- **Small finance banks and newer banks** often choose modern or hosted platforms to launch quickly, and build selectively where they compete.
- **Cooperative banks** frequently share a platform rather than run their own. IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.³
- **Fintechs** build most of their product, rent infrastructure and partner with banks for the regulated parts.

These are tendencies, not rules; any single institution may differ.

What RBI expects when a third party is involved

Buying often means a vendor runs part of the service, which makes it outsourcing. RBI's Direction on IT outsourcing sets the expectations:

- Outsourcing does not reduce a regulated entity's obligations; its board and senior management remain ultimately responsible for the outsourced activity.¹
- Responsibility for resolving customers' grievances about outsourced services stays with the regulated entity, and outsourcing cannot reduce customers' rights against it.¹
- Due diligence on an IT service provider must cover its experience and competence to deliver over the contract period and its financial soundness.¹
- Regulated entities must consider the risk of concentrating their outsourcing with a single provider or a few providers.¹

- A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement.²
- RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud.²

How lock-in happens

Lock-in is rarely one decision. It accumulates through customisations that only the vendor can maintain, proprietary data formats, integrations built against vendor-specific interfaces, contracts without data-export clauses, and skills that exist only at the vendor. Each of these is manageable on its own; together they can make leaving impractical. The defences are configuration over customisation, owning data in documented formats, putting your own APIs in front of bought systems, contract clauses for exit, and keeping enough in-house knowledge to run a transition.

A worked example

This example is illustrative. A mid-sized bank wants better fraud detection for UPI payments. It rates the six factors:

- **Differentiation: high.** Fraud losses and false declines both affect customers.
- **Regulatory complexity: medium.**
- **Scale: high.**
- **Urgency: high.** Losses are rising.
- **Talent: medium.** It has data scientists but no real-time engineering team.
- **Control: high.** The models use sensitive customer data.

The factors pull in both directions, which points to a hybrid. The bank buys a proven real-time scoring engine to deploy quickly. It then builds its own features and models on its data, and keeps the right to export rules and models. It also plans, from the start, what it would take to replace the engine.

Questions for a decision

- Would a customer notice, or care, if this capability were the same as every competitor's?
- What will it cost over ten years, including people, upgrades and exit, for both options?
- If we buy, which parts will we still build, and who owns them?
- How would we leave this vendor, how long would it take, and what would we lose?
- Which RBI outsourcing requirements does this arrangement trigger, and who will evidence them?

Notes

1. [Master Direction on Outsourcing of Information Technology Services \(full text\)](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486) https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Outsourcing does not reduce a regulated entity's obligations; its board and senior management remain ultimately responsible for the outsourced activity (as of 10 April 2023); Responsibility for resolving customers' grievances about outsourced services stays with the regulated entity, and outsourcing cannot reduce customers' rights against it (as of 10 April 2023); Regulated entities must consider the risk of concentrating their outsourcing with a single provider or a few providers (as of 10 April 2023); Due diligence on an IT service provider must cover its experience and competence to deliver over the contract period and its financial soundness (as of 10 April 2023).

2. [Master Direction on Outsourcing of Information Technology Services \(RBI/2023-24/102\)](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486) https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement (as of 10 April 2023); RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud (as of 10 April 2023).

3. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services (as of 20 September 2022).

4. **SBI deepens partnership with TCS to drive innovation and enhance customer experience** <https://tcs.com/who-we-are/newsroom/press-release/sbi-deepens-partnership-with-tcs-drive-innovation-enhance-customer-experience>. Tata Consultancy Services. **Vendor**, accessed 29 September 2026.

Supports: SBI's core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years (as of 6 October 2021).

Chapter 27

Limitations and known problems

Indian banking technology works at huge scale but carries known weaknesses. Most trace back to batch-era cores and estates that grew by addition. Each has a cause, an effect and a mitigation.

Part IV closes by facing the weaknesses directly, including the cases where a regulator stepped in.

How to read this page

Each limitation is described the same way: its **cause**, its **effect**, the **common mitigation** and its **status** today. The page names an institution only where a regulator or reputable press has published the facts. Everything else describes patterns seen across the industry.

Public examples

Regulators have acted when technology weaknesses reached customers:

- On 24 April 2024 RBI directed Kotak Mahindra Bank to stop onboarding new customers through online and mobile channels and to stop issuing new credit cards, citing concerns from its IT examinations of the bank for 2022 and 2023. ¹ RBI said the bank's core banking system and online channels had suffered frequent and significant outages over the previous two years, and that rapid growth in digital transactions was adding load on its IT systems. ² RBI said it had found serious deficiencies in areas including IT inventory management, patch and change management, user access management, vendor risk management, data security and leak prevention, and business continuity and DR drills. ³ RBI lifted the restrictions on Kotak Mahindra Bank in February 2025, after an external audit and remedial measures. ⁴
- In 2020 RBI placed similar restrictions on HDFC Bank, barring new digital business-generating launches and new credit card sourcing; they were lifted in 2022. ²

Both cases show the same pattern: digital growth outpacing the resilience of the systems underneath, and a regulator choosing to slow a bank's growth until the gap was closed.

The limitations

1. Cores designed for a batch era

- **Cause.** Many cores assume a nightly window when postings stop and batch work runs.
- **Effect.** Round-the-clock payments must be handled by stand-in layers during end of day, adding complexity and reconciliation.
- **Common mitigation.** Shorter, incremental batch cycles; stand-in processing; payment hubs that shield the core.
- **Status.** Widespread; eased gradually through core upgrades and modernisation.

2. Monolithic scaling limits

- **Cause.** One large database behind one application holds every account.
- **Effect.** Capacity is capped by the biggest machine, and busy accounts become hot spots.
- **Common mitigation.** Caching, queuing, read replicas and moving non-ledger functions out of the core.
- **Status.** Managed rather than solved at most banks.

3. Vendor lock-in and migration risk

- **Cause.** Heavily customised platforms, proprietary formats and long contracts.

- **Effect.** Changing vendor becomes impractical, weakening the bank's negotiating position.
- **Common mitigation.** Configuration over customisation, owned data formats, APIs in front of vendor systems and tested exit plans. Regulated entities must consider the risk of concentrating their outsourcing with a single provider or a few providers.⁷
- **Status.** A standing risk that rises with every customisation.

4. Legacy skills

- **Cause.** Critical systems written in older languages or on platforms few people now learn.
- **Effect.** Knowledge concentrates in a few people; changes slow down and become riskier.
- **Common mitigation.** Documenting business rules, pairing and training, wrapping legacy code behind APIs and moving logic out in stages.
- **Status.** Growing as experienced staff retire.

5. Pending and reversal states

- **Cause.** Payments cross several independently run systems, and any link can time out.
- **Effect.** Customers are debited without the payee being credited, and must wait for a reversal. At about 791 million a day⁵, even a tiny failure rate means many cases a day.
- **Common mitigation.** Unique references, automated status checks and reversal jobs, within regulatory limits. RBI's framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint.⁶
- **Status.** Well governed by rules; still a common customer complaint.

6. Liquidity and settlement risk

- **Cause.** Customers are credited instantly while banks settle later, on a net basis.
- **Effect.** A bank carries exposure to other banks until settlement; a failure in the cycle affects many participants.
- **Common mitigation.** Settlement guarantees, limits and monitoring of intraday positions by operators and banks.
- **Status.** Managed by operators and regulators; invisible to most customers.

7. Retail limits versus business needs

- **Cause.** Instant rails were designed first for consumers, with per-transaction and daily ceilings.
- **Effect.** Businesses making large payments must switch rails or split payments.
- **Common mitigation.** Higher ceilings for specified merchant categories, and RTGS for large values.
- **Status.** Improving as ceilings rise for specific uses; see payment rails (chapter 3).

8. Reconciliation burden

- **Cause.** The same transaction is recorded by the app, the switch, the payment hub, the core and the general ledger.
- **Effect.** Mismatches need investigation, often manually, and delay the resolution of customer complaints.
- **Common mitigation.** Automated matching on shared references, with exceptions routed to named owners.
- **Status.** Large operational effort at most banks.

9. Social-engineering fraud versus technical controls

- **Cause.** Fraudsters persuade customers to authorise payments themselves, so strong authentication is passed rather than broken.

- **Effect.** Losses continue even when systems work exactly as designed.
- **Common mitigation.** Behavioural fraud scoring, cooling-off periods for new payees, warnings at the point of payment, mule-account detection and customer education.
- **Status.** A leading and growing risk.

10. API security gaps between channels and the core

- **Cause.** New channels expose older functions through APIs that were never designed for direct exposure.
- **Effect.** Weaknesses such as missing authorisation checks or excessive data in responses.
- **Common mitigation.** A gateway that enforces identity and limits, fine-grained authorisation in each service, and API security testing.
- **Status.** Improving; a frequent audit finding.

11. Fragmented AML views

- **Cause.** Customer and transaction data sit in separate systems for deposits, cards, loans and payments.
- **Effect.** Suspicious patterns that span products are harder to see.
- **Common mitigation.** A single customer view feeding transaction monitoring, and entity resolution across systems.
- **Status.** A long-running programme at most banks.

12. Many regulatory returns and data-lineage risk

- **Cause.** Returns are produced from many source systems through many transformations.
- **Effect.** Errors are hard to trace, and the same figure can differ between returns.
- **Common mitigation.** A governed data warehouse, documented lineage and automated quality checks. See data architecture (chapter 8).
- **Status.** Improving with investment; still labour-intensive.

13. Cloud adoption constraints

- **Cause.** Data residency, outsourcing duties and exit planning all apply to cloud use. RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad.⁹ RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud.¹⁰
- **Effect.** Slower adoption than in some other sectors, especially for systems of record.
- **Common mitigation.** Cloud regions in India, clear placement rules and reusable control evidence.
- **Status.** Adoption growing for channels, analytics and development.

14. Depth of disaster-recovery testing

- **Cause.** Full switch-overs are disruptive, so drills can be narrowed to what is safe.
- **Effect.** A DR site that has passed drills may still fail in a real disaster.
- **Common mitigation.** Regular, realistic drills that run real business at the DR site. DR drills for critical information systems must be held at least every six months, and major issues found in a drill must be fixed and tested again before the next cycle.⁸
- **Status.** Required by rule; depth varies in practice.

15. Talent asymmetry

- **Cause.** Engineering talent concentrates in large banks, technology firms and fintechs.
- **Effect.** Smaller banks depend more on vendors and struggle to keep in-house knowledge.

- **Common mitigation.** Shared platforms, managed services and focused hiring for the capabilities that matter most.
- **Status.** Persistent.

Why “too complex to change” is not the end

Many of these limitations share one root: estates that grew by adding systems rather than replacing them. It is tempting to conclude that nothing can change without a risky replacement. In practice, banks improve step by step:

- wrap the core behind APIs;
- move one capability at a time to newer systems;
- automate reconciliation;
- test resilience for real;
- retire what is no longer needed.

Each step is small enough to reverse and valuable on its own. Legacy modernisation (chapter 9) describes the patterns.

Notes

1. **RBI directs Kotak Mahindra Bank to cease issue of fresh credit cards, bars onboarding of new online customers** <https://newsonair.gov.in/rbi-directs-kotak-mahindra-bank-to-cease-issue-of-fresh-credit-cards-bars-onboarding-of-new-online-customers>. All India Radio News (Prasar Bharati). **Reported**, accessed 29 September 2026.
Supports: On 24 April 2024 RBI directed Kotak Mahindra Bank to stop onboarding new customers through online and mobile channels and to stop issuing new credit cards, citing concerns from its IT examinations of the bank for 2022 and 2023 (as of 24 April 2024).
2. **RBI bars Kotak Mahindra Bank from onboarding new customers via online, mobile banking channels** <https://inc42.com/buzz/rbi-bars-kotak-mahindra-bank-from-onboarding-new-customers-via-online-mobile-banking-channels/>. Inc42. **Reported**, accessed 29 September 2026.
Supports: RBI said the bank’s core banking system and online channels had suffered frequent and significant outages over the previous two years, and that rapid growth in digital transactions was adding load on its IT systems (as of 24 April 2024); In 2020 RBI placed similar restrictions on HDFC Bank, barring new digital business-generating launches and new credit card sourcing; they were lifted in 2022 (as of 24 April 2024).
3. **RBI finds Kotak Mahindra Bank deficient in IT risk management, bars online customer onboarding (PTI)** <https://thefederal.com/category/business/rbi-finds-kotak-mahindra-bank-deficient-in-it-risk-management-bars-online-customer-onboarding-119336>. The Federal. **Reported**, accessed 29 September 2026.
Supports: RBI said it had found serious deficiencies in areas including IT inventory management, patch and change management, user access management, vendor risk management, data security and leak prevention, and business continuity and DR drills (as of 24 April 2024).
4. **RBI lifts business restrictions on Kotak Mahindra Bank** <https://www.newsonair.gov.in/rbi-lifts-business-restrictions-on-kotak-mahindra-bank/>. All India Radio News (Prasar Bharati). **Reported**, accessed 29 September 2026.
Supports: RBI lifted the restrictions on Kotak Mahindra Bank in February 2025, after an external audit and remedial measures (as of 12 February 2025).
5. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-ncpi-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.
Supports: UPI averaged 791 million transactions a day in August 2026 (as of 31 August 2026).
6. **Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems (RBI/2019-20/67)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11693>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI’s framework for failed transactions, in force since 15 October 2019, sets out time limits for reversal and requires compensation to be paid automatically, without a complaint (as of 20 September 2019).
7. **Master Direction on Outsourcing of Information Technology Services (full text)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: Regulated entities must consider the risk of concentrating their outsourcing with a single provider or a few providers (as of 10 April 2023).
8. **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text)** <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: DR drills for critical information systems must be held at least every six months, and major issues found in a drill must be fixed and tested again before the next cycle (as of 7 November 2023).

9. **Storage of Payment System Data (RBI/2017-18/153)** <https://rbi.org.in/scripts/NotificationUser.aspx?Id=11244>, Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad (as of 6 April 2018).

10. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486, Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud (as of 10 April 2023).

Part V

Governance

The rules and the institutions. The first chapter explains who regulates bank technology, how rules are made and how they are enforced. The second describes the institutions around the Reserve Bank of India, what each one does and how they connect.

Chapter 28

Regulators and mandates

Several regulators shape bank technology in India, with RBI at the centre. They make rules through consultation and directions, and enforce them through inspection and business restrictions.

Part V turns to governance, beginning with the bodies that set the rules for bank technology.

Who regulates what

A bank's technology answers to more than one authority. RBI regulates banks and payment systems; other bodies cover cyber incidents, identity, personal data and the financial markets in which banks also operate.

