

DB — Certificate Examination in Digital Banking

Complete Book | Table of Contents | 10 chapters + 10 additional sections

Module A — Digital Banking Products

CH-1	Digital Delivery Channels	2
CH-2	Cards	5
CH-3	Automated Teller Machines (ATMs)	9
CH-4	Mobile Banking	13
CH-5	Internet or Online Banking	16
CH-6	POS Terminals	20

Module B — Digital Banking and Financial Inclusion

CH-7	Digital Banking and Financial Inclusion	24
------	---	----

Module C — Marketing of Digital Banking Products

CH-8	Marketing of Digital Banking Products	29
------	---------------------------------------	----

Module D — Developments in Payment Systems in India and Digital Banking

CH-9	Developments in Payment Systems in India and Digital Banking	33
------	--	----

Module E — Future Trends in Digital Banking

CH-10	Future Trends in Digital Banking	37
-------	----------------------------------	----

Additional Resources

—	Case Studies — Module A: Digital Banking Products	41
—	Case Studies — Module B: Digital Banking and Financial Inclusion	50
—	Case Studies — Module C: Marketing of Digital Banking Products	51
—	Case Studies — Module D: Developments in Payment Systems in India and Digital Banking	52
—	Case Studies — Module E: Future Trends in Digital Banking	53
—	Mega Tests — Mega Test 1 — 100 Questions (Full Syllabus)	54
—	Mega Tests — Mega Test 2 — 100 Questions (Full Syllabus)	61
—	Mega Tests — Mega Test 3 — 100 Questions (Full Syllabus)	68
—	Mega Tests — Mega Test 4 — 100 Questions (Full Syllabus)	75
—	Mega Tests — Mega Test 5 — 100 Questions (Full Syllabus)	83

CH-1 Digital Delivery Channels

Topic 1 — Digital Banking

- **Meaning** — Digital banking uses computer-based technologies to bind online, mobile and electronic banking services together.
- **Aim** — It improves the value of the service and the **user experience**.
- **Beyond paper** — It is **more than going paperless**.
- **Main focus** — A richer product suite with **value-added services** and an **integrated channel experience**.
- **Data capture** — Banks capture customer actions in their applications along with market data.
- **Insight** — This large data is processed to understand **customer behaviour and needs**.
- **Delivery** — Banks then design, market and deliver products where the customer expects them.
- **Result** — This is the basis of **customer centricity**.

Example: While a customer is logged in, analytics running in the background changes the on-screen content to help the transaction and to offer an **up-sale** or a **loyalty** offer.

- **Anywhere service** — Customers can transfer money, get statements, make enquiries and open deposits **without visiting a branch**.
- **More services** — They can also settle online trades and pay fees and taxes.
- **Add-ons** — By studying portfolios and transaction habits, banks send **payment reminders**, investment analysis and market advisories.
- **Basis** — These add-ons rest on **connectivity, software and the business value of the customer**.

Topic 2 — Need for Digital Channels and Customer Preferences

Adopting digital channels helps banks **cut costs**, deepen **customer satisfaction and loyalty**, and build **long-term relationships and profitability**.

- **Drivers** — Customer preference for digital banking varies with **access, trust, cost and ease of use**.
- **Transparency** — Banks should explain charges clearly and offer services only with customer **consent**.
- **Payment** — Convenience attracts customers, but **willingness to pay is not universal**.

Drivers of digital adoption
Better user-experience design
Internet access from anywhere
Advanced analytical tools that build customer profiles
Technologies enabling end-to-end communication between customer and bank

Topic 3 — Banking Relationship and Customer Expectations

- **Early wins** — A bank that meets needs in the desired **content, functionality, platform, speed and ease** early on gains an edge.
- **Outcome** — It is likely to become the **bank of choice** for the next product.
- **Comparison** — Customers compare banks on **price, convenience, reliability and service**.
- **Varied adoption** — Digital adoption differs across **age groups and personal circumstances**.
- **No assumptions** — Banks should not assume all young customers are high earners or want only digital contact.

- **Retention** — **Accessible digital services with assisted channels** support retention.
- **High standards** — Customers expect good digital communication, sleek page design, rich functions and fast search results.
- **Example** — A self-generated account statement **24 × 7** is preferred over a monthly postal statement.
- **Risk** — A bank that ignores changing needs risks customers becoming a source of **bad publicity**.
- **Influence** — A customer's choice also influences friends and contacts.

