oliveboard

PPB

Crash course

Module- C

Lec-5

oliveboard

Security Considerations and Mitigation Measures in Banks

Cybersecurity in Banking: Managing Risk in the Digital Age

The Digital Banking Landscape

Technology Transformation

Banks have revolutionized operations through digital platforms, mobile banking, wallets, and 24x7 services. Government's push toward a cashless economy has accelerated adoption.

Rising Cyber Threats

Unprecedented growth in digital payments brings renewed focus on cybersecurity. Criminal sophistication and organization produce ominous results for financial institutions.

Critical Risk Areas

Data & Software

Critical resources vulnerable to tampering, unauthorized access, and fraudulent modifications that bypass security controls.

Infrastructure

Hardware components, power systems, and environmental controls requiring regular maintenance to prevent service interruption.

Peopleware

Human resources managing systems face risks from skill stagnation, high turnover, and potential insider threats.

Major Threat Categories

Accidental Damages

Human failures, natural calamities, and improperly tested systems leading to higher failure rates and processing errors.

Environmental Hazards

Fire, power instability, humidity, water damage, and radio interference affecting system operations and data transmission.

Malicious Attacks

Disgruntled employees and cybercriminals exploiting system vulnerabilities for financial gain or service disruption.

Common Cyber Attack Methods

1

ATM Card Skimming

Fraudsters install skimming devices and cameras to capture card data and PINs, creating duplicate cards for unauthorized withdrawals.

2

Phishing/Vishing/Smishing

Spoofed communications designed to extract confidential banking details through emails, phone calls, or text messages.

3

Social Engineering

Imposters pose as bank officials or government agents to pressure customers into revealing sensitive authentication credentials.

Advanced Fraud Techniques

Account Takeover

Criminals obtain access through data breaches and impersonate cardholders to request replacement cards or change account details.

Business Email Compromise

Attackers impersonate business networks to fool targets into transferring money to criminal accounts, particularly targeting cross-border payments.

SIM Swapping

Fraudsters collect personal information to obtain duplicate SIM cards, intercepting OTP codes for unauthorized digital transactions.

Control Mechanisms Framework

01

Preventive Controls

Eliminate errors before they occur through good user interface design, input validation, and security protocols.

02

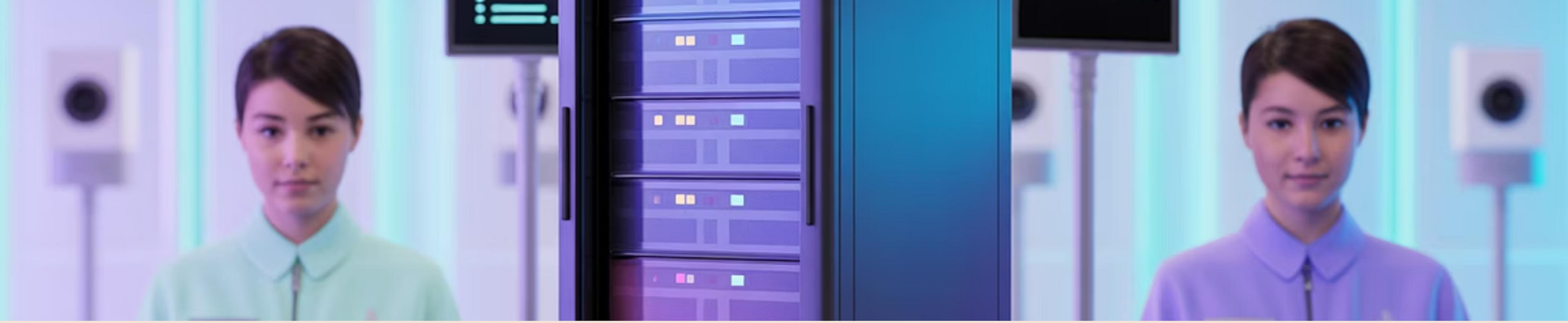
Detective Controls

Identify irregularities after occurrence through monitoring systems, audit trails, and anomaly detection.

03

Corrective Controls

Remove or reduce effects of identified problems through automated recovery processes and incident response.



Physical Security Controls

Access Control

Restrict physical access to computer rooms, media, and documentation. Implement password protection, PINs, and biometric verification systems.

Output Security

Preserve hard copies of critical reports with proper access controls and maintain secure storage protocols.

Environmental Protection

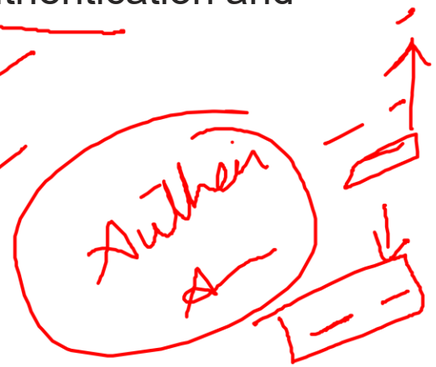
Regular checks of fire extinguishers, smoke detectors, and hardware failure protections to ensure operational continuity.

Logical & Internal Controls

Authentication & Authorization

Operating systems and databases control access at directory, file, record, and field levels. Systems administration manages user authentication and authorization.

- User identity verification
- Minimum access privileges
- Session management



Application Controls

Built-in accounting and administrative controls ensure data accuracy and operational efficiency.