Regulators and what they cover

Body	What it regulates or runs	Where it touches bank technology
Reserve Bank of India (RBI)	Banks, non-bank lenders and payment systems	IT governance, outsourcing and cloud, cyber security, payment data storage, authentication, KYC, failed-transaction rules
National Payments Corporation of India (NPCI)	Operator of retail payment systems, authorised by RBI	Technical specifications, certification and operating rules for UPI, IMPS, cards and other systems it runs
CERT-In	National agency for cyber incidents, under MeitY	Incident reporting deadlines and log retention
Ministry of Electronics and IT (MeitY)	IT Act and data protection law	Digital Personal Data Protection Act and Rules
UIDAI	Aadhaar	Aadhaar authentication and e-KYC for banks acting as authentication or e-KYC user agencies
FIU-IND	Financial intelligence under the Prevention of Money-laundering Act	Suspicious and cash transaction reporting systems
SEBI, IRDAI, PFRDA	Securities, insurance and pensions	Rules for bank activities in those markets, such as broking, depository and insurance distribution
Ministry of Finance and FSDC	Financial policy and coordination between regulators	Laws such as the SARFAESI Act; inter-regulatory issues

NPCI is not a regulator in the legal sense, but its rules bind every participant in the systems it runs. NPCI was incorporated in December 2008 as a not-for-profit company, an initiative of RBI and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007.¹⁹ RBI classified NPCI as a system-wide important payment system in June 2020.¹⁹

How rules are made

RBI usually consults before it regulates. It publishes a draft, invites comments, then issues a final instrument. The 2025 authentication framework followed that path: Before issuing its 2025 authentication Directions, RBI published draft directions for comment on 31 July 2024 and 7 February 2025.⁷ RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026.⁶ Model risk guidance is at the draft stage now: On 24 June 2026 RBI released draft guidance on model risk management across the model lifecycle, including models that use AI and machine learning, for public comment.¹⁸

RBI's rules take a few forms:

- **Master Directions** set out all the rules on a subject in one place and are updated as the rules change.
- **Circulars** issue specific instructions.
- **Master Circulars** consolidate circulars on a subject as of a date.

Other bodies use their own instruments: CERT-In issues directions under the IT Act, and MeitY notifies rules under the laws it administers.

The main technology mandates

Technology mandates, with primary sources

Mandate	Issued by	Date	What it requires, in brief
IT Governance, Risk, Controls and Assurance Practices Directions	RBI	7 Nov 2023	Board-level IT governance, risk management, recovery objectives and DR drills
Outsourcing of IT Services Master Direction	RBI	10 Apr 2023	Due diligence, accountability, cloud use, incident reporting and exit plans
Storage of Payment System Data	RBI	6 Apr 2018	Payment data stored only in India
Restriction on storage of actual card data (card-on-file)	RBI	28 Jul 2022	Only issuers and networks may store card data; merchants use tokens
Harmonisation of turnaround time for failed transactions	RBI	20 Sep 2019	Deadlines for reversals and automatic compensation
Positive Pay System for CTS	RBI	25 Sep 2020	Advance confirmation for large cheques
Continuous clearing in CTS: Phase 2 postponed	RBI	24 Dec 2025	Phase 1 continues; Phase 2 postponed; new session hours
Account Aggregator Master Direction	RBI	2 Sep 2016	Licensing and operation of consent-based data sharing
Central KYC Records Registry operationalised	RBI	8 Jul 2016	Use of the central KYC registry run by CERSAI
Directions under section 70B(6) of the IT Act	CERT-In	28 Apr 2022	Report incidents within 6 hours; keep logs for 180 days in India

Dates are issue dates. Check each source for amendments and effective dates. Sources [1](#) [2](#) [3](#) [4](#) [5](#) [10](#) [11](#) [8](#) [9](#) [12](#)

The detail behind several of these:

- **Payment data.** RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad. ³ Payment system providers had to comply within six months and submit a system audit report by a CERT-In-empowered auditor; the circular was issued under the Payment and Settlement Systems Act, 2007. ³
- **Cyber incidents.** CERT-In's directions of 28 April 2022 under section 70B(6) of the IT Act require reportable cyber incidents to be reported to CERT-In within 6 hours of noticing them; they took effect 60 days after issue. ¹² The same CERT-In directions require logs of all ICT systems to be kept securely for a rolling 180 days, within Indian jurisdiction. ¹² RBI adds its own clock for incidents at suppliers: A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them. ²
- **Personal data.** MeitY notified the Digital Personal Data Protection Rules on 13 November 2025. Provisions on the Data Protection Board applied at once, consent-manager rules apply from 13 November 2026, and most obligations on organisations apply from 13 May 2027. ¹³

How rules are enforced

RBI supervises banks through off-site returns and on-site inspections, including IT examinations. When it finds weaknesses, it issues corrective action plans; when those are not met, it can restrict business.

- **Payment data storage.** RBI had earlier restricted American Express and Diners Club from onboarding new domestic customers from 1 May 2021 on the same grounds. ¹⁶ RBI barred Mastercard from onboarding new domestic card customers from 22 July 2021 for not complying with the payment data

storage directions.¹⁶ RBI lifted the restriction on Mastercard in June 2022 after satisfactory compliance with the data storage directions.¹⁷

- **IT resilience.** On 24 April 2024 RBI directed Kotak Mahindra Bank to stop onboarding new customers through online and mobile channels and to stop issuing new credit cards, citing concerns from its IT examinations of the bank for 2022 and 2023.¹⁴

The pattern is consistent. Restrictions target growth, such as new customers or new cards, rather than existing customers, and they are lifted once the regulator is satisfied the gaps are closed. Limitations and known problems (chapter 27) describes these cases in more detail.

Questions for a compliance review

- Which of the mandates above apply to this system, and who owns evidence for each?
- Where is this system's payment data stored, including backups and logs?
- Could a cyber incident here be reported to CERT-In and RBI within 6 hours?
- Which parts of this system are outsourced, and is the outsourcing assessment complete?
- Which rules affecting this system are still in draft, and who is tracking them?

Notes

1. **Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI/2023-24/107)** <https://website.rbi.org.in/web/rbi/-/notifications/master-direction-on-information-technology-governance-risk-controls-and-assurance-practices>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI issued the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on 7 November 2023 (RBI/2023-24/107) (as of 7 November 2023).

2. **Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023 (as of 10 April 2023); A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them (as of 10 April 2023).

3. **Storage of Payment System Data (RBI/2017-18/153)** <https://rbi.org.in/scripts/NotificationUser.aspx?id=11244>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad (as of 6 April 2018); Payment system providers had to comply within six months and submit a system audit report by a CERT-In-empanelled auditor; the circular was issued under the Payment and Settlement Systems Act, 2007 (as of 6 April 2018).

4. **Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)] (RBI/2022-2023/95)** <https://website.rbi.org.in/web/rbi/-/notifications/restriction-on-storage-of-actual-card-data-i.e.-card-on-file-cof-12363>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead (as of 28 July 2022).

5. **Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems (RBI/2019-20/67)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?id=11693>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI's framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint (as of 20 September 2019).

6. **RBI unveils new directions to strengthen digital payment security** <https://www.tribuneindia.com/news/business/rbi-unveils-new-directions-to-strengthen-digital-payment-security>. The Tribune. **Reported**, accessed 29 September 2026.

Supports: RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026 (as of 25 September 2025).

7. **RBI issues Directions on Framework on Authentication Mechanisms for Digital Payment Transactions** https://www.business-standard.com/markets/capital-market-news/rbi-issues-directions-on-framework-on-authentication-mechanisms-for-digital-payment-transactions-125092501090_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: Before issuing its 2025 authentication Directions, RBI published draft directions for comment on 31 July 2024 and 7 February 2025 (as of 25 September 2025).

8. **Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 (updated 6 September 2024)** https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI issued its Master Direction for Account Aggregators on 2 September 2016; an Account Aggregator must be a non-bank financial company registered with RBI (as of 6 September 2024).

9. **Amendment to Master Direction on KYC: Operationalisation of Central KYC Registry (RBI/2016-17/11)** <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10498>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: The Government of India authorised CERSAI to act as the Central KYC Records Registry by notification S.O. 3183(E) of 26 November 2015; the registry went live on 15 July 2016 (as of 8 July 2016).

10. **Positive Pay System for Cheque Truncation System (RBI/2020-21/41)** <https://website.rbi.org.in/web/rbi/-/notifications/positive-pay-system-for-cheque-truncation-system-11969>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: Since 1 January 2021, banks must offer Positive Pay for cheques of ₹50,000 and above; using it is the account holder's choice, and banks may make it mandatory from ₹5 lakh (as of 25 September 2020).

11. **Continuous Clearing and Settlement on Realisation in Cheque Truncation System: Phase 2 (RBI/2025-26/156)** <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=13232&Mode=0>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI moved the Cheque Truncation System from batch processing to continuous clearing with settlement on realisation; Phase 1 took effect on 4 October 2025 (as of 24 December 2025).

12. **Directions under sub-section (6) of section 70B of the IT Act, 2000 (28 April 2022)** https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf. CERT-In, Ministry of Electronics and Information Technology. **Primary source**, accessed 29 September 2026.

Supports: CERT-In's directions of 28 April 2022 under section 70B(6) of the IT Act require reportable cyber incidents to be reported to CERT-In within 6 hours of noticing them; they took effect 60 days after issue (as of 28 April 2022); The same CERT-In directions require logs of all ICT systems to be kept securely for a rolling 180 days, within Indian jurisdiction (as of 28 April 2022).

13. **MeitY notifies final Digital Personal Data Protection Rules 2025** <https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/>. S.S. Rana & Co.. **Analyst**, accessed 29 September 2026.

Supports: MeitY notified the Digital Personal Data Protection Rules on 13 November 2025. Provisions on the Data Protection Board applied at once, consent-manager rules apply from 13 November 2026, and most obligations on organisations apply from 13 May 2027 (as of 14 November 2025).

14. **RBI directs Kotak Mahindra Bank to cease issue of fresh credit cards, bars onboarding of new online customers** <https://newsonair.gov.in/rbi-directs-kotak-mahindra-bank-to-cease-issue-of-fresh-credit-cards-bars-onboarding-of-new-online-customers>. All India Radio News (Prasar Bharati). **Reported**, accessed 29 September 2026.

Supports: On 24 April 2024 RBI directed Kotak Mahindra Bank to stop onboarding new customers through online and mobile channels and to stop issuing new credit cards, citing concerns from its IT examinations of the bank for 2022 and 2023 (as of 24 April 2024).

15. **RBI restricts Mastercard from onboarding new domestic customers** https://www.business-standard.com/article/finance/rbi-restricts-mastercard-from-onboarding-new-domestic-customers-121071400974_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: RBI barred Mastercard from onboarding new domestic card customers from 22 July 2021 for not complying with the payment data storage directions (as of 14 July 2021).

16. **RBI bars Mastercard from adding new clients in India** <https://www.tribuneindia.com/news/business/rbi-bars-mastercard-from-adding-new-clients-in-india-283510>. The Tribune. **Reported**, accessed 29 September 2026.

Supports: RBI had earlier restricted American Express and Diners Club from onboarding new domestic customers from 1 May 2021 on the same grounds (as of 14 July 2021).

17. **Restrictions on Mastercard lifted (press release)** https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53877. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI lifted the restriction on Mastercard in June 2022 after satisfactory compliance with the data storage directions (as of 16 June 2022).

18. **Reserve Bank issues draft Regulatory Principles for Management of Model Risks** https://www.business-standard.com/markets/capital-market-news/reserve-bank-issues-draft-regulatory-principles-for-management-of-model-risks-in-credit-126062500401_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: On 24 June 2026 RBI released draft guidance on model risk management across the model lifecycle, including models that use AI and machine learning, for public comment (as of 25 June 2026).

19. **National Payments Corporation of India: rating rationale** <https://www.icra.in/Rating/GetRationalReportFilePdf?id=135865>. ICRA. **Analyst**, accessed 29 September 2026.

Supports: RBI classified NPCI as a system-wide important payment system in June 2020 (as of 30 June 2025); NPCI was incorporated in December 2008 as a not-for-profit company, an initiative of RBI and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007 (as of 30 June 2025).

Chapter 29

RBI ecosystem

The institutions around RBI that build and run India's banking infrastructure. Only five are owned by RBI; others were set up by it or belong to the Government. Each page gives sourced facts.

The final chapter describes the institutions around the Reserve Bank, what each one does and how they connect.

Three kinds of relationship with RBI

Earlier descriptions often called all of these bodies “RBI subsidiaries”. The sources show three different relationships:

- **Wholly owned by RBI.** DICGC, BRBNMPL, ReBIT, IFTAS and RBIH are companies that RBI owns outright. DICGC is a wholly owned subsidiary of RBI, governed by the DICGC Act, 1961.¹
- **Set up by RBI or at its instance, but not owned by it.** IDRBT is a society RBI established. NPCI and CCIL were created at RBI’s initiative but are owned by banks and financial institutions. NPCI was incorporated in December 2008 as a not-for-profit company, an initiative of RBI and the Indian Banks’ Association under the Payment and Settlement Systems Act, 2007.⁷
- **Owned by the Government of India.** NABARD and NHB were once held by RBI, which sold its stakes by 2019, and CERSAI is a Government company. RBI sold its remaining stakes in NABARD (26 February 2019) and NHB (19 March 2019); the Government of India now owns 100% of both.⁹ CERSAI is a Government company, licensed under section 25 of the Companies Act, 1956, set up to run the central registry under the SARFAESI Act; the registry became operational on 31 March 2011.¹⁰

Employee numbers appear only where an official source gives them. Where none was found, the page says so rather than estimating.

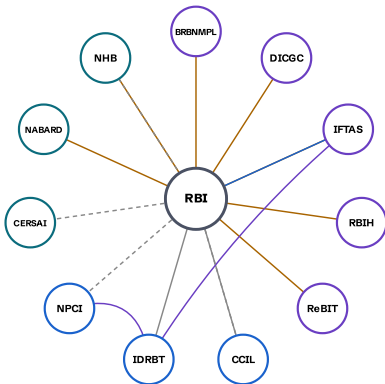
Relationship map

The map shows every sourced relationship; the table after it lists each one, generated from the same data. Colours show the kind of relationship with RBI.

Wholly owned by RBI

Set up by RBI or at its instance, not owned by RBI

Owned by the Government of India



Ownership Founding Operational Infrastructure - - - Regulatory

Every sourced relationship between the institutions

From	To	Type	Relationship
RBI	DICGC	ownership	Wholly owned subsidiary
RBI	BRBNMPL	ownership	Wholly owned subsidiary
RBI	ReBIT	ownership	Wholly owned subsidiary
RBI	IFTAS	ownership	Wholly owned subsidiary
RBI	RBIH	ownership	Wholly owned subsidiary
RBI	IDRBT	founding	Established IDRBT (1996)
RBI	CCIL	founding	Set up at RBI's behest (2001)
IDRBT	IFTAS	operational	Handed over INFINET, SFMS, RTGS and NEFT systems (2015)
IDRBT	NPCI	operational	Handed over the National Financial Switch (2009)
IFTAS	RBI	infrastructure	Network and messaging for RTGS and NEFT
RBI	NPCI	regulatory	Authorises NPCI's payment systems
RBI	CCIL	regulatory	Authorises CCIL as a central counterparty
RBI	NABARD	ownership	Former owner (stake sold by 2019)
RBI	NHB	ownership	Former owner (stake sold in 2019)
NHB	RBI	regulatory	Housing finance regulation moved to RBI (2019)
RBI	CERSAI	regulatory	RBI circulars point lenders to CERSAI's registry

The institutions compared

Institutions in the RBI ecosystem

Institution	Relationship with RBI	Headquarters	Established	Employees
BRBNMPL (chapter 29)	Wholly owned by RBI	Bengaluru	1995	No official figure found
DICGC (chapter 29)	Wholly owned by RBI	Mumbai	1978	No official figure found
IFTAS (chapter 29)	Wholly owned by RBI	Not confirmed	Not confirmed	No official figure found
RBIH (chapter 29)	Wholly owned by RBI	Bengaluru	2022	No official figure found
ReBIT (chapter 29)	Wholly owned by RBI	Not confirmed	Not confirmed	No official figure found
CCIL (chapter 29)	Set up by RBI or at its instance, not owned by RBI	Mumbai	2001	No official figure found
IDRBT (chapter 29)	Set up by RBI or at its instance, not owned by RBI	Hyderabad	1996	No official figure found
NPCI (chapter 29)	Set up by RBI or at its instance, not owned by RBI	Mumbai	2008	No official figure found
CERSAI (chapter 29)	Owned by the Government of India	Not confirmed	2011	No official figure found
NABARD (chapter 29)	Owned by the Government of India	Mumbai	1982	3,134 (as of 31 March 2024, National Bank for Agriculture and Rural Development)
NHB (chapter 29)	Owned by the Government of India	New Delhi	1988	No official figure found

Each institution's page lists the sources for its record. 'Not confirmed' means no official source was found yet.