Topic 4 — Aspects of Robust Digital Services

No.	Aspect banks must reckon with
1	Customer attitudes and behaviour are evolving rapidly
2	Channel preferences vary across customers
3	Digital technology itself keeps changing; each advance opens new ways to improve experience
4	Technology reduces operating and servicing cost ; the saving can be passed to customers
5	Technology reduces delivery time of products and services
6	Digital channels save customers' effort, cost and time
7	Computerised operations bring their own risks ; offerings must be secure against information loss, error and unintended access
8	Customer education and communication for technology services differ in content and mode from traditional practice

Technology lays the foundation for **user-friendliness**, but a digital service must be designed around customer **habits and general practices in society**.

- **Regulatory KYC** — It identifies and verifies customers and supports due diligence and anti-money laundering controls.
- **Customer analytics** — It helps understand service preferences but **does not replace KYC**.
- **Limits** — Analytics must respect consent, privacy and law.

Topic 5 — Security in Digital Banking

- **Cornerstone** — **Security is the cornerstone** of digital banking.
- **Scope** — It extends from the bank's hardware to the **user's device** (PC, tablet or smartphone).
- **What it protects** — Communication, user information and the bank's IT infrastructure.
- **Approach** — Banks should link security with business interests and think **beyond regulatory compliance**.

Issue	What banks must do
Linking security and business (dovetailing)	Build security practices and controls into development, operations and delivery; engage business stakeholders
Aligning business and threats	Balance service and usage needs with the expanding range of information-security threats
Governing the enterprise	Set frameworks, policies and controls to protect IT environments
Keeping pace with persistent threats	Proactive, dynamic approach using intelligence, analytics and specialised security service providers
Security capability	Develop, train and retain staff skilled in security planning, design and execution

Topic 6 — Information Security and the CIA Triad

- **Electronic records** — All values relating to the bank, customers and vendors (customer data, transactions, business data) are recorded electronically.
- **Information Security (IS)** — It is the body of knowledge and practices that keeps this information secure.
- **Threats covered** — **Malicious attacks, accidental errors and operational failures.**

Element	Meaning
Confidentiality	No one other than the authorised can see or access the information
Integrity	Information stays accurate and complete ; authorised changes are controlled and recorded (posting a transaction changes the balance but keeps the audit trail)
Availability	Information is available at places, on media, to people and at times as authorised

- **Tailored controls** — Practices, rules and software are chosen based on the data, the platform and the threats.
- **Threat types** — Threats may be software such as **malware**, or practices such as **phishing**.
- **Scope of IS** — This whole activity falls under IS.

Remember this

- **CIA** = Confidentiality, Integrity, Availability.

Topic 7 — Digital Delivery Channels and Adoption Challenges

Digital channels include **internet and mobile banking, cards, ATMs, POS, business correspondents and interoperable payment services.**

Factors affecting adoption
Availability, accessibility and connectivity
Language and digital literacy
Privacy, fraud and service recovery

Assisted channels remain important for customers who need help.

Topic 8 — e-KYC, Digital KYC and V-CIP

- **KYC** — It is customer identification, verification and due diligence.
- **Aadhaar** — **Aadhaar is not mandatory** for ordinary KYC; it may be submitted **voluntarily**.
- **Exception** — Notified subsidy or benefit cases carry the statutory requirement.
- **Distinct processes** — **Aadhaar e-KYC, offline verification, Digital KYC and V-CIP** are separate permitted processes.

OTP-based non-face-to-face e-KYC account	Limit / condition
Consent	Specific consent of the customer
Aggregate deposit balance	Up to ₹1 lakh
Aggregate credits in a financial year	Up to ₹2 lakh
Loans	Only term loans , up to ₹60,000 in a year
Full KYC	Complete identification or compliant V-CIP within one year ; otherwise close deposits and stop further loan debits

These limits apply only to OTP-based e-KYC accounts, **not to fully verified digital accounts.**

- **V-CIP status** — A compliant **Video-based Customer Identification Process (V-CIP)** is treated **on par with face-to-face** identification.
- **Bank's duty** — The bank stays responsible for identity verification and a secure **live** interaction.