- Dual controls and authorizations
- Data validation checks
- Numerical sequencing
- Transaction limits verification

Data Protection Mechanisms

Data Encryption

Systematic conversion of data into ciphertext using algorithms and keys. Message authentication codes (MAC) verify data integrity during transmission.

Audit Trails

Chronological records of all system events, maintaining accounting and operations trails for monitoring and irregularity detection.

Checksums

Generated numbers based on key data items to ensure file integrity, particularly critical in branch banking environments.

Computer Audit Approaches

Audit Around

Examine input/output without direct software examination. Suitable for simple systems with clear audit trails.

Audit Through

Use computers to test logic and controls within systems. Essential for complex applications with large data volumes.

Audit With

Deploy Computer-Aided Audit Tools (CAATs) for efficient evaluation of computerized files and internal controls.

Information System Security Objectives

Confidentiality

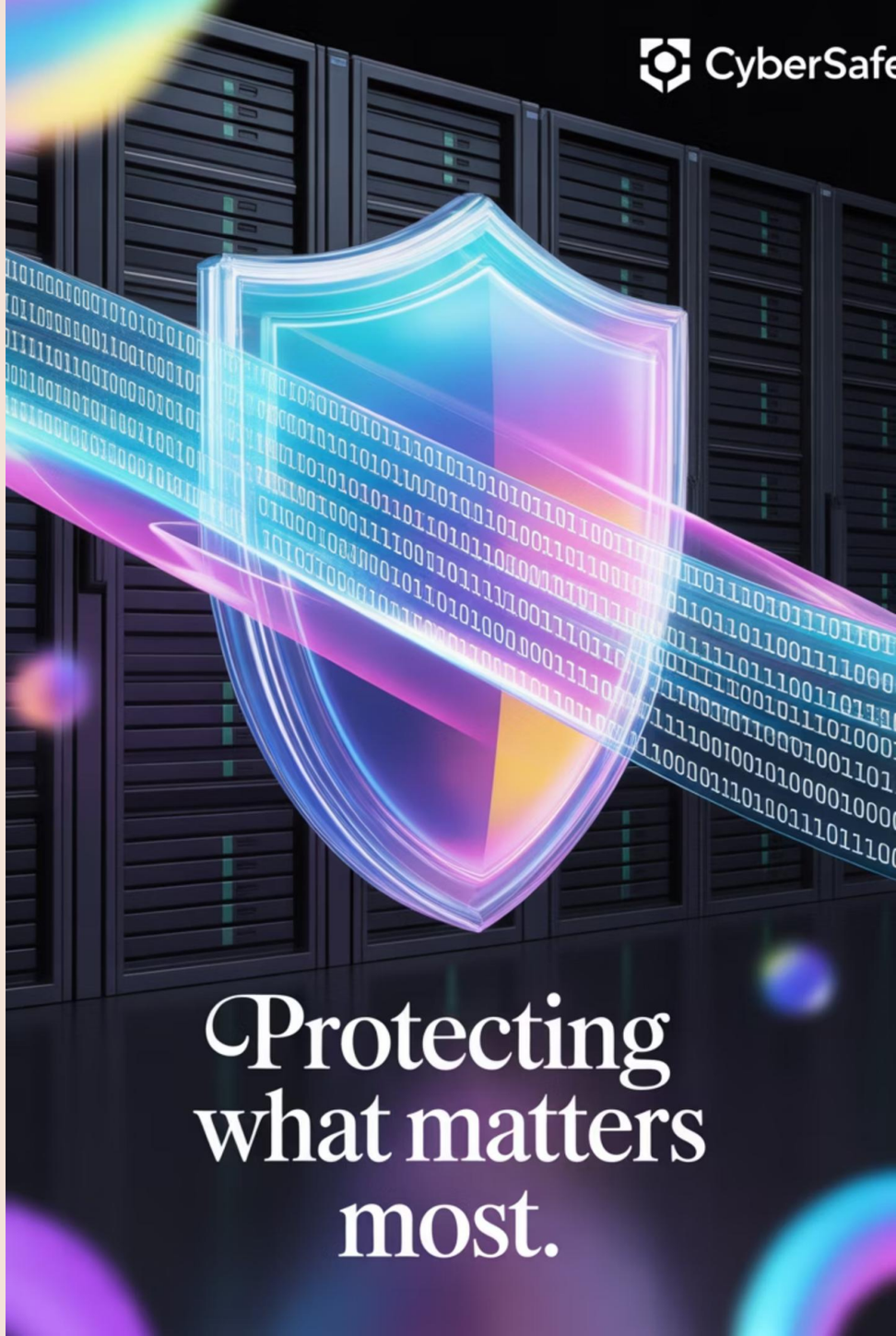
Ensure information disclosure only to authorized users through access controls and encryption protocols.

Integrity

Guarantee that information modifications occur only by authorized users in authorized manners.

Availability

Maintain information accessibility to authorized personnel when required for business operations.



Authentication Methods

Knowledge Factor

Something the user knows - passwords, PINs, or cryptographic keys that verify identity through secret information.

Possession Factor

Something the user possesses - ATM cards, smart cards, or tokens that provide physical authentication credentials.

Biometric Factor

Something the user is - fingerprints, iris scanning, facial recognition, or voice patterns for unique identification.

Major Cybersecurity Threats

1

Malware & Viruses

Malicious software programs designed to harm computers, steal data, and destroy information systems.