Deposit Insurance and Credit Guarantee Corporation

At a glance

Wholly owned by RBI

Short name	DICGC
Legal form	Wholly owned subsidiary of RBI, established under the DICGC Act, 1961
Headquarters	Mumbai
Established	1978 Formed in 1978 by merging the Deposit Insurance Corporation (operating since 1 January 1962) with the Credit Guarantee Corporation of India .
Employees	No official figure found in the sources checked
Official site	www.dicgc.org.in

Roles

- Insures bank deposits up to ₹5 lakh per depositor per bank
- Pays depositors when an insured bank fails or is placed under restrictions
- Collects deposit insurance premiums from banks (risk-based from 2026)

What it does

The Deposit Insurance and Credit Guarantee Corporation protects depositors if a bank fails. DICGC insures deposits up to ₹5 lakh per depositor per bank, covering principal and interest.² DICGC is a wholly owned subsidiary of RBI, governed by the DICGC Act, 1961.¹ DICGC's head office is in Mumbai; deposit insurance in India began on 1 January 1962.³

How it works with banks

Insured banks pay DICGC a premium on their assessable deposits. DICGC's risk-based premium framework, released on 6 February 2026, replaces the flat premium of 12 paise per ₹100 of assessable deposits.⁴ For a bank's technology teams, deposit insurance matters mainly through data: a bank must be able to produce accurate, depositor-level records quickly, so that claims can be paid if it is ever needed.

Connections

- RBI: RBI owns all of DICGC.¹

Sources for this profile

1. **DICGC Information Leaflet** https://dicgc.org.in/sites/default/files/2024-10/DICGC_Information_Leaflet.pdf. Deposit Insurance and Credit Guarantee Corporation. **Primary source**, accessed 29 September 2026.
Supports: DICGC is a wholly owned subsidiary of RBI, governed by the DICGC Act, 1961 (as of 29 September 2026).
2. **A Guide to Deposit Insurance** <https://www.dicgc.org.in/guide-to-deposit-insurance>. Deposit Insurance and Credit Guarantee Corporation. **Primary source**, accessed 29 September 2026.
Supports: DICGC insures deposits up to ₹5 lakh per depositor per bank, covering principal and interest (as of 29 September 2026).
3. **History of DICGC** <https://www.dicgc.org.in/node/17>. Deposit Insurance and Credit Guarantee Corporation. **Primary source**, accessed 29 September 2026.
Supports: DICGC's head office is in Mumbai; deposit insurance in India began on 1 January 1962 (as of 29 September 2026).
4. **RBI's risk-based premium framework for deposit insurance to enhance profitability of stronger banks** <https://www.icra.in/Research/ViewResearchReport/rbi-s-risk-based-premium-framework-for-deposit-insurance-to-enhance-profitability-of-stronger-banks/6780>. ICRA. **Analyst**, accessed 29 September 2026.
Supports: DICGC's risk-based premium framework, released on 6 February 2026, replaces the flat premium of 12 paise per ₹100 of assessable deposits (as of 19 February 2026).

Bharatiya Reserve Bank Note Mudran Private Limited

At a glance

Wholly owned by RBI

Short name	BRBNMPL
Legal form	Wholly owned subsidiary of RBI (private limited company)
Headquarters	Bengaluru
Established	1995
Employees	No official figure found in the sources checked
Official site	www.brbnmpl.co.in

Roles

- Prints banknotes for RBI at presses in Mysuru and Salboni
- Runs a security ink unit and a banknote paper joint venture

What it does

Bharatiya Reserve Bank Note Mudran prints banknotes for RBI. BRBNMPL was established by RBI as a wholly owned subsidiary on 3 February 1995, with its registered and corporate office in Bengaluru.¹ BRBNMPL's two presses, at Mysuru and Salboni, can print 16 billion notes a year on a two-shift basis.¹

Why it belongs here

BRBNMPL is part of the currency side of RBI rather than digital payments, and it is included because it is one of RBI's wholly owned subsidiaries. Its connection to banking technology is indirect: cash still moves through branches, ATMs and currency chests that banks run.

Connections

- RBI: RBI owns all of BRBNMPL.¹

Sources for this profile

1. **Company Profile** <https://www.brbnmpl.co.in/company-profile/>. Bharatiya Reserve Bank Note Mudran Private Limited. **Primary source**, accessed 29 September 2026.

Supports: BRBNMPL was established by RBI as a wholly owned subsidiary on 3 February 1995, with its registered and corporate office in Bengaluru (as of 29 September 2026); BRBNMPL's two presses, at Mysuru and Salboni, can print 16 billion notes a year on a two-shift basis (as of 29 September 2026).

Reserve Bank Information Technology Private Limited

At a glance

Wholly owned by RBI

Short name	ReBIT
Legal form	Wholly owned subsidiary of RBI (private limited company)
Headquarters	Not confirmed from an official source
Established	Not confirmed Reported as 2016 ; not yet confirmed from an official source . RBI was recruiting for ReBIT by January 2017 .
Employees	No official figure found in the sources checked
Official site	rebit.org.in

Roles

- Delivers and manages RBI's IT projects
- Supports RBI's risk-based supervision through security audits and incident analysis
- Works to improve the cyber resilience of the banking sector

What it does

Reserve Bank Information Technology supports RBI's own technology and the sector's cyber resilience. ReBIT is a wholly owned subsidiary of RBI set up to serve RBI's IT and cyber security needs and improve the cyber resilience of Indian banking. ¹

Its public role

Much of ReBIT's work is internal to RBI, but it also publishes technical standards the wider ecosystem builds against. Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT. ² Its headquarters and founding year could not be confirmed from an official source, so they are shown as not confirmed.

Connections

- RBI: RBI owns all of ReBIT. ¹

Sources for this profile

1. **Chief Executive Officer (CEO) for Reserve Bank Information Technology Pvt. Ltd. (ReBIT)** https://opportunities.rbi.org.in/Scripts/bs_viewcontent.aspx?id=4187. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: ReBIT is a wholly owned subsidiary of RBI set up to serve RBI's IT and cyber security needs and improve the cyber resilience of Indian banking (as of 20 September 2022).

2. **Consultation paper on Financial Information Users in the securities markets under the Account Aggregator framework** https://www.sebi.gov.in/sebi_data/attachdocs/aug-2023/1690887848711.pdf. Securities and Exchange Board of India. **Primary source**, accessed 29 September 2026.

Supports: Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT (as of 1 August 2023).

Indian Financial Technology and Allied Services

At a glance

Wholly owned by RBI

Short name	IFTAS
Legal form	Wholly owned subsidiary of RBI (company under the Companies Act, 2013)
Headquarters	Not confirmed from an official source
Established	Not confirmed Took over INFINET, SFMS, the RTGS and NEFT systems and IBCC from IDRBT in February 2015; transferred to RBI in 2019.
Employees	No official figure found in the sources checked
Official site	www.iftas.in

Roles

- Runs INFINET, the closed network of the banking sector
- Runs SFMS, the messaging system behind RTGS and NEFT
- Runs the Indian Banking Community Cloud and the GIFT payment system

What it does

Indian Financial Technology and Allied Services runs the network and messaging layers that RBI's payment systems depend on. IFTAS is a wholly owned subsidiary of RBI, registered under the Companies Act, 2013; it runs INFINET, SFMS, the Indian Banking Community Cloud and GIFT.¹

Where its systems came from

IFTAS took over systems originally built at IDRBT. IDRBT transferred INFINET, SFMS, the RTGS and NEFT systems and its banking community cloud to its subsidiary IFTAS in February 2015; IFTAS was transferred to RBI in 2019.² IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS.² SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities.²

Why banks care

Every bank that sends RTGS or NEFT payments connects through this infrastructure, so its availability matters to the whole system. Smaller banks may also use its shared platform: IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.¹

Connections

- RBI: RBI owns all of IFTAS.¹
- IDRBT (chapter 29): IDRBT transferred these systems to its subsidiary IFTAS in February 2015; IFTAS moved to RBI in 2019.²
- RBI: SFMS and INFINET, run by IFTAS, carry the messages of RBI-operated RTGS and NEFT.¹

Sources for this profile

1. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: IFTAS is a wholly owned subsidiary of RBI, registered under the Companies Act, 2013; it runs INFINET, SFMS, the Indian Banking Community Cloud and GIFT (as of 20 September 2022); IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services (as of 20 September 2022).

2. **About IDRBT** <https://www.idrbt.ac.in/about-idrbt>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.

29 RBI ecosystem

Supports: IDRBT transferred INFINET, SFMS, the RTGS and NEFT systems and its banking community cloud to its subsidiary IFTAS in February 2015; IFTAS was transferred to RBI in 2019 (as of 1 January 2025); IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS (as of 1 January 2025); SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities (as of 1 January 2025).

Reserve Bank Innovation Hub

At a glance

Wholly owned by RBI

Short name	RBIH
Legal form	Wholly owned subsidiary of RBI (Section 8 not-for-profit company)
Headquarters	Bengaluru
Established	2022 Inaugurated on 24 March 2022; its company registration number indicates incorporation in 2021.
Employees	No official figure found in the sources checked
Official site	rbihub.in

Roles

- Promotes innovation in financial services, with a focus on low-income users
- Builds the Unified Lending Interface (ULI)
- Built MuleHunter.ai for detecting mule accounts

What it does

The Reserve Bank Innovation Hub promotes innovation in financial services. RBI set up the Reserve Bank Innovation Hub as a Section 8 company with ₹100 crore of initial capital; it was inaugurated in Bengaluru on 24 March 2022.¹ The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai.²

Why it matters to banks

The Unified Lending Interface is intended to connect lenders to the data they need for credit decisions through one platform, rather than many separate integrations. MuleHunter.ai addresses a fraud problem every bank shares: accounts used to receive and move stolen money.

Connections

- RBI: RBI owns all of RBIH.²

Sources for this profile

1. **Inauguration of the Reserve Bank Innovation Hub (Press Release 2021-2022/1903)** https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53458. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI set up the Reserve Bank Innovation Hub as a Section 8 company with ₹100 crore of initial capital; it was inaugurated in Bengaluru on 24 March 2022 (as of 24 March 2022).
2. **Reserve Bank Innovation Hub** <https://rbihub.in/>. Reserve Bank Innovation Hub. **Primary source**, accessed 29 September 2026.
Supports: The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai (as of 29 September 2026).

Institute for Development and Research in Banking Technology

At a glance

Set up by RBI or at its instance, not owned by RBI

Short name	IDRBT
Legal form	Society established by RBI (not a company and not RBI-owned)
Headquarters	Hyderabad
Established	1996
Employees	No official figure found in the sources checked
Official site	www.idrbt.ac.in

Roles

- Research, training and advisory work on banking technology
- Certifying authority for digital certificates in banking
- Built INFINET, SFMS and the National Financial Switch before handing them on

What it does

The Institute for Development and Research in Banking Technology works on research, training and advisory services in banking technology. IDRBT was established by RBI in March 1996 as a society under the Societies Registration Act.¹ IDRBT has worked from its premises at Castle Hills, Masab Tank, Hyderabad since 1 July 1996.² IDRBT is the certifying authority for digital certificates in the Indian banking and financial sector under the IT Act, 2000.¹

What it built

Much of India's interbank infrastructure began at IDRBT and was later handed to operators. IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS.¹ SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities.¹ NPCI took over operation of the National Financial Switch from IDRBT with effect from 14 December 2009, under an RBI authorisation.³ IDRBT transferred INFINET, SFMS, the RTGS and NEFT systems and its banking community cloud to its subsidiary IFTAS in February 2015; IFTAS was transferred to RBI in 2019.¹

A registered society

Earlier drafts of this site gave it university status. Its own description is of a society registered under the Societies Registration Act.

Connections

- RBI: RBI established IDRBT in March 1996 as a registered society.¹
- IFTAS (chapter 29): IDRBT transferred these systems to its subsidiary IFTAS in February 2015; IFTAS moved to RBI in 2019.¹
- NPCI (chapter 29): NPCI took over NFS operations from IDRBT with effect from 14 December 2009.³

Sources for this profile

1. **About IDRBT** <https://www.idrbt.ac.in/about-idrbt>, Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.

Supports: IDRBT was established by RBI in March 1996 as a society under the Societies Registration Act (as of 1 January 2025); IDRBT is the certifying authority for digital certificates in the Indian banking and financial sector under the IT Act, 2000 (as of 1 January 2025); IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS (as of 1 January 2025); SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and

delivery-versus-payment settlement of government securities (as of 1 January 2025); IDRBT transferred INFINET, SFMS, the RTGS and NEFT systems and its banking community cloud to its subsidiary IFTAS in February 2015; IFTAS was transferred to RBI in 2019 (as of 1 January 2025).

2. **Milestones 1994-1998** <https://www.idrbt.ac.in/?p=34318>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.

Supports: IDRBT has worked from its premises at Castle Hills, Masab Tank, Hyderabad since 1 July 1996 (as of 1 January 2025).

3. **Takeover of NFS by NPCI from IDRBT (NPCI/NFS/OC No.1)** <https://www.npci.org.in/PDF/nfs/circular/2009-10/NFS-OC-1-Takeover-of-NFS-by-NPCI-from-IDRBT.pdf>. National Payments Corporation of India. **Primary source**, accessed 29 September 2026.

Supports: NPCI took over operation of the National Financial Switch from IDRBT with effect from 14 December 2009, under an RBI authorisation (as of 18 December 2009).

National Payments Corporation of India

At a glance

Set up by RBI or at its instance, not owned by RBI

Short name	NPCI
Legal form	Not-for-profit company promoted by RBI and the Indian Banks' Association, owned by banks
Headquarters	Mumbai
Established	2008
Employees	No official figure found in the sources checked
Official site	www.npci.org.in

Roles

- Runs retail payment systems, including UPI and the National Financial Switch
- Operates under authorisation from RBI under the PSS Act, 2007

What it does

The National Payments Corporation of India runs most of India's retail payment systems. NPCI was incorporated in December 2008 as a not-for-profit company, an initiative of RBI and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007.¹ NPCI was promoted by 10 banks, and its shareholding was spread across 65 entities as of 31 May 2025.¹ RBI classified NPCI as a system-wide important payment system in June 2020.¹

Systems it runs

UPI is the best known. In August 2026 it processed 24.51 billion transactions⁴. NPCI also runs the switch that connects ATMs across banks, and it operates cheque clearing. NPCI took over operation of the National Financial Switch from IDRBT with effect from 14 December 2009, under an RBI authorisation.² RBI asked NPCI to build the Positive Pay facility into CTS and make it available to participant banks, and refers to the CTS grids that NPCI runs.³

Not an RBI subsidiary

NPCI was set up at the initiative of RBI and the Indian Banks' Association and is owned by banks. RBI authorises and oversees the systems it runs, but does not own it. This site does not describe NPCI's internal systems, which are not publicly documented.

Connections

- IDRBT (chapter 29): NPCI took over NFS operations from IDRBT with effect from 14 December 2009.²
- RBI: RBI authorises NPCI to operate payment systems under the Payment and Settlement Systems Act, 2007.²

Sources for this profile

1. **National Payments Corporation of India: rating rationale** <https://www.icra.in/Rating/GetRationalReportFilePdf?Id=135865>. ICRA. **Analyst**, accessed 29 September 2026.