- **Controls** — Consent, **liveness checks** and retained records are required.
- **Uses** — V-CIP supports eligible onboarding, conversion of OTP e-KYC accounts and **periodic KYC updation.**

Remember this

- OTP e-KYC: **₹1 lakh** balance, **₹2 lakh** credits a year, **₹60,000** term loan, full KYC in **1 year**.

Topic 9 — Digital Payment Security Controls

For commercial banks, the RBI **Digital Payment Security Controls Directions, 2026** apply; other bank categories have separate directions.

Area	Requirement
Authentication	Unless expressly relaxed, electronic payments need multi-factor authentication with at least one dynamic or non-replicable factor
Session and account controls	Secure sessions, failed-attempt blocking , alerts, protection of beneficiary and limit changes, risk-based adaptive authentication
Monitoring	Watch suspicious patterns and analyse fraud
Reconciliation	Settlement files reconciled in real or near-real time, not later than 24 hours from receipt
Customer option	Digital products only on a specific written or authenticated electronic request , with acknowledgement of terms
In-app information	Secure use, rights, liabilities, grievance and dispute timelines; authenticated fraud reporting

Threat	How it works
Phishing	Deceptive links or messages to obtain credentials
Vishing	Phone calls to obtain credentials
Remote-access apps	Expose the device and accounts to fraudsters

Customers should use only authorised apps, **never share PIN, password or OTP**, and report suspicious transactions promptly through the bank's official channels.

Topic 10 — Customer Liability in Unauthorised Electronic Transactions

- **Source** — The RBI **Responsible Business Conduct Directions** for commercial banks govern liability.
- **Basis** — Liability depends on **who was at fault** and **how quickly** the customer reports.
- **Counting days** — Working days follow the **home branch** schedule, **excluding** the date of the bank's communication.

Situation	Customer liability
Bank's fraud, negligence or deficiency	Zero , whether reported or not
Third-party breach, reported within 3 working days	Zero
Third-party breach, reported in 4–7 working days	Transaction value or cap below, whichever is lower
Reported after 7 working days	As per the bank's Board-approved policy
Customer negligence (credentials shared)	Full loss until reporting ; loss after reporting borne by the bank

Account type	Cap (4–7 working days)
BSBD accounts	₹5,000
Other savings accounts; prepaid and gift cards; MSME current/CC/OD; individual current/CC/OD with average balance up to ₹25 lakh ; credit cards with limit up to ₹5 lakh	₹10,000
All other current/CC/OD accounts; credit cards with limit above ₹5 lakh	₹25,000

Liability for a third-party breach reported in 4–7 working days, where V is the transaction value:

$$\text{Liability} = \min(V, \text{Cap})$$

Example: Savings account, third-party breach reported on the 5th working day, unauthorised debit ₹14,000: liability = $\min(\text{₹14,000}, \text{₹10,000}) = \text{₹10,000}$; the bank bears ₹4,000.

- **Shadow reversal** — It is due within **10 working days** of notification, value-dated to the unauthorised transaction.
- **Resolution** — Liability must be decided and the complaint resolved within **90 days**.
- **Burden of proof** — The **burden of proving** customer liability lies on the **bank**.

Revised framework from 1 January 2027

- **Start date** — RBI's revised framework applies from **1 January 2027** and is **not to be applied earlier**.
- **Zero liability** — Applies for a third-party breach reported within **5 calendar days**.
- **Resolution time** — **45 days** (60 days for cross-border).
- **Small-fraud compensation** — One-time **85% of net loss** or **₹25,000, whichever is lower**, for net loss up to **₹50,000**.

Remember this

- Now: **3 days** zero; **4–7 days** cap ₹5,000 / ₹10,000 / ₹25,000; shadow reversal **10 working days**; resolve in **90 days**.

Topic 11 — Grievance Redressal: RBI Integrated Ombudsman Scheme, 2026

- **Merger** — The **Digital Transactions Ombudsman Scheme** was merged into the RBI Integrated Ombudsman Scheme, 2021.
- **Current scheme** — The **Reserve Bank – Integrated Ombudsman Scheme, 2026 (RB-IOS 2026)** applies from **1 July 2026**.
- **Earlier complaints** — Complaints filed before that stay under the saving provisions.

