

Group – 3 Financial Management System (FinSecure Bank)

Group member:

student id:

- | | |
|--------------------------------|----------------|
| 1) Dipkumar Patel | 2535265 |
| 2) Dev Gajera | 2538542 |
| 3) Prem Joshi | 2537632 |
| 4) Yaskumar Bhingradiya | 2528447 |

Week 2: The Need for Security

Date: 16 June 2026

Executive Summary

As the banking industry continues to adopt cloud-based and API-driven technologies, the number of potential cybersecurity risks has increased significantly. FinSecure Bank manages not only financial assets but also large amounts of sensitive customer information, making security a critical business requirement.

This report outlines the security foundations of the FinSecure platform. It examines the importance of security in modern banking, identifies key threats facing financial institutions, reviews relevant legal and regulatory requirements, introduces a Zero-Trust security model, and discusses the measures needed to protect customer data and maintain system reliability.

The Core Drivers of Financial Security

Moving from system design to system protection requires a strong focus on the principles of information security. For FinSecure Bank, these principles are based on the CIA Triad—Confidentiality, Integrity, and Availability—along with non-repudiation.

1. The CIA Triad in Banking

Confidentiality

Customer information, including account balances, transaction histories, and personal details, must be protected from unauthorized access. Any exposure of this data could result in serious privacy breaches, financial losses, and damage to customer trust.

Integrity

Financial data must remain accurate and protected from unauthorized modification. For example, no user should be able to alter account balances or transaction records without proper authorization. Maintaining data integrity ensures that all banking information remains reliable and trustworthy.

Availability

Banking services are considered essential infrastructure. Customers depend on access to their accounts for daily activities such as making purchases, paying bills, and managing finances. To support this, FinSecure aims to achieve 99.999% uptime, ensuring that services remain available even during periods of high demand or cyberattacks.

2. Non-Repudiation and Auditability

Every action performed within the FinSecure system must be traceable and verifiable. When a transaction takes place, the system records details such as who initiated the action, when it occurred, and where it originated. Secure audit logs provide evidence that can be used to investigate disputes, detect fraud, and support regulatory compliance.

The 2026 Banking Threat Landscape

Financial institutions face increasingly sophisticated cyber threats from organised criminal groups, state-sponsored attackers, and automated attack networks. Many of these threats now make use of artificial intelligence to improve their effectiveness.

Threat Type	Description	Target Area
AI-Generated Phishing	Highly personalised phishing emails and messages created using large language models to deceive employees and customers.	Employee devices and customer login portals
Ransomware and Data Exfiltration	Malware that steals sensitive information before encrypting systems and demanding payment.	Cloud storage systems and internal documents
API Swarming	Automated attacks targeting application programming interfaces (APIs) to discover vulnerabilities or gain unauthorized access.	Mobile banking applications and microservices
Deepfake Identity Fraud	Synthetic audio and video used to impersonate legitimate users during identity verification processes.	Customer onboarding and KYC procedures
Supply Chain Attacks	Malicious code introduced through third-party software components or open-source dependencies.	Software development and CI/CD pipelines

The Cost of Failure

A successful cyberattack can have serious consequences for a financial institution. These include direct financial losses, regulatory penalties, operational disruption, and long-term damage to the bank’s reputation. Maintaining strong security controls is therefore essential for both legal compliance and customer confidence.

Regulatory Compliance and Legal Frameworks

Financial organisations must comply with a range of regulations designed to protect customers, ensure operational resilience, and reduce cybersecurity risks.

Major Regulatory Frameworks

1. PCI DSS v4.0 (Payment Card Industry Data Security Standard)

PCI DSS defines security requirements for handling payment card information. It requires measures such as network segmentation, strong encryption, vulnerability management, and regular security testing.

2. GDPR and the UK Data Protection Act

These regulations govern the collection, processing, and storage of personal data. FinSecure must ensure that customer information is processed lawfully, stored securely, and deleted when no longer required. Customers must also be able to exercise rights such as the “Right to be Forgotten.”

3. Digital Operational Resilience Act (DORA)

DORA focuses on strengthening the resilience of financial institutions against technology-related disruptions. It requires organisations to prepare for, respond to, and recover from cyber incidents and operational failures.

4. Financial Conduct Authority (FCA) Regulations

The FCA requires financial organisations to maintain effective risk management practices and operational resilience measures that protect consumers and support market stability.

System Architecture: The Zero-Trust Blueprint

Traditional perimeter-based security models are no longer sufficient in modern cloud environments. FinSecure adopts a Zero-Trust Architecture (ZTA), based on the principle of “Never Trust, Always Verify.”

Security Implementation Process

1. Threat Modelling (STRIDE)

Before development begins, systems are assessed using the STRIDE framework to identify potential risks related to:

- Spoofing
- Tampering
- Repudiation

- Information Disclosure
- Denial of Service
- Elevation of Privilege

2. Identity and Access Management (IAM)

User authentication is strengthened through Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC). These controls ensure that users can access only the resources necessary for their roles.

3. Micro-Segmentation

The network is divided into isolated security zones to limit the movement of attackers if a breach occurs. For example, the public-facing web application cannot directly communicate with the database layer.

4. Continuous Validation

Every API request must be authenticated and validated before access is granted. Short-lived JSON Web Tokens (JWTs) are used to verify user identity and permissions across all services.

Data Protection and Security Operations

Protecting customer information requires both strong technical safeguards and continuous monitoring of system activity.

Cryptographic Safeguards

Encryption in Transit

All data transmitted across internal and external networks is protected using TLS 1.3 encryption. Any unencrypted communication is automatically blocked.

Encryption at Rest

Sensitive information, including customer records, account balances, and authentication data, is encrypted using AES-256. Encryption keys are managed and rotated through dedicated Hardware Security Modules (HSMs).

Tokenization

Payment card numbers are replaced with randomly generated tokens within internal systems. This reduces the risk of exposing sensitive card information through logs, applications, or APIs.

Continuous Security Operations

FinSecure uses a Security Information and Event Management (SIEM) platform supported by machine-learning-based anomaly detection. The system continuously analyses user behaviour and network activity to identify suspicious events.

For example, if a customer successfully logs in from London and then attempts to perform a high-value transaction from a Singapore-based data centre only a few minutes later, the system automatically flags the activity as suspicious. Additional identity verification is triggered, the account may be temporarily restricted, and the Security Operations Centre (SOC) is alerted to investigate.