2

DDoS Attacks

Distributed denial-of-service attacks using compromised systems to overwhelm and shut down target services.

3

Ransomware

Malicious software that blocks data access or threatens to publish victim information unless ransom is paid.

Safe Banking Practices

Password Security

- Change passwords regularly
- Create strong, complex passwords
- Disable auto-save features
- Never share credentials

Online Behavior

- Avoid public computer banking
- Type URLs directly
- Monitor accounts regularly
- Use licensed antivirus software

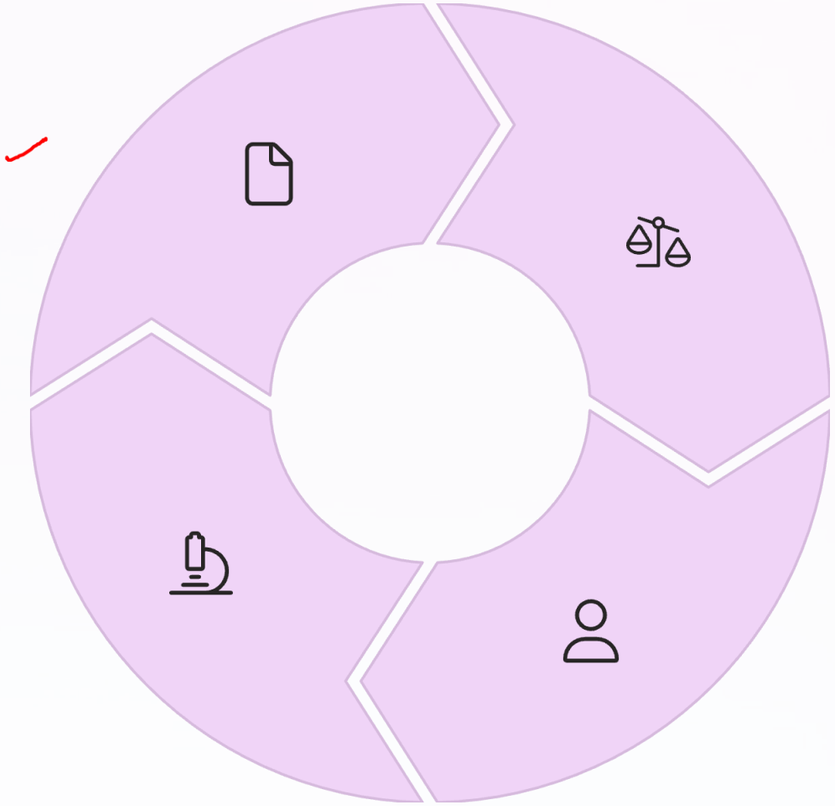
Disaster Recovery Planning

Awareness

Identify critical activities, systems, and resources necessary for business continuity during disasters.

Testing

Conduct regular exercises including tabletop drills and live migration tests to verify plan effectiveness.



Legal & Financial

Maintain proper inventory, insurance coverage, and warranty documentation for all IT assets.

Preparation

Establish core teams, alternate sites, data backups, and comprehensive recovery documentation.