Step / item	Rule
First step	Complain to the regulated entity and keep proof
When to approach the Ombudsman	Unsatisfactory reply, or no reply within 30 days or the applicable RBI / NPCI / card-network timeline, whichever is higher
Time limit	Within 90 days of expiry of the resolution timeline or the last communication from the entity, whichever is later
Compensation – consequential loss	Up to ₹30 lakh
Compensation – loss of time, expenses, harassment, mental anguish	Up to ₹3 lakh

Maximum award, where L is the proved consequential loss and H the claim for time, expenses and harassment:

$$\text{Award}_{\text{max}} = \min(L, 30 \text{ lakh}) + \min(H, 3 \text{ lakh})$$

Example: Proved loss ₹42 lakh and harassment claim ₹5 lakh: maximum award = ₹30 lakh + ₹3 lakh = **₹33 lakh**.

Remember this

- Ombudsman: wait **30 days**, file within **90 days**, award up to **₹30 lakh + ₹3 lakh**.

DB | Module A | CH-1 | MCQs

Q1. A bank's app shows a loan offer on screen while the customer is checking the balance, based on analytics run in the background. This illustrates:

- (a) Integrity under the CIA triad
- (b) Customer centricity through up-sale using customer data
- (c) Digital KYC
- (d) A third-party breach

Q2. Which statement on customer analytics and KYC is correct?

- (a) Analytics can replace KYC if the customer transacts online
- (b) KYC is needed only for customers who use branches
- (c) Analytics helps understand preferences but does not replace KYC and must respect consent and privacy
- (d) Analytics data can be used without customer consent

Q3. Posting a transaction changes an account balance while the audit trail and supporting records are kept. This reflects which element of information security?

- (a) Confidentiality
- (b) Availability
- (c) Non-repudiation
- (d) Integrity

Q4. Keeping internet banking accessible to authorised users at the agreed times and places is the information-security goal of:

- (a) Availability
- (b) Integrity
- (c) Confidentiality
- (d) Authentication

Q5. Developing, training and retaining staff skilled in security planning and execution addresses which security issue?

- (a) Governing the enterprise
- (b) Security capability need
- (c) Dovetailing security with business
- (d) Keeping pace with persistent threats

Q6. A customer opened an account through OTP-based non-face-to-face e-KYC. Which of these is permitted?

- (a) A cash credit limit of ₹50,000
- (b) Aggregate deposit balance of ₹1.5 lakh
- (c) A term loan of ₹55,000 in the year
- (d) Credits of ₹2.5 lakh in the financial year

Q7. An OTP e-KYC account holder has a balance of ₹62,000. How much more can be held before the aggregate balance cap is reached?

- (a) ₹1,38,000
- (b) ₹62,000
- (c) ₹2,000
- (d) ₹38,000

Q8. If full identification or compliant V-CIP is not completed within one year for an OTP e-KYC account, the bank must:

- (a) Close the deposits and stop further loan debits
- (b) Raise the balance limit to ₹2 lakh
- (c) Convert it into a BSBD account automatically
- (d) Freeze it for another one year

Q9. Under the digital payment security framework, settlement files must be reconciled not later than:

- (a) 3 working days from receipt
- (b) 7 days from receipt
- (c) 24 hours from receipt
- (d) End of the month

Q10. A fraudster calls a customer posing as a bank officer and asks for the OTP. This is:

- (a) Phishing by e-mail
- (b) Skimming
- (c) SIM swap
- (d) Vishing

Q11. A savings account holder (not BSBD) reports a third-party breach on the 6th working day; the unauthorised debit is ₹8,000. Customer liability is:

- (a) ₹8,000
- (b) ₹10,000
- (c) ₹5,000
- (d) Zero

Q12. A customer with a credit card of limit ₹7 lakh reports a third-party breach on the 4th working day; the unauthorised debit is ₹40,000. Customer liability is:

- (a) ₹10,000
- (b) ₹25,000
- (c) ₹40,000
- (d) Zero

Q13. An unauthorised debit occurred because of a deficiency in the bank's system; the customer reported it after 12 working days. Customer liability is:

- (a) As per Board-approved policy
(b) Full amount
(c) Zero
(d) Capped at ₹25,000

Q14. Under RB-IOIS 2026, a complainant proves consequential loss of ₹36 lakh and claims ₹4 lakh for harassment. The maximum award is:

- (a) ₹33 lakh (b) ₹40 lakh (c) ₹30 lakh (d) ₹36 lakh

Q15. A customer may approach the Ombudsman under RB-IOIS 2026 when the regulated entity has not replied within:

- (a) 15 days of the complaint
(b) 30 days or the applicable RBI/NPCI/card-network timeline, whichever is higher
(c) 7 working days of the complaint
(d) 90 days of the transaction

Answer key

Q	Ans	Q	Ans	Q	Ans	Q	Ans	Q	Ans
1	b	4	a	7	d	10	d	13	c
2	c	5	b	8	a	11	a	14	a
3	d	6	c	9	c	12	b	15	b

CH-2 Cards

Topic 1 — Payment Cards and Card Standards

- Magnetic-stripe cards** — They spread in transport and payments in the second half of the twentieth century.
- Standardisation** — They were **standardised across the industry** as the information age began.
- Debit growth** — Debit cards grew through **ATM, PIN-based POS** and other acceptance arrangements.
- Older mode** — **Signature-based** debit was another, older mode of cardholder verification.
- Size** — Plastic cards are usually **85.60 × 53.98 mm** so that they fit a wallet.
- ISO standards** — They cover dimensions, mechanical strength, electrical properties and card slots in ATMs and POS.
- Interoperability** — Cards from any producer therefore work across the industry.
- ISO/IEC 7813** — It defines physical characteristics (size, shape, magnetic stripe location) and magnetic track data structures of financial transaction cards.

Every card is **linked to an account** at the back end with the bank or non-bank entity that issued it.

Topic 2 — Types of Cards

Card	Features
Debit card	Cash at ATMs, payment at merchant PoS and online; the bank account is debited when the transaction is processed
Credit card	Used against a line of credit ; repay in full or in part (monthly minimum repayment); PoS and online use
ATM-only card	Permitted ATM services including cash withdrawal; no PoS or e-commerce payments
Prepaid card (PPI)	Purchases, financial services and remittances against stored value
Stored value card	Prepaid value kept on the card or in the issuer's system; e.g. most metro rail cards , where fare is deducted at entry
Charge card	Like a credit card, but the entire usage is repaid at one go at the end of the grace period
Virtual card	Digital debit, credit or prepaid credentials; limits, expiry and single or repeat use set by the issuer

Online transactions are **Card Not Present (CNP)** transactions: only the card number, validity date and **Card Verification Value (CVV)** are used and the physical card is not presented.

For a virtual card, the issuer securely notifies the **cardholder's name, card number, expiry date and Card Verification Data number (CVD2)**.

Topic 3 — Prepaid Payment Instruments

- PPIs — Prepaid Payment Instruments (PPIs)** enable purchases, financial services and remittances against value stored on them.
- Current classes** — RBI-authorised PPIs are now **Small PPIs** and **Full-KYC PPIs**.
- Restricted class** — **Gift PPIs** form a restricted category.

Category	Limits and permitted use
Small PPI	Outstanding up to ₹10,000 ; loading up to ₹10,000 a month and ₹1,20,000 a financial year ; purchases only, no cash withdrawal or funds transfer ; cash-loading variant to be converted to full KYC within 24 months
Full-KYC PPI	Issued by banks and permitted non-banks after full KYC; outstanding normally up to ₹2 lakh ; purchases, permitted transfers and cash withdrawal
Cash withdrawal (non-bank Full-KYC PPI)	Up to ₹2,000 per transaction and ₹10,000 per month across channels
Gift PPI	Up to ₹10,000 ; non-reloadable ; no cash withdrawal or funds transfer except return to source account with consent

Full-KYC wallet PPIs can be linked to **third-party UPI apps**; card PPIs use authorised **card-network interoperability**.

Older classification	Feature
Closed system	Used only at the issuer's own outlets; no cash withdrawal; not a payment system as no third-party settlement (e.g. a bookstore or restaurant card)
Semi-closed system	Used at a group of identified merchants under contract with the issuer; no cash withdrawal
Open system	Used at any card-accepting merchant; cash withdrawal at ATMs / BCs

- Single-purpose (closed-loop)** — These serve a specific merchant or purpose, such as store cards, prepaid telephone cards and employer benefit cards.
- Multi-purpose** — These may carry a network brand and are accepted at participating merchants.