Supports: NPCI was incorporated in December 2008 as a not-for-profit company, an initiative of RBI and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007 (as of 30 June 2025); NPCI was promoted by 10 banks, and its shareholding was spread across 65 entities as of 31 May 2025 (as of 31 May 2025); RBI classified NPCI as a system-wide important payment system in June 2020 (as of 30 June 2025).

2. **Takeover of NFS by NPCI from IDRBT (NPCI/NFS/OC No.1)** <https://www.npci.org.in/PDF/nfs/circular/2009-10/NFS-OC-1-Takeover-of-NFS-by-NPCI-from-IDRBT.pdf>. National Payments Corporation of India. **Primary source**, accessed 29 September 2026.

Supports: NPCI took over operation of the National Financial Switch from IDRBT with effect from 14 December 2009, under an RBI authorisation (as of 18 December 2009).

3. **Positive Pay System for Cheque Truncation System (RBI/2020-21/41)** <https://website.rbi.org.in/web/rbi/-/notifications/positive-pay-system-for-cheque-truncation-system-11969>, Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI asked NPCI to build the Positive Pay facility into CTS and make it available to participant banks, and refers to the CTS grids that NPCI runs (as of 25 September 2020).

4. **UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn** https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html. Business Standard. **Reported**, accessed 29 September 2026.

Supports: UPI processed 24.51 billion transactions worth ₹29.82 trillion in August 2026, its highest monthly volume to date (as of 31 August 2026).

The Clearing Corporation of India Limited

At a glance

Set up by RBI or at its instance, not owned by RBI

Short name	CCIL
Legal form	Financial market infrastructure set up at RBI's instance, owned by banks and financial institutions
Headquarters	Mumbai
Established	2001
Employees	No official figure found in the sources checked
Official site	www.ccilindia.com

Roles

- Central counterparty for government securities, money market, forex and rupee derivative trades
- Trade repository for over-the-counter derivatives

What it does

The Clearing Corporation of India stands between the two sides of trades in government securities, money markets, foreign exchange and rupee derivatives, so that each side's risk is on CCIL rather than on the other party. CCIL is a central counterparty authorised by RBI under the Payment and Settlement Systems Act, 2007.²

Who owns it

CCIL was set up in April 2001; a core committee appointed at RBI's behest chose SBI, IDBI Bank, ICICI Bank, LIC, Bank of Baroda and HDFC Bank as its core promoters.¹ CCIL's largest shareholders include SBI (16.8%), LIC (10%), STCI Finance (10%), ICICI Bank (9.9%) and HDFC Bank (9%).²

Why banks care

Banks' treasury systems send trades to CCIL for clearing and settlement, and its rules for margins and settlement timing shape how those systems are built.

Connections

- RBI: A core committee appointed at RBI's behest chose CCIL's promoter banks and institutions.¹
- RBI: CCIL is authorised by RBI under the Payment and Settlement Systems Act, 2007.²

Sources for this profile

1. **Promoters / Shareholders** <https://www.ccilindia.com/web/ccil/promoters-stakeholders>. The Clearing Corporation of India Limited. **Primary source**, accessed 29 September 2026.
Supports: CCIL was set up in April 2001; a core committee appointed at RBI's behest chose SBI, IDBI Bank, ICICI Bank, LIC, Bank of Baroda and HDFC Bank as its core promoters (as of 29 September 2026).
2. **The Clearing Corporation of India Limited (Revised): rating press release** https://www.careratings.com/upload/CompanyFiles/PR/202503120310_The_Clearing_Corporation_of_India_Limited.pdf. CARE Ratings. **Analyst**, accessed 29 September 2026.
Supports: CCIL's largest shareholders include SBI (16.8%), LIC (10%), STCI Finance (10%), ICICI Bank (9.9%) and HDFC Bank (9%) (as of 12 March 2025); CCIL is a central counterparty authorised by RBI under the Payment and Settlement Systems Act, 2007 (as of 12 March 2025).

National Bank for Agriculture and Rural Development

At a glance

Owned by the Government of India

Short name	NABARD
Legal form	Statutory development bank wholly owned by the Government of India; RBI's stake was sold in 2010 and 2019
Headquarters	Mumbai
Established	1982
Employees	3,134(as of 31 March 2024; National Bank for Agriculture and Rural Development, source 3)
Official site	www.nabard.org

Roles

- Refinances and develops rural credit, including cooperative banks and regional rural banks
- Supervises regional rural banks and state and district cooperative banks

What it does

The National Bank for Agriculture and Rural Development finances and supervises rural credit. NABARD was established on 12 July 1982 by an Act of Parliament and is wholly owned by the Government of India.¹ NABARD's head office is at Bandra-Kurla Complex, Mumbai.⁴

Ownership

NABARD was once majority-owned by RBI. RBI sold its remaining stakes in NABARD (26 February 2019) and NHB (19 March 2019); the Government of India now owns 100% of both.² Earlier drafts dated this change to 2023; the correct year is 2019.

Size

NABARD had 3,134 staff members as of 31 March 2024.³ Earlier drafts gave a figure of about 28,000, which has no official basis.

Connections

- RBI: RBI sold its last NABARD shares to the Government of India on 26 February 2019.²

Sources for this profile

1. **Citizen's Charter** <https://www.nabard.org/fitrcontent.aspx?id=492>. National Bank for Agriculture and Rural Development. **Primary source**, accessed 29 September 2026.
Supports: NABARD was established on 12 July 1982 by an Act of Parliament and is wholly owned by the Government of India (as of 31 March 2024).
2. **Reserve Bank of India divests its share in NABARD and NHB (Press Release 2018-2019/2528)** https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=46885. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI sold its remaining stakes in NABARD (26 February 2019) and NHB (19 March 2019); the Government of India now owns 100% of both (as of 24 April 2019).
3. **Annual Report 2023-24, chapter 9: People, Processes and Policies** <https://www.nabard.org/annual-report/people-processes-and-policies.html>. National Bank for Agriculture and Rural Development. **Primary source**, accessed 29 September 2026.
Supports: NABARD had 3,134 staff members as of 31 March 2024 (as of 31 March 2024).
4. **Standalone Financial Results for the quarter ended June 30, 2025** https://www.nabard.org/pdf/Financial%20Results_June-2025.pdf. National Bank for Agriculture and Rural Development. **Primary source**, accessed 29 September 2026.
Supports: NABARD's head office is at Bandra-Kurla Complex, Mumbai (as of 30 June 2025).

National Housing Bank

At a glance

Owned by the Government of India

Short name	NHB
Legal form	Statutory body wholly owned by the Government of India; RBI's stake was sold in 2019
Headquarters	New Delhi
Established	1988
Employees	No official figure found in the sources checked
Official site	nhb.org.in

Roles

- Finances and promotes housing finance institutions
- Supervises housing finance companies (regulation moved to RBI in 2019)

What it does

The National Housing Bank finances and promotes housing finance institutions. NHB was set up on 9 July 1988 under the National Housing Bank Act, 1987; its head office is in New Delhi.¹

Ownership and regulation

RBI sold its remaining stakes in NABARD (26 February 2019) and NHB (19 March 2019); the Government of India now owns 100% of both.² Its role changed in the same year: Regulation of housing finance companies moved from NHB to RBI with effect from 9 August 2019.¹

Connections

- RBI: RBI sold its entire NHB stake to the Government of India on 19 March 2019.²
- RBI: Regulation of housing finance companies moved from NHB to RBI from 9 August 2019; NHB still supervises them.¹

Sources for this profile

1. **About Us: Genesis** <https://nhb.org.in/about-us/>. National Housing Bank. **Primary source**, accessed 29 September 2026.

Supports: NHB was set up on 9 July 1988 under the National Housing Bank Act, 1987; its head office is in New Delhi (as of 29 September 2026); Regulation of housing finance companies moved from NHB to RBI with effect from 9 August 2019 (as of 29 September 2026).

2. **Reserve Bank of India divests its share in NABARD and NHB (Press Release 2018-2019/2528)** https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=46885. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Supports: RBI sold its remaining stakes in NABARD (26 February 2019) and NHB (19 March 2019); the Government of India now owns 100% of both (as of 24 April 2019).

Central Registry of Securitisation Asset Reconstruction and Security Interest of India

At a glance

Owned by the Government of India

Short name	CERSAI
Legal form	Government company set up by the Ministry of Finance (not RBI-promoted)
Headquarters	Not confirmed from an official source
Established	2011
Employees	No official figure found in the sources checked
Official site	www.cersai.org.in

Roles

- Runs the central registry of security interests under the SARFAESI Act, to stop multiple loans against the same property
- Acts as the Central KYC Records Registry (since 2016)

What it does

CERSAI keeps two national registries that banks rely on. The first records security interests, so a lender can check whether a property already secures another loan. CERSAI is a Government company, licensed under section 25 of the Companies Act, 1956, set up to run the central registry under the SARFAESI Act; the registry became operational on 31 March 2011.¹ The second holds central KYC records. The Government of India authorised CERSAI to act as the Central KYC Records Registry by notification S.O. 3183(E) of 26 November 2015; the registry went live on 15 July 2016.²

A Government company

Earlier drafts of this site said RBI had promoted it. RBI's own circular describes it as a Government company. It appears on this page because banks and other lenders regulated by RBI use its registries every day.

Connections

- RBI: RBI informed securitisation and reconstruction companies and cooperative banks about registering security interests with CERSAI.¹

Sources for this profile

1. **Setting up of Central Electronic Registry under the SARFAESI Act 2002 (RBI/2010-2011/545)** https://rbi.org.in/scripts/BS_NBFCNotificationView.aspx?id=6435. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: CERSAI is a Government company, licensed under section 25 of the Companies Act, 1956, set up to run the central registry under the SARFAESI Act; the registry became operational on 31 March 2011 (as of 25 May 2011).
2. **Amendment to Master Direction on KYC: Operationalisation of Central KYC Registry (RBI/2016-17/11)** <https://www.rbi.org.in/Scripts/NotificationUser.aspx?id=10498>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: The Government of India authorised CERSAI to act as the Central KYC Records Registry by notification S.O. 3183(E) of 26 November 2015; the registry went live on 15 July 2016 (as of 8 July 2016).

Notes

1. **DICGC Information Leaflet** https://dicgc.org.in/sites/default/files/2024-10/DICGC_Information_Leaflet.pdf. Deposit Insurance and Credit Guarantee Corporation. **Primary source**, accessed 29 September 2026.
Supports: DICGC is a wholly owned subsidiary of RBI, governed by the DICGC Act, 1961 (as of 29 September 2026).
2. **Chief Executive Officer (CEO) for Reserve Bank Information Technology Pvt. Ltd. (ReBIT)** https://opportunities.rbi.org.in/Scripts/bs_viewcontent.aspx?71d=4187. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

- Supports: ReBIT is a wholly owned subsidiary of RBI set up to serve RBI's IT and cyber security needs and improve the cyber resilience of Indian banking (as of 20 September 2022).
3. **Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS)** <https://website.rbi.org.in/web/rbi/-/chief-executive-office-r-ceo-for-indian-financial-technology-and-allied-services-iftas-1>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: IFTAS is a wholly owned subsidiary of RBI, registered under the Companies Act, 2013; it runs INFINET, SFMS, the Indian Banking Community Cloud and GIFT (as of 20 September 2022).
 4. **Reserve Bank Innovation Hub** <https://rbihub.in/>. Reserve Bank Innovation Hub. **Primary source**, accessed 29 September 2026.
Supports: The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai (as of 29 September 2026).
 5. **Company Profile** <https://www.brbtnmpl.co.in/company-profile/>. Bharatiya Reserve Bank Note Mudran Private Limited. **Primary source**, accessed 29 September 2026.
Supports: BRBN MPL was established by RBI as a wholly owned subsidiary on 3 February 1995, with its registered and corporate office in Bengaluru (as of 29 September 2026).
 6. **About IDRBT** <https://www.idrbt.ac.in/about-idrbt>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.
Supports: IDRBT was established by RBI in March 1996 as a society under the Societies Registration Act (as of 1 January 2025).
 7. **National Payments Corporation of India: rating rationale** <https://www.icra.in/Rating/GetRationalReportFilePdf?id=135865>. ICRA. **Analyst**, accessed 29 September 2026.
Supports: NPCI was incorporated in December 2008 as a not-for-profit company, an initiative of RBI and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007 (as of 30 June 2025).
 8. **Promoters / Shareholders** <https://www.ccilindia.com/web/ccil/promoters-stakeholders>. The Clearing Corporation of India Limited. **Primary source**, accessed 29 September 2026.
Supports: CCIL was set up in April 2001; a core committee appointed at RBI's behest chose SBI, IDBI Bank, ICICI Bank, LIC, Bank of Baroda and HDFC Bank as its core promoters (as of 29 September 2026).
 9. **Reserve Bank of India divests its share in NABARD and NHB (Press Release 2018-2019/2528)** https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=46885. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: RBI sold its remaining stakes in NABARD (26 February 2019) and NHB (19 March 2019); the Government of India now owns 100% of both (as of 24 April 2019).
 10. **Setting up of Central Electronic Registry under the SARFAESI Act 2002 (RBI/2010-2011/545)** https://rbi.org.in/scripts/BS_NBFCNotificationView.aspx?id=6435. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
Supports: CERSAI is a Government company, licensed under section 25 of the Companies Act, 1956, set up to run the central registry under the SARFAESI Act; the registry became operational on 31 March 2011 (as of 25 May 2011).
 11. **Takeover of NFS by NPCI from IDRBT (NPCI/NFS/OC No.1)** <https://www.npci.org.in/PDF/nfs/circular/2009-10/NFS-OC-1-Takeover-of-NFS-by-NPCI-from-IDRBT.pdf>. National Payments Corporation of India. **Primary source**, accessed 29 September 2026.
 12. **Availability of National Electronic Funds Transfer (NEFT) System on 24x7 basis (RBI/2019-20/111)** <https://www.rbi.org.in/scripts/NotificationUser.aspx?id=11750>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
 13. **History of DICGC** <https://www.dicgc.org.in/node/17>. Deposit Insurance and Credit Guarantee Corporation. **Primary source**, accessed 29 September 2026.
 14. **A Guide to Deposit Insurance** <https://www.dicgc.org.in/guide-to-deposit-insurance>. Deposit Insurance and Credit Guarantee Corporation. **Primary source**, accessed 29 September 2026.
 15. **RBI's risk-based premium framework for deposit insurance to enhance profitability of stronger banks** <https://www.icra.in/Research/ViewResearchReport/rbi-s-risk-based-premium-framework-for-deposit-insurance-to-enhance-profitability-of-stronger-banks/6780>. ICRA. **Analyst**, accessed 29 September 2026.
 16. **Inauguration of the Reserve Bank Innovation Hub (Press Release 2021-2022/1903)** https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53458. Reserve Bank of India. **Primary source**, accessed 29 September 2026.
 17. **Milestones 1994-1998** <https://www.idrbt.ac.in/?p=34318>. Institute for Development and Research in Banking Technology. **Primary source**, accessed 29 September 2026.
 18. **The Clearing Corporation of India Limited (Revised): rating press release** https://www.careratings.com/upload/CompanyFiles/PR/202503120310_The_Clearing_Corporation_of_India_Limited.pdf. CARE Ratings. **Analyst**, accessed 29 September 2026.
 19. **Annual Report 2023-24, chapter 9: People, Processes and Policies** <https://www.nabard.org/annual-report/people-processes-and-policies.html>. National Bank for Agriculture and Rural Development. **Primary source**, accessed 29 September 2026.
 20. **Standalone Financial Results for the quarter ended June 30, 2025** https://www.nabard.org/pdf/Financia%20Results_June-2025.pdf. National Bank for Agriculture and Rural Development. **Primary source**, accessed 29 September 2026.
 21. **Citizen's Charter** <https://www.nabard.org/ftrcontent.aspx?id=492>. National Bank for Agriculture and Rural Development. **Primary source**, accessed 29 September 2026.
 22. **About Us: Genesis** <https://nhb.org.in/about-us/>. National Housing Bank. **Primary source**, accessed 29 September 2026.
 23. **Amendment to Master Direction on KYC: Operationalisation of Central KYC Registry (RBI/2016-17/11)** <https://www.rbi.org.in/Scripts/NotificationUser.aspx?id=10498>. Reserve Bank of India. **Primary source**, accessed 29 September 2026.