Recovery Objectives

0

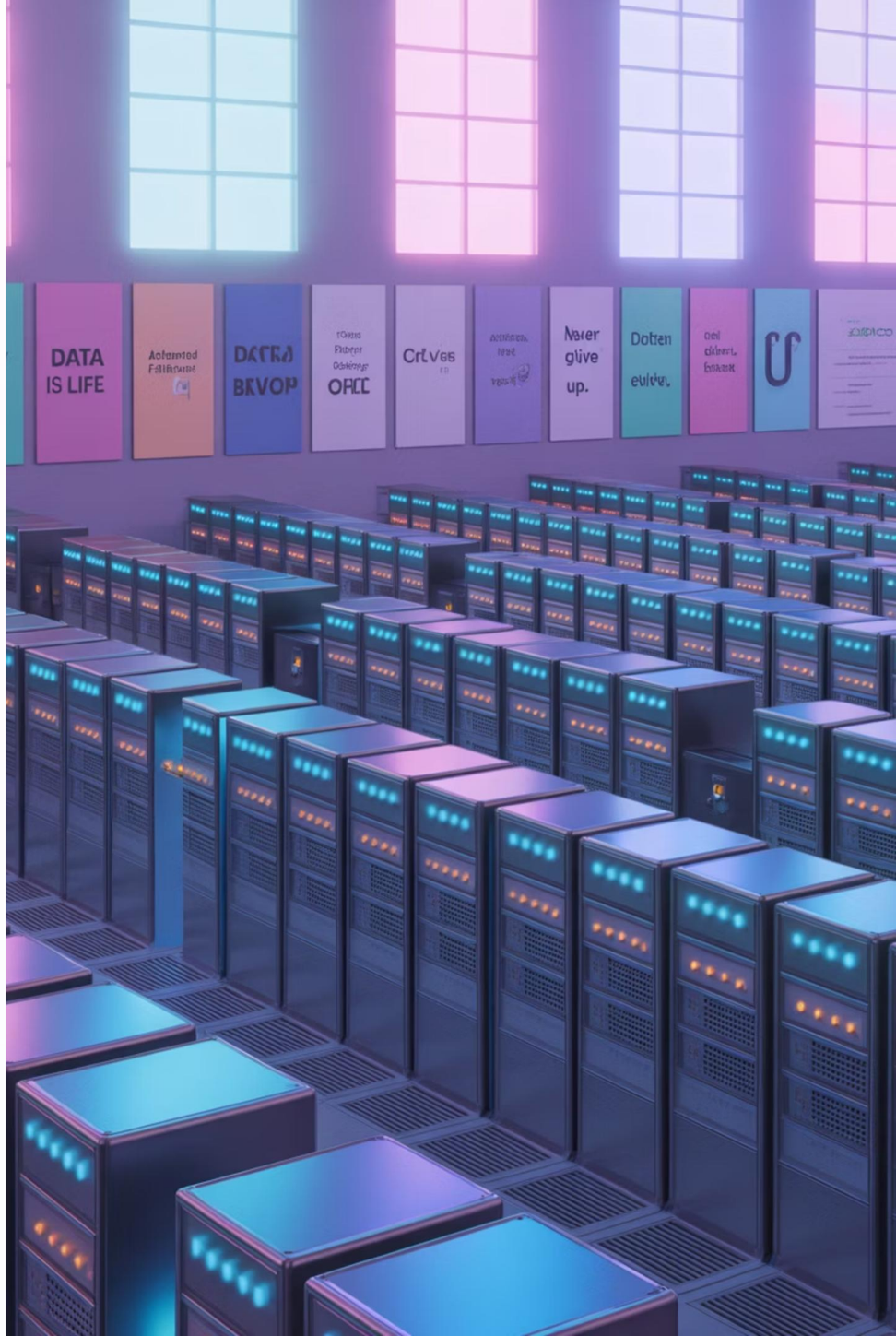
Recovery Point Objective

RPO represents the maximum acceptable data loss measured in time. Banks should ideally maintain zero RPO.

24/7

Recovery Time Objective

RTO defines the maximum acceptable downtime. Critical banking services require minimal recovery time.



Legal Framework: IT Act 2000

1

Electronic Recognition

Provides legal validation for Electronic Data Interchange, Electronic Records, and Electronic Signatures with non-repudiation assurance.

2

Cybercrime Definitions

Identifies IT offences including hacking, data tampering, obscenity, unauthorized access, and breach of confidentiality.

3

Legal Amendments

Updates Indian Penal Code, Evidence Act, and RBI Act to include electronic records and digital signatures.

RBI Cybersecurity Framework

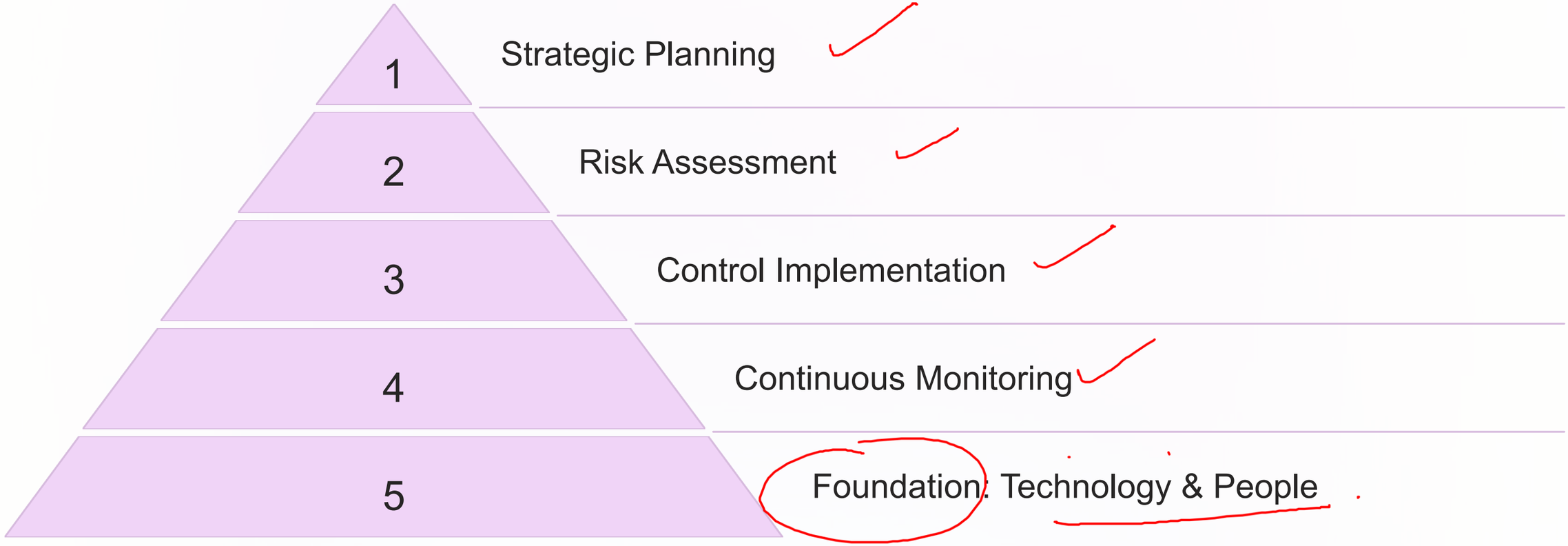
Key Requirements

- Board-approved cybersecurity policy
- Security Operations Centre (SOC)
- Secure IT architecture design
- Customer information protection

Governance & Reporting

- Cyber Crisis Management Plan
- Preparedness indicators
- Incident reporting to RBI
- Stakeholder awareness programs

Building Cyber Resilience



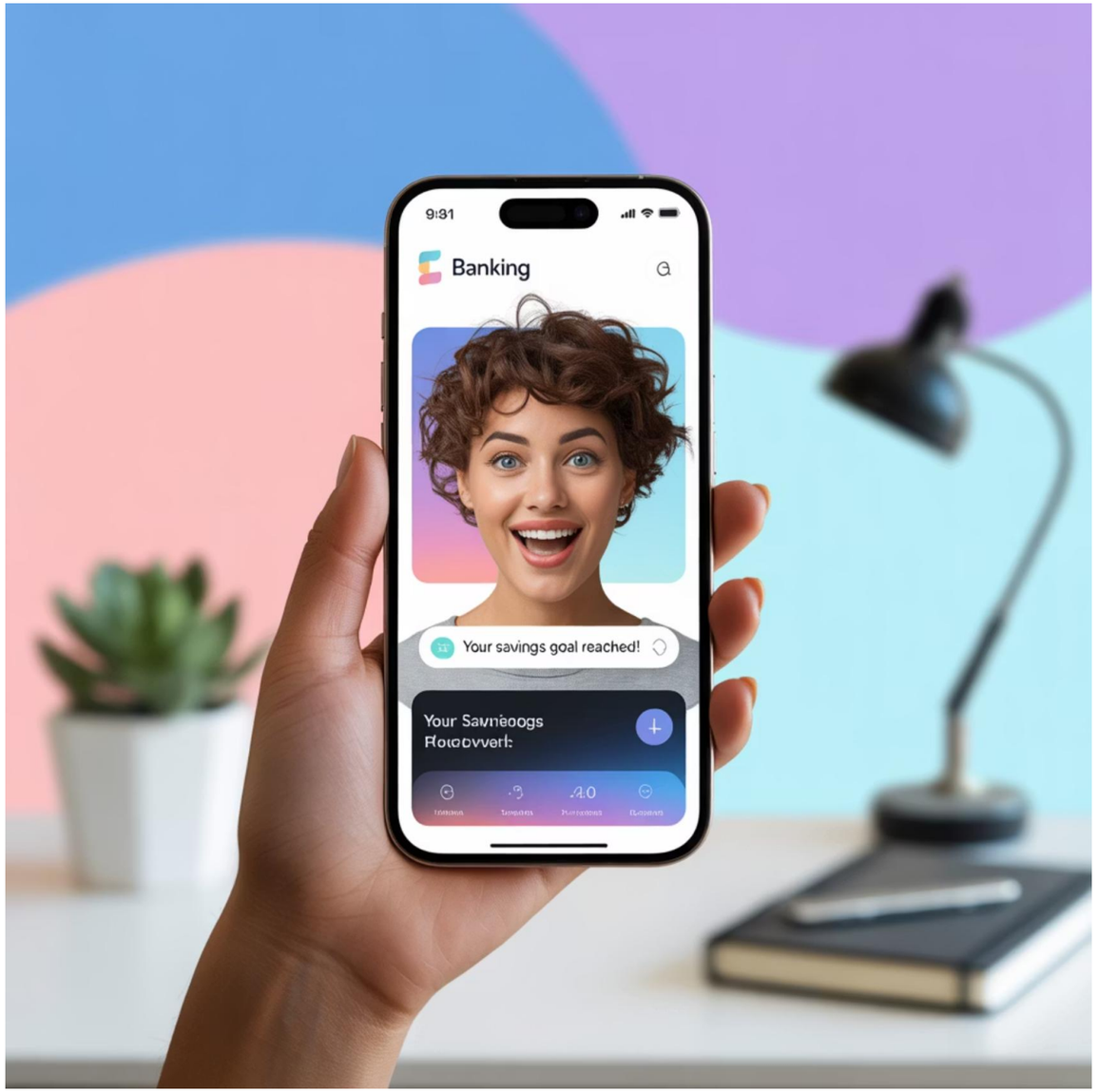
Banks must embed cybersecurity into strategic business planning, treating risk management as value creation rather than cost. Effective cyber resilience requires comprehensive approach combining technology, processes, and people development.

Technology Trends In Banking, E-Rupi, Fintech – Regtech, Suptech, Hashtag Banking Etc.

The Technology-Finance Convergence

Driving Forces

- Growing smartphone penetration worldwide
- Inefficiencies in traditional financial systems
- Evolving consumer behavioral patterns
- Demand for instant, digital-first services



e-RUPI

India's breakthrough digital voucher system revolutionizing targeted payment distribution

Understanding e-RUPI Technology

Launch & Authority

Launched August 2, 2021 by National Payments Corporation of India (NPCI) as an innovative digital payment solution

Mechanism

QR code or SMS string-based e-voucher delivered directly to beneficiaries' mobile devices

Redemption

Users redeem at participating merchants without digital payment apps, cards, or internet banking

e-RUPI Key Features & Benefits

Contactless & Secure

Maintains beneficiary confidentiality with pre-stored amounts, ensuring faster and more reliable transactions than traditional methods.

Offline Capability

Functions without smartphones, making it ideal for remote and rural areas where digital infrastructure is limited.