Appendix A

Glossary of short names

*129 short names used in this book. 25 definitions have been checked against a cited source; the rest are marked **unsourced** and are still being sourced.*

AA

Account Aggregator. An RBI-licensed firm that moves a customer's financial data between institutions only with the customer's consent. It does not store the data. **unsourced**

AML

Anti-money laundering. The controls, monitoring and reporting that stop criminals using banks to disguise illegal money. **unsourced**

APB

Aadhaar Payment Bridge. NPCI's system for sending government benefit payments to bank accounts linked to the recipient's Aadhaar number. **unsourced**

API

Application programming interface. A defined way for one system to request data or actions from another. **unsourced**

AUA

Authentication User Agency. An organisation permitted by UIDAI to use Aadhaar authentication to verify its customers. **unsourced**

AutoPay

UPI AutoPay. The UPI feature for recurring payments under a mandate the customer approves once, such as subscriptions or instalments. **unsourced**

BBPS

Bharat Bill Payment System. An interoperable system for paying utility and other recurring bills through many channels. **unsourced**

BCP

Business continuity plan. The plan for keeping critical services running, or restoring them, during a disruption. **unsourced**

BFF

Backend for frontend. A server layer built for one client, such as a mobile app, that shapes data from many services for that client. **unsourced**

BHIM

Bharat Interface for Money. NPCI's own UPI app. **unsourced**

BOD

Beginning of day. The batch run that opens a new business date in a core banking system after end of day. **unsourced**

BRBNMPL

Bharatiya Reserve Bank Note Mudran Private Limited. A wholly owned subsidiary of RBI that prints banknotes at presses in Mysuru and Salboni.

CASA

Current account and savings account. Deposits in current and savings accounts, a low-cost source of funds for banks. **unsourced**

CBDC

Central bank digital currency. Digital money issued by a central bank. RBI's version is the e-rupee. **unsourced**

CBS

Core banking system. The central system of record for a bank's customers, accounts, deposits, loans and general ledger. **unsourced**

CCIL

The Clearing Corporation of India Limited. The central counterparty for India's government securities, money market, forex and rupee derivative trades, authorised by RBI.

CDC

Change data capture. Streaming every change made to a database so other systems can react to it or keep a copy up to date. **unsourced**

CERSAI

Central Registry of Securitisation Asset Reconstruction and Security Interest of India. A Government company that runs the central registry of security interests, so lenders can check whether a property already secures a loan.

CERT-In

Indian Computer Emergency Response Team. India's national agency for responding to cyber security incidents. Organisations, including banks, must report certain incidents to it.

CFT

Countering the financing of terrorism. Controls that stop money reaching terrorist groups, usually run alongside anti-money-laundering controls. **unsourced**

CI/CD

Continuous integration and continuous delivery. Automatically building and testing every change, and releasing it through a repeatable pipeline. **unsourced**

CIC

Credit information company, or core investment company.

Usually a credit bureau licensed by RBI that holds borrowers' credit histories. In RBI rules it can also mean a core investment company, a type of NBFC. **unsourced**

Circular

Circular. An RBI instruction issued to the entities it regulates, such as banks. **unsourced**

CKYC

Central KYC. A shared record of a customer's KYC details that regulated entities can reuse instead of collecting documents again.

CKYCRR

Central KYC Records Registry. The registry of central KYC records. The Government of India authorised CERSAI to run it; it went live in July 2016.

CQRS

Command query responsibility segregation. A design that handles writes and reads with separate models, so each can be optimised on its own. **unsourced**

CRAR

Capital to risk-weighted assets ratio. A bank's capital as a share of its assets weighted by risk. RBI sets a minimum. **unsourced**

CRR

Cash reserve ratio. The share of deposits a bank must keep as a balance with RBI. **unsourced**

CSPM

Cloud security posture management. Tools that continuously check cloud accounts for risky settings and policy violations. **unsourced**

CTR

Cash transaction report. A report of large cash transactions that a bank files with FIU-IND under the PMLA rules. **unsourced**

CTS

Cheque Truncation System. The system that clears cheques using scanned images instead of moving paper. Since October 2025 it clears continuously through the day.

DC

Data centre. A facility that houses servers, storage and networking equipment. [unsourced](#)

DCCB

District central co-operative bank. A co-operative bank at district level that lends to primary agricultural credit societies. [unsourced](#)

DICGC

Deposit Insurance and Credit Guarantee Corporation. A wholly owned subsidiary of RBI that insures bank deposits, currently up to ₹5 lakh per depositor per bank.

DLP

Data loss prevention. Controls that detect and stop sensitive data leaving an organisation by email, upload or device. [unsourced](#)

DPDP Act

Digital Personal Data Protection Act, 2023. India's law on the processing of digital personal data, including consent and the duties of organisations that hold such data. [unsourced](#)

DR

Disaster recovery. The plans and systems for restoring service at another site after a major failure. [unsourced](#)

EDW

Enterprise data warehouse. A central store of cleaned, integrated data used for reporting and analysis across an organisation. [unsourced](#)

eKYC

Electronic KYC. KYC completed by fetching identity details from UIDAI through Aadhaar authentication, with the customer's consent. [unsourced](#)

EOD

End of day. The daily batch run in a core banking system that closes the business day: interest accrual, charges, ledger posting and reports. [unsourced](#)

ESB

Enterprise service bus. Middleware that connects many applications through a central hub, often translating messages between them. [unsourced](#)

ETL

Extract, transform, load. Moving data from source systems, reshaping it and loading it into a warehouse or other store. [unsourced](#)

FIP

Financial information provider. In the Account Aggregator system, an institution that holds a customer's data, such as a bank, and shares it on consent. [unsourced](#)

FIU

Financial information user. In the Account Aggregator system, an institution that asks for a customer's data with consent, such as a lender. Not the same as FIU-IND. [unsourced](#)

FIU-IND

Financial Intelligence Unit – India. The national agency that receives, analyses and shares reports of suspicious and large transactions under the PMLA. Not the same as FIU, a financial information user. [unsourced](#)

FSDC

Financial Stability and Development Council. A council chaired by the Finance Minister that brings together India's financial regulators on stability and coordination. [unsourced](#)

GitOps

GitOps. Running systems so that a Git repository holds the desired state, and automation keeps the live system matched to it. [unsourced](#)

GL

General ledger. The bank's master set of accounts, where every transaction is recorded as debits and credits. [unsourced](#)

HSM

Hardware security module. A tamper-resistant device that stores cryptographic keys and performs operations such as PIN verification. [unsourced](#)

IaC

Infrastructure as code. Defining servers, networks and other infrastructure in version-controlled files instead of setting them up by hand. [unsourced](#)

IBA

Indian Banks' Association. An association of banks in India. With RBI, it set up NPCI.

IDRBT

Institute for Development and Research in Banking

Technology. A society set up by RBI in 1996 in Hyderabad for research and training in banking technology. It built INFINET, SFMS and the National Financial Switch.

IFSC

Indian Financial System Code. An 11-character code that identifies a bank branch for NEFT, RTGS and IMPS transfers. [unsourced](#)

IFTAS

Indian Financial Technology and Allied Services. A wholly owned subsidiary of RBI that runs INFINET, the banking sector's private network, and SFMS, the messaging system behind RTGS and NEFT.

IMPS

Immediate Payment Service. NPCI's instant, round-the-clock interbank transfer service, used with an account number and IFSC or with a mobile number. [unsourced](#)

INFINET

Indian Financial Network. The closed, private network of the banking sector, launched in 1999 and now run by IFTAS.

IRDAI

Insurance Regulatory and Development Authority of India. The regulator of India's insurance sector. [unsourced](#)

ISO 20022

ISO 20022. An international standard for richly structured financial messages, increasingly used for high-value and cross-border payments. [unsourced](#)

ISO 8583

ISO 8583. An international standard for card and similar transaction messages, used by card networks and ATM switches. [unsourced](#)

IT Act

Information Technology Act, 2000. India's main law on electronic records, digital signatures and cyber offences. [unsourced](#)

JIT access

Just-in-time access. Granting elevated access only when needed and only for a short time, instead of permanently. [unsourced](#)

K8s

Kubernetes. An open-source system for running and scaling containerised applications across a cluster of machines. [unsourced](#)

KMM

Kotlin Multiplatform Mobile. A way to share Kotlin code between Android and iOS apps, now called Kotlin Multiplatform. [unsourced](#)

KUA

e-KYC User Agency. An organisation permitted by UIDAI to receive Aadhaar e-KYC data for its customers. [unsourced](#)

KYC

Know your customer. The process of verifying a customer's identity and address, required before a bank or other regulated entity opens an account. [unsourced](#)

LAF

Liquidity adjustment facility. RBI's operations that lend to or absorb money from banks for short periods to steer short-term interest rates. [unsourced](#)

LLM

Large language model. A machine learning model trained on large amounts of text that can generate and interpret language. [unsourced](#)

Master Circular

Master Circular. An RBI document that consolidates its circulars on a subject as of a date. [unsourced](#)

Master Direction

Master Direction. An RBI instrument that sets out all its rules on a subject in one place, updated whenever the rules change.

MeitY

Ministry of Electronics and Information Technology. The ministry responsible for the IT Act and the Digital Personal Data Protection Act. [unsourced](#)

MICR

Magnetic Ink Character Recognition. The machine-readable line printed on a cheque that identifies the bank, branch and cheque number. [unsourced](#)

MLOps

Machine learning operations. Practices for deploying, monitoring and updating machine learning models reliably in production. [unsourced](#)

MMID

Mobile Money Identifier. A seven-digit number that, with a mobile number, identifies a bank account for IMPS transfers. [unsourced](#)

MSF

Marginal standing facility. An RBI window where banks can borrow overnight against government securities at a penal rate when other sources dry up. [unsourced](#)

mTLS

Mutual TLS. TLS in which both sides present certificates, so each proves its identity to the other. [unsourced](#)

NABARD

National Bank for Agriculture and Rural Development. A statutory development bank for agriculture and rural credit, wholly owned by the Government of India since RBI sold its last shares in 2019.

NACH

National Automated Clearing House. NPCI's system for bulk and recurring payments, such as salaries, dividends and loan instalments collected under a mandate. [unsourced](#)

NEFT

National Electronic Funds Transfer. RBI's account-to-account transfer system. It settles in half-hourly batches, around the clock, in banks' accounts at RBI.

NETC

National Electronic Toll Collection. NPCI's system for electronic toll payments using FASTag stickers on vehicles. [unsourced](#)

NFS

National Financial Switch. The network that lets a card from one bank work at another bank's ATM. Built by IDRBT, it has been run by NPCI since December 2009.

NHB

National Housing Bank. A statutory body, wholly owned by the Government of India, that finances and promotes housing finance institutions and supervises housing finance companies.

Notification

Notification. A formal RBI publication that issues or amends regulations and directions. [unsourced](#)

NPA

Non-performing asset. A loan on which interest or principal has stayed overdue beyond the period RBI sets. [unsourced](#)

NPCI

National Payments Corporation of India. A not-for-profit company set up in 2008 as an initiative of RBI and the Indian Banks' Association, owned by banks. It runs retail payment systems such as UPI and the National Financial Switch.

OLAP

Online analytical processing. Systems designed for analysing large volumes of data, such as reporting and dashboards. [unsourced](#)

OLTP

Online transaction processing. Systems that record many small transactions quickly and reliably, such as a core banking ledger. [unsourced](#)

PA

Payment aggregator. An RBI-authorised firm that collects payments on behalf of merchants and settles the money to them. [unsourced](#)

PAM

Privileged access management. Tools and controls that govern who can use powerful administrator accounts, and record what they do. [unsourced](#)

PCA

Prompt corrective action. RBI's framework that places restrictions on a weak bank until its capital, asset quality or profits recover. [unsourced](#)

PFRDA

Pension Fund Regulatory and Development Authority. The regulator of pension funds in India, including the National Pension System. [unsourced](#)

PG

Payment gateway. Technology that routes online payment details between the customer, merchant and banks. It does not hold the funds. [unsourced](#)

PMLA

Prevention of Money-laundering Act, 2002. The law that requires banks and other reporting entities to keep records and report certain transactions to FIU-IND. [unsourced](#)

PPI

Prepaid payment instrument. A stored-value product, such as a wallet or gift card, loaded in advance and used to pay. [unsourced](#)

PSL

Priority sector lending. RBI's requirement that banks direct a share of lending to sectors such as agriculture, small business and weaker sections. [unsourced](#)

PSP

Payment service provider. In UPI, a bank that offers UPI to its customers or to a third-party app. More generally, any firm that provides payment services. [unsourced](#)

PSS Act

Payment and Settlement Systems Act, 2007. The law under which RBI authorises and regulates payment systems in India.

QR

Quick Response code. A two-dimensional barcode. In Indian payments, a merchant QR code carries the details a UPI or card app needs to pay. [unsourced](#)

RBI

Reserve Bank of India. India's central bank. It regulates banks and payment systems, runs RTGS and NEFT, and holds the accounts in which banks settle with one another. [unsourced](#)

RBIIH

Reserve Bank Innovation Hub. A wholly owned, not-for-profit subsidiary of RBI in Bengaluru that promotes financial innovation. It builds the Unified Lending Interface.

ReBIT

Reserve Bank Information Technology Private Limited. A wholly owned subsidiary of RBI that handles RBI's IT projects and cyber security, and supports its supervision of banks through security audits.

RPO

Recovery point objective. The most data, measured in time, that an organisation is prepared to lose when a system fails.

unsourced

RRB

Regional rural bank. A bank set up to serve rural areas, jointly owned by the Government of India, a state government and a sponsor bank.

unsourced

RTGS

Real Time Gross Settlement. RBI's system that settles each payment individually and immediately, on a gross basis, between banks.

RTO

Recovery time objective. How quickly a system must be working again after a failure.

unsourced

RuPay

RuPay. India's domestic card network, run by NPCI, for debit, credit and prepaid cards.

unsourced

SEBI

Securities and Exchange Board of India. The regulator of India's securities markets, including stock exchanges, brokers, depositories and mutual funds.

unsourced

SFB

Small finance bank. A bank licensed by RBI to focus on small businesses, small farmers and others with limited access to banking.

unsourced

SFMS

Structured Financial Messaging System. The secure messaging system, launched in 2001 and now run by IFTAS, that carries RTGS, NEFT and government securities settlement messages.