Wide Adoption

Over 1,600 hospitals and 16 banks now support e-RUPI, with 11 banks actively facilitating transactions.

e-RUPI Ecosystem Stakeholders

01

Issuer Bank

Authorized bank that initiates e-RUPI creation requests and manages the voucher issuance process

02

Sponsor

Corporate entities, government departments, or business customers requesting voucher creation

03

Designated Merchant

Specific acceptance points where beneficiaries can redeem their e-RUPI vouchers

04

Acquiring Bank

Financial institution providing merchants with e-RUPI acceptance and redemption capabilities

e-RUPI Technical Specifications

Authorization & Limits

- Only RBI-authorized PPI banks can issue
- Maximum voucher value: ₹100,000
- Up to 10 vouchers per beneficiary
- No cash-out or cashback permitted

User Benefits

- No charges for beneficiaries
- Digital-only distribution
- No bank account required
- Prepaid gift voucher functionality

Corporate Benefits of e-RUPI

1

Employee Well-being

Enable targeted employee benefits and wellness programs through secure digital vouchers

2

Cost Reduction

End-to-end digital transactions eliminate human intervention and reduce operational costs

3

Tracking Capability

Real-time monitoring of voucher redemption provides valuable usage analytics

4

Distribution Efficiency

Quick, safe, and contactless voucher distribution streamlines benefit programs

Merchant & Consumer Advantages

Merchant Benefits

- **Secure Authorization:** Verification code system ensures transaction security
- **Contactless Payments:** No cash handling required
- **Quick Redemption:** Pre-blocked amounts reduce decline rates

Consumer Benefits

- **Privacy Protection:** No personal details shared during redemption
- **Easy Process:** Simple 2-step redemption
- **No Prerequisites:** No digital payment app or bank account needed

e-RUPI vs UPI: Key Distinctions

Difference between e-RUPI and UPI	
e-RUPI	UPI
e-RUPI is one time cashless and contactless payment mechanism.	UPI is an application used for receipt or payment of money
e-RUPI is an e-voucher.	UPI is an application used for receipt or payment of money.
The Reserve Bank of India operates e-RUPI.	The National Payments Corporation of India operates UPI.
e-RUPI vouchers can be redeemed at service providers counters.	UPI is used for receipt or payment of money.

UPI

Real-time payment application for money transfer operated by NPCI, requiring bank accounts and digital apps

e-RUPI

Purpose-specific digital voucher system that works offline without bank accounts or payment apps

Fintech Ecosystem

Exploring the convergence of RegTech and SupTech in modern financial services

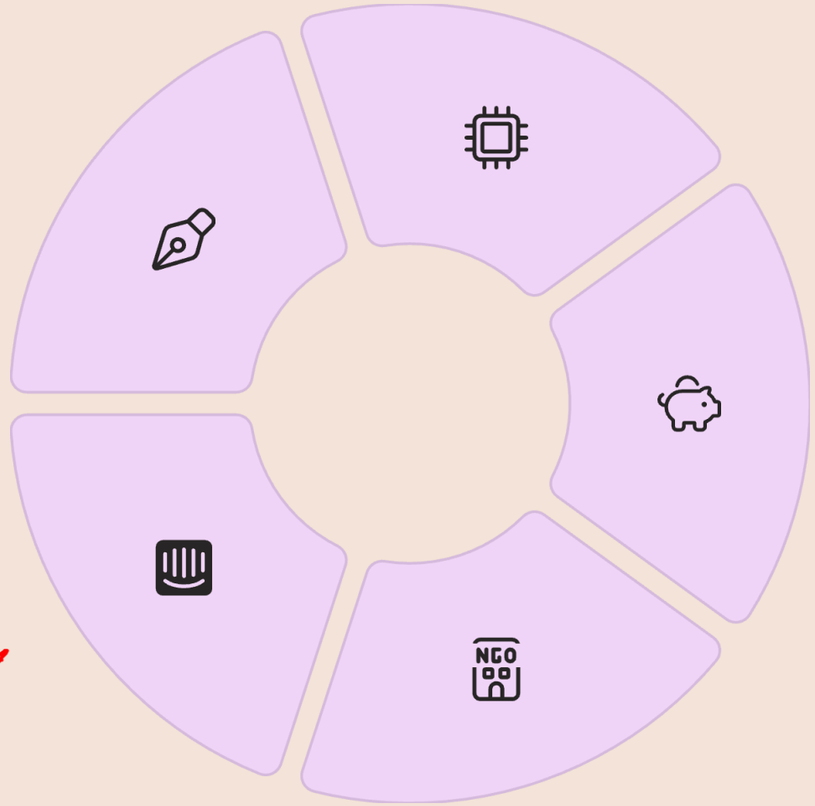
Defining Financial Technology

Startups

Innovative companies developing new financial solutions

Customers

End users driving demand for digital financial services



Big Tech

Large technology companies entering financial services

Traditional Banks

Established financial institutions adopting new technologies

Government

Regulatory bodies and policy makers enabling innovation

Fintech leverages specialized software and algorithms to improve financial operations, procedures, and customer experiences across all ecosystem participants.