SIEM

Security information and event management. A system that collects security logs from many sources and raises alerts on suspicious patterns.

unsourced

SLI

Service level indicator. The measurement used to judge a service against its objective, such as the share of successful payments.

unsourced

SLO

Service level objective. A target for how reliable or fast a service should be, measured over a period.

unsourced

SLR

Statutory liquidity ratio. The share of deposits a bank must hold in safe liquid assets such as government securities.

unsourced

SOAR

Security orchestration, automation and response. Tools that automate responses to security alerts, such as isolating a machine or blocking an address.

unsourced

StCB

State co-operative bank. The apex co-operative bank in a state, above the district central co-operative banks.

unsourced

STR

Suspicious transaction report. A report a bank files with FIU-IND when a transaction looks suspicious under the PMLA.

unsourced

SWIFT

Society for Worldwide Interbank Financial

Telecommunication. The global cooperative network banks use to exchange cross-border payment and other financial messages.

unsourced

TPAP

Third-party application provider. A UPI app run by a company that is not a bank. It connects to UPI through one or more partner banks that act as payment service providers.

unsourced

TPS

Transactions per second. A measure of how many transactions a system handles each second.

unsourced

TReDS

Trade Receivables Discounting System. RBI-authorised platforms where small businesses sell unpaid invoices owed by large buyers to financiers, to get paid sooner.

unsourced

TREPS

Tri-party Repo Dealing and Settlement. CCIL's platform for tri-party repo, a form of short-term borrowing against government securities.

UCB

Urban co-operative bank. A co-operative bank serving mainly urban and semi-urban areas.

unsourced

UIDAI

Unique Identification Authority of India. The authority that issues Aadhaar numbers and runs Aadhaar authentication and e-KYC.

unsourced

ULI

Unified Lending Interface. A platform built by the Reserve Bank Innovation Hub that connects lenders to the data they need to assess and process loans.

UPI

Unified Payments Interface. NPCI's real-time system for paying from a bank account with a UPI ID, QR code or phone number, through apps on a phone.

unsourced

UPI123PAY

UPI123PAY. UPI for feature phones, used through voice calls, missed calls, simple apps or sound-based payments.

unsourced

UPI Lite

UPI Lite. A small on-device balance for quick, low-value UPI payments without entering the UPI PIN each time. See NPCI for current limits.

unsourced

VKYC

Video KYC. Customer identification carried out over a live video call with an official of the regulated entity.

unsourced

VPA

Virtual payment address. A UPI ID, such as name@bank, that stands in for an account number and IFSC.

unsourced

WAF

Web application firewall. A filter in front of web applications that blocks common attacks on web traffic.

unsourced

Appendix B

Register of facts

Every figure, date, limit and named regulation in this book comes from one of these 116 records. Each was checked against the source named, which was opened and read. "As of" is the date the fact was true.

Fact	As of	Source	Type
No financial information is retrieved, shared or transferred through an Account Aggregator without the customer's explicit consent, and joining is voluntary.	29 September 2026	Department of Financial Services, Ministry of Finance	Official
Customer data passing through an Account Aggregator is not visible to, and does not reside with, the aggregator.	1 August 2023	Securities and Exchange Board of India	Official
RBI issued its Master Direction for Account Aggregators on 2 September 2016; an Account Aggregator must be a non-bank financial company registered with RBI.	6 September 2024	Reserve Bank of India	Official
RBI had earlier restricted American Express and Diners Club from onboarding new domestic customers from 1 May 2021 on the same grounds.	14 July 2021	The Tribune	Reported
RBI's Authentication Mechanisms for Digital Payment Transactions Directions, 2025, issued on 25 September 2025, require at least two factors of authentication for domestic digital payments, with compliance from 1 April 2026.	25 September 2025	The Tribune	Reported
Card issuers must be able to validate an additional authentication factor for non-recurring cross-border card-not-present transactions, when the overseas merchant asks, by 1 October 2026.	25 September 2025	The Tribune	Reported
Before issuing its 2025 authentication Directions, RBI published draft directions for comment on 31 July 2024 and 7 February 2025.	25 September 2025	Business Standard	Reported
For digital payments other than card-present transactions, at least one authentication factor must be dynamic, that is, unique to the transaction.	1 December 2025	KPMG in India	Reported
The 2025 authentication framework encourages new authentication factors but does not require banks to stop using SMS-based OTP.	25 September 2025	Business Standard	Reported
BRBNMPL was established by RBI as a wholly owned subsidiary on 3 February 1995, with its registered and corporate office in Bengaluru.	29 September 2026	Bharatiya Reserve Bank Note Mudran Private Limited	Official
BRBNMPLs two presses, at Mysuru and Salboni, can print 16 billion notes a year on a two-shift basis.	29 September 2026	Bharatiya Reserve Bank Note Mudran Private Limited	Official
CCIL was set up in April 2001; a core committee appointed at RBI's behest chose SBI, IDBI Bank, ICICI Bank, LIC, Bank of Baroda and HDFC Bank as its core promoters.	29 September 2026	The Clearing Corporation of India Limited	Official
CCIL is a central counterparty authorised by RBI under the Payment and Settlement Systems Act, 2007.	12 March 2025	CARE Ratings	Reported
CCIL's largest shareholders include SBI (16.8%), LIC (10%), STCI Finance (10%), ICICI Bank (9.9%) and HDFC Bank (9%).	12 March 2025	CARE Ratings	Reported
CERSAI is a Government company, licensed under section 25 of the Companies Act, 1956, set up to run the central registry under the SARFAESI Act; the registry became operational on 31 March 2011.	25 May 2011	Reserve Bank of India	Official
CERT-In's directions of 28 April 2022 under section 70B(6) of the IT Act require reportable cyber incidents to be reported to CERT-In within 6 hours of noticing them; they took effect 60 days after issue.	28 April 2022	CERT-In, Ministry of Electronics and Information Technology	Official
The same CERT-In directions require logs of all ICT systems to be kept securely for a rolling 180 days, within Indian jurisdiction.	28 April 2022	CERT-In, Ministry of Electronics and Information Technology	Official
The Government of India authorised CERSAI to act as the Central KYC Records Registry by notification S.O. 3183(E) of 26 November 2015; the registry went live on 15 July 2016.	8 July 2016	Reserve Bank of India	Official
As of 2026, AWS runs cloud regions in Mumbai and Hyderabad, Microsoft Azure in Pune, Chennai and Mumbai, Google Cloud in Mumbai and Delhi NCR, and Oracle Cloud in Mumbai and Hyderabad.	29 September 2026	Cloud Infrastructure Map	Reported
Since 1 October 2022, no entity in the card payment chain other than card issuers and card networks may store actual card data; merchants use tokens instead.	28 July 2022	Reserve Bank of India	Official
Under continuous clearing, CTS settles every hour from 11:00, based on positive confirmations and deemed approvals from drawee banks.	13 August 2025	Reserve Bank of India	Official

Indian Banking Ecosystem

Fact	As of	Source	Type
RBI moved the Cheque Truncation System from batch processing to continuous clearing with settlement on realisation; Phase 1 took effect on 4 October 2025.	24 December 2025	Reserve Bank of India	Official
RBI postponed Phase 2 of continuous cheque clearing, which had been planned for 3 January 2026, until further notice.	24 December 2025	Reserve Bank of India	Official
RBI set the CTS presentation session at 09:00 to 15:00 and the confirmation session at 09:00 to 19:00.	24 December 2025	Reserve Bank of India	Official
RBI's circular of 6 April 2018 requires payment system providers to store the entire data relating to their payment systems only in India; data on the foreign leg of a transaction may also be stored abroad.	6 April 2018	Reserve Bank of India	Official
DICGC insures deposits up to ₹5 lakh per depositor per bank, covering principal and interest.	29 September 2026	Deposit Insurance and Credit Guarantee Corporation	Official
DICGC's head office is in Mumbai; deposit insurance in India began on 1 January 1962.	29 September 2026	Deposit Insurance and Credit Guarantee Corporation	Official
DICGC's risk-based premium framework, released on 6 February 2026, replaces the flat premium of 12 paise per ₹100 of assessable deposits.	19 February 2026	ICRA	Reported
DICGC is a wholly owned subsidiary of RBI, governed by the DICGC Act, 1961.	29 September 2026	Deposit Insurance and Credit Guarantee Corporation	Official
MeltY notified the Digital Personal Data Protection Rules on 13 November 2025. Provisions on the Data Protection Board applied at once, consent-manager rules apply from 13 November 2026, and most obligations on organisations apply from 13 May 2027.	14 November 2025	S.S. Rana & Co.	Reported
EDB stated in 2019 that multiple Finacle modules had been migrated to EDB Postgres and implemented at financial institutions in Asia.	11 April 2019	EDB	Vendor claim
Finacle is developed by EdgeVerve Systems, a wholly owned subsidiary of Infosys, and marketed as Infosys Finacle.	31 August 2020	EdgeVerve Systems	Vendor claim
The vendor states that banks in over 100 countries use Finacle to serve more than a billion consumers and 1.3 billion accounts.	31 August 2020	EdgeVerve Systems	Vendor claim
An RBI committee's report on responsible AI in finance (FREE-AI), placed on RBI's website on 13 August 2025, sets out 7 guiding principles and 26 recommendations under six pillars.	13 August 2025	Reserve Bank of India	Official
In 2020 RBI placed similar restrictions on HDFC Bank, barring new digital business-generating launches and new credit card sourcing; they were lifted in 2022.	24 April 2024	Inc42	Reported
IFTAS's Indian Banking Community Cloud provides core banking and other applications, such as SFMS and mobile banking, as web services.	20 September 2022	Reserve Bank of India	Official
IDRBT is the certifying authority for digital certificates in the Indian banking and financial sector under the IT Act, 2000.	1 January 2025	Institute for Development and Research in Banking Technology	Official
IDRBT has worked from its premises at Castle Hills, Masab Tank, Hyderabad since 1 July 1996.	1 January 2025	Institute for Development and Research in Banking Technology	Official
IDRBT was established by RBI in March 1996 as a society under the Societies Registration Act.	1 January 2025	Institute for Development and Research in Banking Technology	Official
IDRBT transferred INFINET, SFMS, the RTGS and NEFT systems and its banking community cloud to its subsidiary IFTAS in February 2015; IFTAS was transferred to RBI in 2019.	1 January 2025	Institute for Development and Research in Banking Technology	Official
IFTAS is a wholly owned subsidiary of RBI, registered under the Companies Act, 2013; it runs INFINET, SFMS, the Indian Banking Community Cloud and GIFT.	20 September 2022	Reserve Bank of India	Official
IMPS processed 360 million transactions worth ₹7.04 trillion in August 2026.	31 August 2026	Business Standard	Reported
IDRBT launched INFINET, a closed user group network for banks, in June 1999; it now runs on MPLS.	1 January 2025	Institute for Development and Research in Banking Technology	Official
Regulated entities must back up data and periodically restore it to check that it is usable.	7 November 2023	Reserve Bank of India	Official
Configurations and security patches must be identical at the primary data centre and the DR site.	7 November 2023	Reserve Bank of India	Official
DR drills for critical information systems must be held at least every six months, and major issues found in a drill must be fixed and tested again before the next cycle.	7 November 2023	Reserve Bank of India	Official

Fact	As of	Source	Type
A DR test must switch over to the DR or alternate site and run it as the primary site long enough to cover at least a full working day, from beginning of day to end of day.	7 November 2023	Reserve Bank of India	Official
For critical information systems, regulated entities should prioritise a minimal RTO, approved by their IT Strategy Committee, and a near-zero RPO; with a non-zero RPO they need a documented method for reconciling data when resuming from the alternate site.	7 November 2023	Reserve Bank of India	Official
RBI requires regulated entities to define recovery metrics, including a recovery point objective (RPO) and recovery time objective (RTO), for all critical information systems.	7 November 2023	Reserve Bank of India	Official
On 24 April 2024 RBI directed Kotak Mahindra Bank to stop onboarding new customers through online and mobile channels and to stop issuing new credit cards, citing concerns from its IT examinations of the bank for 2022 and 2023.	24 April 2024	All India Radio News (Prasar Bharati)	Reported
RBI said it had found serious deficiencies in areas including IT inventory management, patch and change management, user access management, vendor risk management, data security and leak prevention, and business continuity and DR drills.	24 April 2024	The Federal	Reported
RBI lifted the restrictions on Kotak Mahindra Bank in February 2025, after an external audit and remedial measures.	12 February 2025	All India Radio News (Prasar Bharati)	Reported
RBI said the bank's core banking system and online channels had suffered frequent and significant outages over the previous two years, and that rapid growth in digital transactions was adding load on its IT systems.	24 April 2024	Inc42	Reported
RBI lifted the restriction on Mastercard in June 2022 after satisfactory compliance with the data storage directions.	16 June 2022	Reserve Bank of India	Official
RBI barred Mastercard from onboarding new domestic card customers from 22 July 2021 for not complying with the payment data storage directions.	14 July 2021	Business Standard	Reported
RBI's draft circular of 5 August 2024 on model risk in credit proposed a board-approved model risk policy, independent validation before deployment, and outcomes that are unbiased, explainable and verifiable.	5 August 2024	Lexology	Reported
On 24 June 2026 RBI released draft guidance on model risk management across the model lifecycle, including models that use AI and machine learning, for public comment.	25 June 2026	Business Standard	Reported
NABARD was established on 12 July 1982 by an Act of Parliament and is wholly owned by the Government of India.	31 March 2024	National Bank for Agriculture and Rural Development	Official
NABARD's head office is at Bandra-Kurla Complex, Mumbai.	30 June 2025	National Bank for Agriculture and Rural Development	Official
RBI sold its remaining stakes in NABARD (26 February 2019) and NHB (19 March 2019); the Government of India now owns 100% of both.	24 April 2019	Reserve Bank of India	Official
NABARD had 3,334 staff members as of 31 March 2024.	31 March 2024	National Bank for Agriculture and Rural Development	Official
NEFT has been available 24x7, on all days of the year including holidays, since 16 December 2019.	6 December 2019	Reserve Bank of India	Official
When NEFT moved to 24x7 in December 2019, RBI set 48 half-hourly settlement batches a day.	6 December 2019	Reserve Bank of India	Official
NEFT was launched in November 2005.	1 January 2025	Institute for Development and Research in Banking Technology	Official
A beneficiary bank must credit or return an NEFT transaction within 2 hours of the batch settling.	6 December 2019	Reserve Bank of India	Official
NEFT processes transactions received up to a set time in batches, while RTGS processes them continuously, one at a time.	29 September 2026	Reserve Bank of India	Official
The National Financial Switch connected 2.61 lakh ATMs of 1,317 member banks as of 31 July 2024.	31 July 2024	Institute for Development and Research in Banking Technology	Reported
NPCI took over operation of the National Financial Switch from IDRBT with effect from 14 December 2009, under an RBI authorisation.	18 December 2009	National Payments Corporation of India	Official
NHB was set up on 9 July 1988 under the National Housing Bank Act, 1987; its head office is in New Delhi.	29 September 2026	National Housing Bank	Official
Regulation of housing finance companies moved from NHB to RBI with effect from 9 August 2019.	29 September 2026	National Housing Bank	Official