Core Fintech Technologies

Peer-to-Peer Lending

Direct lending platforms connecting borrowers with investors without traditional intermediaries

Blockchain & DLT

Distributed ledger technologies enabling secure, transparent transactions and smart contracts

Big Data Analytics

Advanced data processing for risk assessment, customer insights, and automated decision-making

Robo Advisors

AI-powered investment management platforms providing automated financial planning services

Banking Benefits from Fintech Adoption

Reduced Operational Costs

Automation and digital processes significantly lower overhead expenses

Faster Time to Market

Rapid deployment of new financial products and services

Enhanced Customer Experience

Improved service delivery leading to increased revenue opportunities

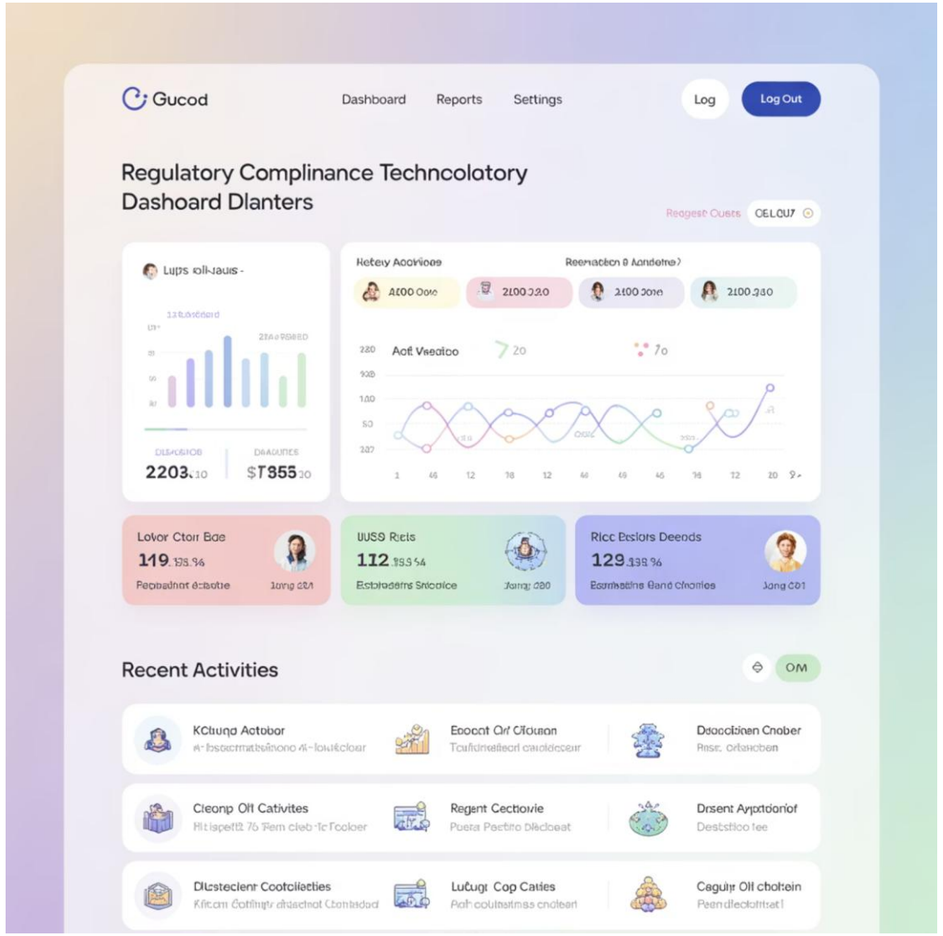
Advanced Security

World-class compliance systems and robust security frameworks

RegTech: Regulatory Technology Revolution

What is RegTech?

Technology solutions that streamline regulatory processes, helping financial institutions manage compliance more efficiently through automation and advanced analytics.



Key Applications

- Regulatory monitoring and reporting
- Compliance management automation
- Risk assessment and mitigation
- Real-time regulatory tracking

RegTech Implementation Areas

Regulatory Monitoring

Real-time tracking of regulatory changes and requirements

Compliance Management

Automated systems for managing regulatory obligations

Risk Management

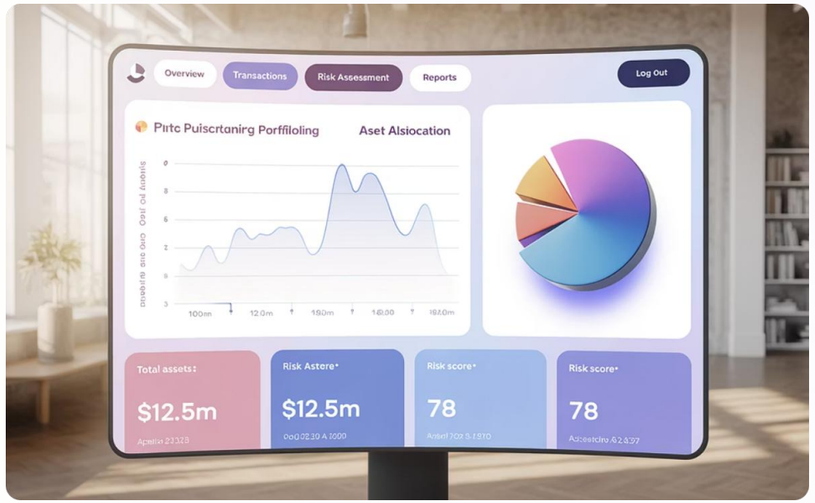
Advanced analytics for identifying and mitigating compliance risks

Transaction Monitoring

AI-powered systems for detecting suspicious activities

RegTech leverages AI, machine learning, big data, and cloud computing to minimize human error while enabling rapid adaptation to new regulations.