Indian Banking Ecosystem

Fact	As of	Source	Type
NPCI was incorporated in December 2008 as a not-for-profit company, an initiative of RBI and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007.	30 June 2025	ICRA	Reported
RBI asked NPCI to build the Positive Pay facility into CTS and make it available to participant banks, and refers to the CTS grids that NPCI runs.	25 September 2020	Reserve Bank of India	Official
NPCI was promoted by 10 banks, and its shareholding was spread across 65 entities as of 31 May 2025.	31 May 2025	ICRA	Reported
RBI classified NPCI as a system-wide important payment system in June 2020.	30 June 2025	ICRA	Reported
A service provider must report cyber incidents to the regulated entity without undue delay, so that the entity can report them to RBI within 6 hours of the provider detecting them.	10 April 2023	Reserve Bank of India	Official
Outsourcing does not reduce a regulated entity's obligations; its board and senior management remain ultimately responsible for the outsourced activity.	10 April 2023	Reserve Bank of India	Official
When using cloud services, a regulated entity's outsourcing policy must cover the whole lifecycle of data, from creation and entry into the cloud until it is permanently deleted.	10 April 2023	Reserve Bank of India	Official
RBI's IT outsourcing Direction counts cloud computing services as outsourced IT services and adds specific requirements for storing, computing and moving data in the cloud.	10 April 2023	Reserve Bank of India	Official
RBI's Direction describes cloud security as a shared responsibility between the regulated entity and the cloud service provider.	10 April 2023	Reserve Bank of India	Official
Regulated entities must consider the risk of concentrating their outsourcing with a single provider or a few providers.	10 April 2023	Reserve Bank of India	Official
Due diligence on an IT service provider must cover its experience and competence to deliver over the contract period and its financial soundness.	10 April 2023	Reserve Bank of India	Official
A regulated entity's outsourcing policy must include termination processes and exit strategies, including business continuity if a service provider leaves the arrangement.	10 April 2023	Reserve Bank of India	Official
Responsibility for resolving customers' grievances about outsourced services stays with the regulated entity, and outsourcing cannot reduce customers' rights against it.	10 April 2023	Reserve Bank of India	Official
RBI publishes monthly Payment System Indicators with volumes and values for every payment system; the latest edition found covers July 2026.	29 September 2026	Reserve Bank of India	Official
Since 1 January 2021, banks must offer Positive Pay for cheques of ₹50,000 and above; using it is the account holder's choice, and banks may make it mandatory from ₹5 lakh.	25 September 2020	Reserve Bank of India	Official
RBI issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (RBI/2023-24/102), effective 1 October 2023.	10 April 2023	Reserve Bank of India	Official
RBI issued the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on 7 November 2023 (RBI/2023-24/107).	7 November 2023	Reserve Bank of India	Official
RBI's Payment System Indicators list RTGS and NEFT under RBI-operated payment systems.	29 September 2026	Reserve Bank of India	Official
RBI set up the Reserve Bank Innovation Hub as a Section 8 company with ₹100 crore of initial capital; it was inaugurated in Bengaluru on 24 March 2022.	24 March 2022	Reserve Bank of India	Official
The Reserve Bank Innovation Hub describes itself as a wholly owned subsidiary of RBI; its work includes the Unified Lending Interface and MuleHunter.ai.	29 September 2026	Reserve Bank Innovation Hub	Official
Financial information users in the Account Aggregator framework adopt technical specifications published by ReBIT.	1 August 2023	Securities and Exchange Board of India	Official
ReBIT is a wholly owned subsidiary of RBI set up to serve RBI's IT and cyber security needs and improve the cyber resilience of Indian banking.	20 September 2022	Reserve Bank of India	Official
RTGS has run 24x7 since December 2020, and NEFT since December 2019.	1 January 2025	Institute for Development and Research in Banking Technology	Official
RTGS has been available 24x7x365 since 14 December 2020.	29 September 2026	Reserve Bank of India	Official
RTGS settles each transaction in real time on a one-to-one gross basis.	1 January 2025	Institute for Development and Research in Banking Technology	Official
RTGS was launched on 26 March 2004.	1 January 2025	Institute for Development and Research in Banking Technology	Official
RTGS is meant mainly for large-value transfers: the minimum is ₹2 lakh, with no upper ceiling.	29 September 2026	Reserve Bank of India	Official

Fact	As of	Source	Type
RBI announced on 8 June 2022 that credit cards, starting with RuPay, could be linked to UPI.	8 June 2022	Business Today	Reported
SBIs core banking has run on TCS BaNCS since an implementation that began in 2001; in October 2021 TCS said the partnership was extended for five years.	6 October 2021	Tata Consultancy Services	Vendor claim
SFMS, a secure financial messaging platform, was launched on 14 December 2001 and is used by NEFT, RTGS and delivery-versus-payment settlement of government securities.	1 January 2025	Institute for Development and Research in Banking Technology	Official
Payment system providers had to comply within six months and submit a system audit report by a CERT-In-empanelled auditor; the circular was issued under the Payment and Settlement Systems Act, 2007.	6 April 2018	Reserve Bank of India	Official
RBI's framework for failed transactions, in force since 15 October 2019, sets outer time limits for reversal and requires compensation to be paid automatically, without a complaint.	20 September 2019	Reserve Bank of India	Official
If an ATM debits the account but does not dispense cash, the bank must reverse it within T+5 days; after that, ₹100 a day is payable.	20 September 2019	Reserve Bank of India	Official
A failed transaction is one not fully completed for a reason not attributable to the customer, such as a link failure, an ATM without cash or a session time-out.	20 September 2019	Reserve Bank of India	Official
If an IMPS transfer debits the payer but does not credit the beneficiary, it must be reversed by T+1 day; after that, ₹100 a day is payable.	20 September 2019	Reserve Bank of India	Official
If a UPI payment to a merchant debits the payer but the merchant gets no confirmation, it must be reversed within T+5 days; after that, ₹100 a day is payable.	20 September 2019	Reserve Bank of India	Official
If a UPI transfer debits the payer but does not credit the beneficiary, the beneficiary bank must reverse it by T+1 day; after that, ₹100 a day is payable.	20 September 2019	Reserve Bank of India	Official
From 15 September 2025, credit card bills can be paid by UPI up to ₹5 lakh per transaction and ₹6 lakh a day.	15 September 2025	All India Radio News (Prasar Bharati)	Reported
Since RBI's circular of 4 September 2023, pre-sanctioned credit lines at scheduled commercial banks can fund UPI payments, with the customer's prior consent.	4 September 2023	Khaitan & Co	Reported
UPI averaged 791 million transactions a day in August 2026.	31 August 2026	Business Standard	Reported
From 15 September 2025, UPI payments on the Government e-Marketplace, including taxes and earnest money deposits, can be up to ₹5 lakh per transaction.	15 September 2025	DD News (Prasar Bharati)	Reported
From 15 September 2025, NPCI raised UPI limits for verified merchants in capital markets and insurance to ₹5 lakh per transaction and ₹10 lakh a day.	15 September 2025	DD News (Prasar Bharati)	Reported
The UPI limit for person-to-person transfers stayed at ₹1 lakh a day.	15 September 2025	All India Radio News (Prasar Bharati)	Reported
UPI's highest monthly value so far was ₹29.9 trillion, in May 2026, across 23.2 billion transactions.	31 August 2026	Business Standard	Reported
UPI processed 23.66 billion transactions worth ₹29.88 trillion in July 2026.	31 July 2026	Business Standard	Reported
UPI processed 24.51 billion transactions worth ₹29.82 trillion in August 2026, its highest monthly volume to date.	31 August 2026	Business Standard	Reported

Appendix C

Bibliography

All 65 sources used, grouped by publisher. Each was accessed on the date shown. Primary sources are those of regulators, government and the institutions themselves.

1. **All India Radio News (Prasar Bharati).** RBI directs Kotak Mahindra Bank to cease issue of fresh credit cards, bars onboarding of new online customers. Press source; accessed 29 September 2026.
<https://newsonair.gov.in/rbi-directs-kotak-mahindra-bank-to-cease-issue-of-fresh-credit-cards-bars-onboarding-of-new-online-customers>
2. **All India Radio News (Prasar Bharati).** RBI lifts business restrictions on Kotak Mahindra Bank. Press source; accessed 29 September 2026.
<https://www.newsonair.gov.in/rbi-lifts-business-restrictions-on-kotak-mahindra-bank/>
3. **All India Radio News (Prasar Bharati).** UPI raises daily P2M payment limit to Rs 10 lakh. Press source; accessed 29 September 2026.
<https://www.newsonair.gov.in/npci-raises-upi-person-to-merchant-transaction-limit-to-%E2%82%B95-lakh>
4. **Bharatiya Reserve Bank Note Mudran Private Limited.** Company Profile. Primary source; accessed 29 September 2026.
<https://www.brbtnmpl.co.in/company-profile/>
5. **Business Standard.** RBI issues Directions on Framework on Authentication Mechanisms for Digital Payment Transactions. Press source; accessed 29 September 2026.
https://www.business-standard.com/markets/capital-market-news/rbi-issues-directions-on-framework-on-authentication-mechanisms-for-digital-payment-transactions-125092501090_1.html
6. **Business Standard.** RBI restricts Mastercard from onboarding new domestic customers. Press source; accessed 29 September 2026.
https://www.business-standard.com/article/finance/rbi-restricts-mastercard-from-onboarding-new-domestic-customers-121071400974_1.html
7. **Business Standard.** Reserve Bank issues draft Regulatory Principles for Management of Model Risks. Press source; accessed 29 September 2026.
https://www.business-standard.com/markets/capital-market-news/reserve-bank-issues-draft-regulatory-principles-for-management-of-model-risks-in-credit-126062500401_1.html
8. **Business Standard.** UPI sets new record at 24.51 bn transactions in Aug, value at ₹29.82 trn. Press source; accessed 29 September 2026.
https://www.business-standard.com/finance/news/upi-transactions-august-2026-record-volume-npci-126090100506_1.html
9. **Business Today.** Credit cards, starting with RuPay, can now be linked to UPI: RBI. Press source; accessed 29 September 2026.
<https://businesstoday.in/amp/latest/economy/story/credit-cards-starting-with-rupay-can-now-be-linked-to-upi-rbi-336757-2022-06-08>
10. **CARE Ratings.** The Clearing Corporation of India Limited (Revised): rating press release. Analyst source; accessed 29 September 2026.
https://www.careratings.com/upload/CompanyFiles/PR/202503120310_The_Clearing_Corporation_of_India_Limited.pdf
11. **CERT-In, Ministry of Electronics and Information Technology.** Directions under sub-section (6) of section 70B of the IT Act, 2000 (28 April 2022). Primary source; accessed 29 September 2026.
https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
12. **Cloud Infrastructure Map.** Cloud Infrastructure Map. Analyst source; accessed 29 September 2026.
<https://www.cloudinfrastructuremap.com/>
13. **DD News (Prasar Bharati).** NPCI raises daily UPI payment limit on P2M transactions to ₹10 lakh. Press source; accessed 29 September 2026.
<https://ddnews.gov.in/en/npci-raises-daily-upi-payment-limit-on-p2m-transactions-to-%E2%82%B910-lakh/>
14. **Department of Financial Services, Ministry of Finance.** Account Aggregator Framework. Primary source; accessed 29 September 2026.
<https://financialservices.gov.in/account-aggregator-framework>
15. **Deposit Insurance and Credit Guarantee Corporation.** A Guide to Deposit Insurance. Primary source; accessed 29 September 2026.
<https://www.dicgc.org.in/guide-to-deposit-insurance>
16. **Deposit Insurance and Credit Guarantee Corporation.** DICGC Information Leaflet. Primary source; accessed 29 September 2026.
https://dicgc.org.in/sites/default/files/2024-10/DICGC_Information_Leaflet.pdf
17. **Deposit Insurance and Credit Guarantee Corporation.** History of DICGC. Primary source; accessed 29 September 2026.
<https://www.dicgc.org.in/node/17>
18. **EDB.** Infosys Finacle Names EnterpriseDB Open Source DB Partner of the Year. Vendor source; accessed 29 September 2026.
<https://www.enterprisedb.com/blog/infosys-finacle-names-enterprisedb-open-source-db-partner-year>
19. **EdgeVerve Systems.** EdgeVerve Systems Positioned a Leader by Gartner for the Finacle Core Banking Solution. Vendor source; accessed 29 September 2026.
<https://www.edgeverve.com/finacle/news/edgeverve-positioned-gartner-for-finacle-solution/>
20. **ICRA.** National Payments Corporation of India: rating rationale. Analyst source; accessed 29 September 2026.
<https://www.icra.in/Rating/GetRationalReportFilePdf?id=135865>
21. **ICRA.** RBI's risk-based premium framework for deposit insurance to enhance profitability of stronger banks. Analyst source; accessed 29 September 2026.
<https://www.icra.in/Research/ViewResearchReport/rbi-s-risk-based-premium-framework-for-deposit-insurance-to-enhance-profitability-of-stronger-banks/6780>
22. **Inc42.** RBI bars Kotak Mahindra Bank from onboarding new customers via online, mobile banking channels. Press source; accessed 29 September 2026.
<https://inc42.com/buzz/rbi-bars-kotak-mahindra-bank-from-onboarding-new-customers-via-online-mobile-banking-channels/>
23. **Institute for Development and Research in Banking Technology.** About IDRBT. Primary source; accessed 29 September 2026.
<https://www.idrbt.ac.in/about-idrbt>

24. **Institute for Development and Research in Banking Technology. Milestones 1994-1998.** Primary source; accessed 29 September 2026.
<https://www.idrbit.ac.in/?p=34318>
25. **Khaitan & Co. Credit lines on UPI: the next step towards digital financial inclusion.** Analyst source; accessed 29 September 2026.
https://khitanco.com/thought-leaderships/Credit_lines_on_UPI_the_next_step_towards_Digital_Financial_Inclusion
26. **KPMG in India. RBI Authentication Mechanisms for Digital Payment Transactions Directions, 2025.** Analyst source; accessed 29 September 2026.
<https://kpmg.com/in/en/insights/2025/12/reserve-bank-of-india-rbi-authentication-mechanisms-for-digital-payment-transactions-directions-2025.html>
27. **Lexology. RBI releases draft circular on model risk management in credit for lenders.** Analyst source; accessed 29 September 2026.
<https://www.lexology.com/library/detail.aspx?g=2e3e5197-a3ec-4b08-9048-8c70dfd82be4>
28. **National Bank for Agriculture and Rural Development. Annual Report 2023-24, chapter 9: People, Processes and Policies.** Primary source; accessed 29 September 2026.
<https://www.nabard.org/annual-report/people-processes-and-policies.html>
29. **National Bank for Agriculture and Rural Development. Citizen's Charter.** Primary source; accessed 29 September 2026.
<https://www.nabard.org/ftrcontent.aspx?id=492>
30. **National Bank for Agriculture and Rural Development. Standalone Financial Results for the quarter ended June 30, 2025.** Primary source; accessed 29 September 2026.
https://www.nabard.org/pdf/Financial%20Results_June-2025.pdf
31. **National Housing Bank. About Us: Genesis.** Primary source; accessed 29 September 2026.
<https://nhb.org.in/about-us/>
32. **National Payments Corporation of India. National Payments Corporation of India.** Primary source; accessed 29 September 2026.
<https://www.npci.org.in/>
33. **National Payments Corporation of India. Takeover of NFS by NPCI from IDRBT (NPCI/NFS/OC No.1).** Primary source; accessed 29 September 2026.
<https://www.npci.org.in/PDF/nfs/circular/2009-10/NFS-OC-1-Takeover-of-NFS-by-NPCI-from-IDRBT.pdf>
34. **Reserve Bank Innovation Hub. Reserve Bank Innovation Hub.** Primary source; accessed 29 September 2026.
<https://rbihub.in/>
35. **Reserve Bank of India. Amendment to Master Direction on KYC: Operationalisation of Central KYC Registry (RBI/2016-17/11).** Primary source; accessed 29 September 2026.
<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10498>
36. **Reserve Bank of India. Availability of National Electronic Funds Transfer (NEFT) System on 24x7 basis (RBI/2019-20/111).** Primary source; accessed 29 September 2026.
<https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11750>
37. **Reserve Bank of India. Chief Executive Officer (CEO) for Indian Financial Technology and Allied Services (IFTAS).** Primary source; accessed 29 September 2026.
<https://website.rbi.org.in/web/rbi/-/chief-executive-officer-ceo-for-indian-financial-technology-and-allied-services-iftas-1>
38. **Reserve Bank of India. Chief Executive Officer (CEO) for Reserve Bank Information Technology Pvt. Ltd. (ReBIT).** Primary source; accessed 29 September 2026.
https://opportunities.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=4187
39. **Reserve Bank of India. Continuous Clearing and Settlement on Realisation in Cheque Truncation System: Phase 2 (RBI/2025-26/156).** Primary source; accessed 29 September 2026.
<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=13232&Mode=0>
40. **Reserve Bank of India. Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems (RBI/2019-20/67).** Primary source; accessed 29 September 2026.
<https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11693>
41. **Reserve Bank of India. Inauguration of the Reserve Bank Innovation Hub (Press Release 2021-2022/1903).** Primary source; accessed 29 September 2026.
https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53458
42. **Reserve Bank of India. Introduction of Continuous Clearing and Settlement on Realisation in Cheque Truncation System (RBI/2025-26/73).** Primary source; accessed 29 September 2026.
<https://website.rbi.org.in/documents/d/rbi/circulardatedaugust132025cts>
43. **Reserve Bank of India. Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 (updated 6 September 2024).** Primary source; accessed 29 September 2026.
https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?Id=10598
44. **Reserve Bank of India. Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI/2023-24/107).** Primary source; accessed 29 September 2026.
<https://website.rbi.org.in/web/rbi/-/notifications/master-direction-on-information-technology-governance-risk-controls-and-assurance-practices>
45. **Reserve Bank of India. Master Direction on Outsourcing of Information Technology Services (full text).** Primary source; accessed 29 September 2026.
https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486
46. **Reserve Bank of India. Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102).** Primary source; accessed 29 September 2026.
https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486
47. **Reserve Bank of India. Payment System Indicators (monthly).** Primary source; accessed 29 September 2026.
<https://rbi.org.in/scripts/TrendsPSIUserView.aspx?Id=56>
48. **Reserve Bank of India. Positive Pay System for Cheque Truncation System (RBI/2020-21/41).** Primary source; accessed 29 September 2026.
<https://website.rbi.org.in/web/rbi/-/notifications/positive-pay-system-for-cheque-truncation-system-11969>