SupTech: Supervisory Technology



Enhanced Supervisory Efficiency

Technological tools that help regulatory authorities improve oversight through automation and data analytics

RBI Implementation

Reserve Bank of India uses systems like IDPMS, EDPMS, and CRILC for comprehensive data collection and analysis

Social Media Banking Evolution

Market Reality

Billions of users globally rely on social media platforms like Instagram, Facebook, LinkedIn, and Snapchat, making social media presence essential for modern banking.

Hashtag Banking Services

Core Banking Operations

Fund transfers, balance inquiries, and account management through Twitter hashtags

Credit Card Services

Card management, payment processing, and customer support via social platforms

Digital Payment Integration

FASTag services, mobile recharges, and digital wallet management

Product Services

Loan applications, fixed deposits, and card blocking/unblocking functionality

Customers follow their bank on Twitter to access these services, appealing especially to socially active younger demographics.

The Future: Account Aggregators & Open Banking

1. **Account Aggregators**

   RBI-regulated entities enabling secure digital sharing of financial information between institutions with customer consent

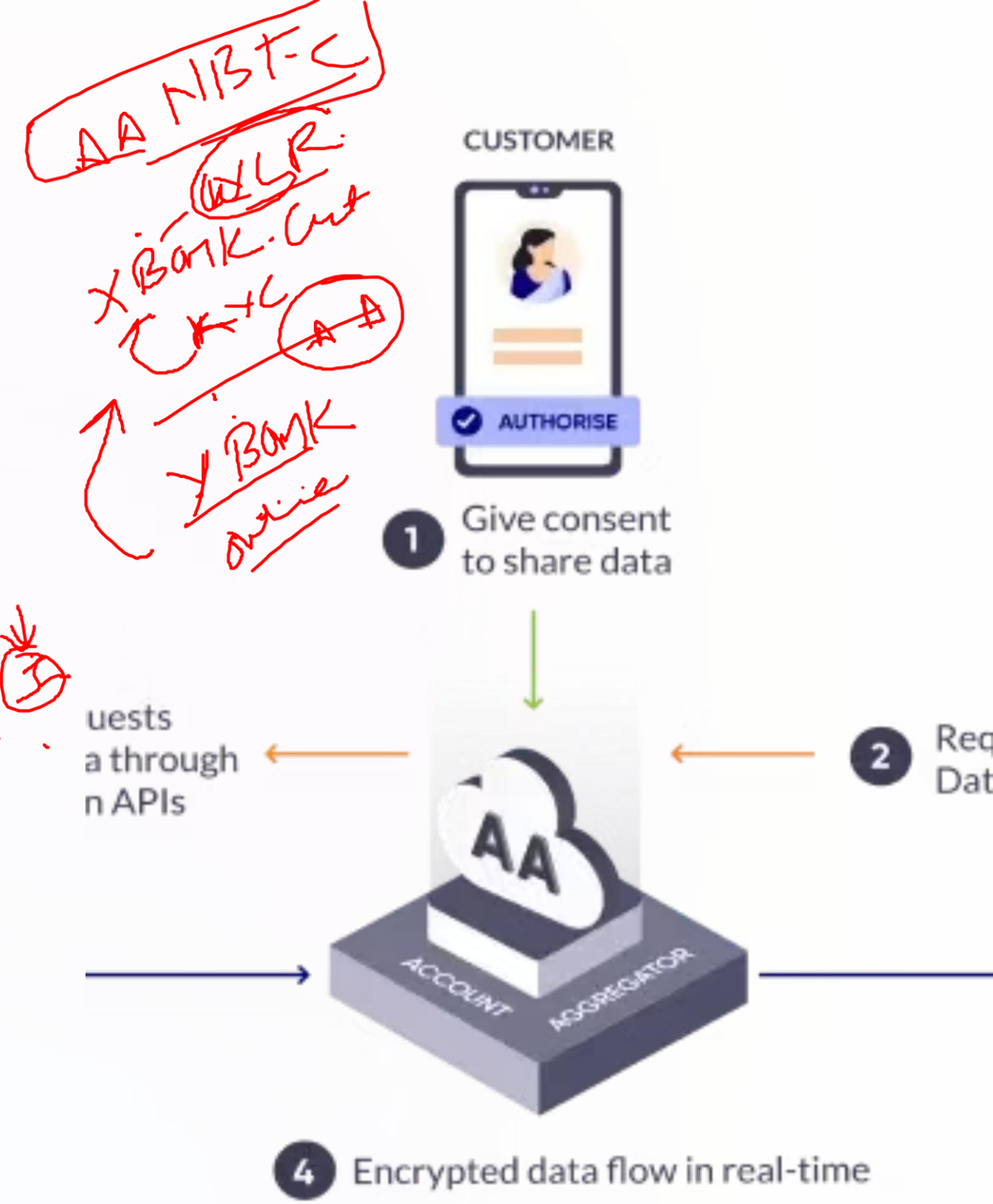
2. **Open Banking**

   API-driven ecosystem allowing third-party providers access to banking data, fostering innovation and competition

3. **API Integration**

   Application Programming Interfaces enabling seamless data exchange and service integration across financial platforms

These technologies create interconnected financial ecosystems that prioritize customer control, data security, and innovative service delivery.



Thank You

Comment Your Feedback