49. **Reserve Bank of India. Real Time Gross Settlement (RTGS) System: FAQs.** Primary source; accessed 29 September 2026.
<https://rbi.org.in/Scripts/FAQView.aspx?id=65>
50. **Reserve Bank of India. Report of the Committee to develop a Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) in the Financial Sector (press release).** Primary source; accessed 29 September 2026.
<https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR902F828551DA4B54AFDA44180762D51FFCD.PDF>
51. **Reserve Bank of India. Reserve Bank of India.** Primary source; accessed 29 September 2026.
<https://www.rbi.org.in/>
52. **Reserve Bank of India. Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (full text).** Primary source; accessed 29 September 2026.
<https://rbi.org.in/Scripts/NotificationUser.aspx?id=12562&Mode=0>
53. **Reserve Bank of India. Reserve Bank of India divests its share in NABARD and NHB (Press Release 2018-2019/2528).** Primary source; accessed 29 September 2026.
https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=46885
54. **Reserve Bank of India. Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)] (RBI/2022-2023/95).** Primary source; accessed 29 September 2026.
<https://website.rbi.org.in/web/rbi/-/notifications/restriction-on-storage-of-actual-card-data-i.e.-card-on-file-cof-12363>
55. **Reserve Bank of India. Restrictions on Mastercard lifted (press release).** Primary source; accessed 29 September 2026.
https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53877
56. **Reserve Bank of India. Setting up of Central Electronic Registry under the SARFAESI Act 2002 (RBI/2010-2011/545).** Primary source; accessed 29 September 2026.
https://rbi.org.in/scripts/BS_NBFCNotificationView.aspx?id=6435
57. **Reserve Bank of India. Storage of Payment System Data (RBI/2017-18/153).** Primary source; accessed 29 September 2026.
<https://rbi.org.in/scripts/NotificationUser.aspx?id=11244>
58. **S.S. Rana & Co., MeitY notifies final Digital Personal Data Protection Rules 2025.** Analyst source; accessed 29 September 2026.
<https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/>
59. **Securities and Exchange Board of India. Consultation paper on Financial Information Users in the securities markets under the Account Aggregator framework.** Primary source; accessed 29 September 2026.
https://www.sebi.gov.in/sebi_data/attachdocs/aug-2023/1690887848711.pdf
60. **Tata Consultancy Services. SBI deepens partnership with TCS to drive innovation and enhance customer experience.** Vendor source; accessed 29 September 2026.
<https://tcs.com/who-we-are/newsroom/press-release/sbi-deepens-partnership-with-tcs-drive-innovation-enhance-customer-experience>
61. **The Clearing Corporation of India Limited. Promoters / Shareholders.** Primary source; accessed 29 September 2026.
<https://www.ccilindia.com/web/ccil/promoters-stakeholders>
62. **The Federal. RBI finds Kotak Mahindra Bank deficient in IT risk management, bars online customer onboarding (PTI).** Press source; accessed 29 September 2026.
<https://thefederal.com/category/business/rbi-finds-kotak-mahindra-bank-deficient-in-it-risk-management-bars-online-customer-onboarding-119336>
63. **The Tribune. RBI bars Mastercard from adding new clients in India.** Press source; accessed 29 September 2026.
<https://www.tribuneindia.com/news/business/rbi-bars-mastercard-from-adding-new-clients-in-india-283510>
64. **The Tribune. RBI unveils new directions to strengthen digital payment security.** Press source; accessed 29 September 2026.
<https://www.tribuneindia.com/news/business/rbi-unveils-new-directions-to-strengthen-digital-payment-security>
65. **Trilegal. 2022 CERT-In Directions on Reporting Cyber Incidents.** Analyst source; accessed 29 September 2026.
<https://trilegal.com/knowledge-repository/2022-cert-in-directions-on-reporting-cyber-incidents/>

Appendix D

Corrections to earlier drafts

Earlier drafts of this material contained claims that research showed to be wrong, outdated or unverifiable. They were removed or corrected, and the build now refuses them. This is the record.

#	Earlier claim	What the sources show
1	SBI runs Fincle	False. SBI has run TCS BaNCS since an implementation that began in 2001
2	"Infosys Fincle" as the maker	Partly true. The vendor or itself brands it "Infosys Fincle"; the developer is EdgeVerve Systems, a wholly owned Infosys subsidiary
3	UPI at 14B+ a month, 450M+ a day	Stale. August 2026: 24.51 billion transactions, 791 million a day
4	UPI limit ₹1 lakh for all payments	Outdated. Verified merchants in specified categories: up to ₹5 lakh per transaction (₹10 lakh a day for capital markets and insurance); person-to-person still ₹1 lakh
5	Cheques clear T+1	Outdated. Continuous clearing since 4 October 2025 (Phase 1); Phase 2 postponed
6	NPCI internals (Oracle RAC, TPS figures, active-active, HSM placement and so on)	Unverifiable. Not publicly documented
7	UPI Lite and UPI 123PAY caps	Not checked. Link out to NPCI
8	RuPay ~60% of debit cards; NFS 1.2 million ATMs	NFS: false. 2.61 lakh ATMs of 1,317 member banks (31 Jul 2024). RuPay share: not checked
9	Visa and Mastercard fined under the 2018 localisation circular	False as stated. Business restrictions, not fines, under section 17 of the PSS Act: American Express and Diners Club from 1 May 2021; Mastercard from 22 July 2021, lifted June 2022. Visa was not named
10	RBI mandates RPO ≤ 6 hours, RTO ≤ 24 hours	False as stated. RBI's 2023 IT Governance Direction sets no fixed values. It requires banks to define RPO and RTO for critical systems and to prioritise a minimal RTO and near-zero RPO (checked in Stage 4b)
11	"RBI Cloud Policy 2023", "Cybersecurity Framework 2016", "IT Framework 2011"	Partly. Verified: IT Governance, Risk, Controls and Assurance Practices MD (7 Nov 2023); Outsourcing of IT Services MD (10 Apr 2023, effective 1 Oct 2023). No "RBI Cloud Policy" found; cloud falls under the outsourcing MD. 2016 and 2011 titles not checked
12	CIBIL has 90%+ market share	Invented
13	Named private banks or SFBs on specific platforms	Not checked. Only sourced users may appear
14	Claims about a bank's outage or DR failure	Policy: omit unless primary or reputable source
15	Invented headcounts ("NABARD ~28,000", "NPCI ~5,500")	False. NABARD had 3,334 staff on 31 March 2024. NPCI: no official figure found
16	CCIL "zero settlement failures since 2001"	Not checked
17	NABARD "33 StCBs, 351 DCCBs, 43 RRBs"	Not checked
18	IDRBT is a deemed university	False. A society registered in March 1996 under the Societies Registration Act
19	NABARD stake moved to Government in 2023	False. RBI's last NABARD shares sold on 26 February 2019 (NHB on 19 March 2019)
20	CERSAI is RBI-promoted	False. A Government company set up for the registry notified by the Ministry of Finance
21	NEFT "48 half-hourly cycles"	True as of the December 2019 circular. RBI now lists that circular as withdrawn (consolidated); confirm current guidelines
22	SFB rules (75% PSL, 50% small loans, 25% rural branches, 15% CRAR)	Not checked
23	Positive Pay applies to cheques of ₹50,000 and above	True, with nuance. Banks must offer it from ₹50,000; using it is the customer's choice; banks may make it mandatory from ₹5 lakh
24	Employer-specific content	Out of scope. Enforced by the optional forbidden-strings.txt gate

Index

A

AA (Account Aggregator) 15, 20, 34
AML (Anti-money laundering) 10-11, 108
API (Application programming interface) 10-11, 33, 35-36, 48, 60, 71-72, 85, 89, 103, 108
AutoPay (UPI AutoPay) 18

B

BBPS (Bharat Bill Payment System) 15, 20
BOD (Beginning of day) 12, 27
BRBNMPL (Bharatiya Reserve Bank Note Mudran Private Limited) 116-117, 119, 132

C

CBS (Core banking system) 10
CCIL (The Clearing Corporation of India Limited) 116-117, 128, 132
CDC (Change data capture) 38-39
CERSAI (Central Registry of Securitisation Asset Reconstruction and Security Interest of India) 11, 13, 113, 115-117, 131-132
CERT-In (Indian Computer Emergency Response Team) 49-50, 80, 112-115
CQRS (Command query responsibility segregation) 38
CSPM (Cloud security posture management) 79
CTS (Cheque Truncation System) 15, 19-21, 30, 32, 113, 126-127

D

DC (Data centre) 51-52
DICGC (Deposit Insurance and Credit Guarantee Corporation) 116-118, 131-132
DLP (Data loss prevention) 60, 79
DR (Disaster recovery) 24-25, 27-28, 45-46, 53-54, 73-74, 100, 106, 108-109, 113

E

EOD (End of day) 12, 26
ESB (Enterprise service bus) 71-72

F

FIP (Financial information provider) 20, 35
FIU (Financial information user) 20, 35
FIU-IND (Financial Intelligence Unit - India) 11, 112
FSDC (Financial Stability and Development Council) 112

G

GitOps (GitOps) 60, 73-74

H

HSM (Hardware security module) 48, 79, 91, 94

I

IDRBT (Institute for Development and Research in Banking Technology) 19-21, 31, 49-50, 80-81, 94-95, 116-117, 121-122, 124-126, 132
IFSC (Indian Financial System Code) 16
IFTAS (Indian Financial Technology and Allied Services) 8, 12-13, 20-21, 27-28, 57-58, 62, 64, 77-78, 93-95, 103, 105, 116-117, 121-122, 124-125, and elsewhere
IMPS (Immediate Payment Service) 14-16, 18, 20-21, 97, 100, 112
INFINET (Indian Financial Network) 20-21, 60, 93-95, 117, 121-122, 124-125, 132

IRDAI (Insurance Regulatory and Development Authority of India) 112

ISO 20022 (ISO 20022) 29, 60, 72, 93

ISO 8583 (ISO 8583) 29, 72, 93

IT Act (Information Technology Act, 2000) 49-50, 80-81, 112-113, 115, 124

K

KYC (Know your customer) 10-11, 13, 103, 112-113, 115, 131-132

M

Master Direction (Master Direction) 13, 20-21, 34, 36, 43, 45-46, 49-50, 58, 62, 64, 74-75, 78, 80, 83, and elsewhere

MeitY (Ministry of Electronics and Information Technology) 112-113, 115

N

NABARD (National Bank for Agriculture and Rural Development) 116-117, 129-130, 132

NACH (National Automated Clearing House) 14-15, 19-20, 71

NEFT (National Electronic Funds Transfer) 14-16, 20-21, 30-31, 93-95, 117, 121-122, 124-125, 132

NFS (National Financial Switch) 15, 21, 124-126, 132

NHB (National Housing Bank) 116-117, 129-130, 132

NPCI (National Payments Corporation of India) 8, 14-19, 21-22, 112, 115-117, 124-127, 132

O

OLAP (Online analytical processing) 40
OLTP (Online transaction processing) 40

P

PAM (Privileged access management) 48-49, 79
PFRDA (Pension Fund Regulatory and Development Authority) 112
PSS Act (Payment and Settlement Systems Act, 2007) 126

Q

QR (Quick Response code) 15, 17, 20, 60, 93

R

RBI (Reserve Bank of India) 8-9, 11, 13-22, 24, 27, 29-32, 34-36, 42-43, 45-46, 49-54, 57-58, 60, 62, 64, and elsewhere
RBIF (Reserve Bank Innovation Hub) 116-117, 123
ReBIT (Reserve Bank Information Technology Private Limited) 20, 22, 34, 36, 72, 116-117, 120, 131-132
RPO (Recovery point objective) 24, 51-54, 66-67
RTGS (Real Time Gross Settlement) 14-16, 20-21, 30-31, 93-95, 107, 117, 121-122, 124-125
RTO (Recovery time objective) 24, 51, 53-54, 66-67
RuPay (RuPay) 15, 18-19, 22

S

SEBI (Securities and Exchange Board of India) 112
SFMS (Structured Financial Messaging System) 8, 13, 20-21, 27-28, 57-58, 60, 62, 64, 77-78, 93-95, 103, 105, 117, 121-122, and elsewhere
SIEM (Security information and event management) 49, 60, 79-80
SLI (Service level indicator) 82
SLO (Service level objective) 82
SOAR (Security orchestration, automation and response) 60, 79
SWIFT (Society for Worldwide Interbank Financial Telecommunication) 20

T

TPAP (Third-party application provider) 16

U

UIDAI (Unique Identification Authority of India) 112

ULI (Unified Lending Interface) 123

UPI (Unified Payments Interface) 8, 10, 12-18, 20-22, 27-28, 30-32, 38-39, 60, 68, 70, 82-83, 88-89, 93-95, 97, and elsewhere

UPI 123PAY (UPI 123PAY) 18

UPI Lite (UPI Lite) 18

W

WAF (Web application firewall) 48, 79

About the author

Infrastructure engineering leader in Indian banking

Neeraj Prem leads infrastructure engineering at a digital-first small finance bank in Bengaluru. His team of SREs, database engineers, DevSecOps and cloud network engineers runs a multi-cloud estate under RBI, NPCI, PCI-DSS and CERT-In requirements. He wrote this guide to explain the machinery behind Indian payments the way he wishes it had been explained to him, with every fact sourced and dated. He writes about engineering leadership and DevOps at neerajprem.in.

The companion website, with the latest version of every chapter, is at ibs.neerajprem.in.

- Blog: neerajprem.in: <https://neerajprem.in>
- GitHub: [neerajprem](https://github.com/neerajprem): <https://github.com/neerajprem>