

GROUP 3:

Janvi (ID: 2543705)

Diya Patel (ID: 2532979)

Sneha (ID: 2544720)

Analysing the Security Needs of FinSecure Bank

FinSecure Bank is a financial institution, such as a bank or investment firm, that offers an online platform for managing accounts, processing transactions, providing loans, and managing investments.

Customers use the platform to check account balances, execute real-time money transfers, apply for digital loans, and track their investment portfolios. Because all these activities happen online, the company collects important information such as customer names, physical addresses, legal identification details, account passwords, transaction records, and credit card/banking credentials.

Analysing security needs means finding out what the financial institution needs to protect, what could go wrong, and what security measures should be used to safeguard capital and data assets.

| The bank needs to protect:

- Customer and employee personal identification information.
- The online banking web portal and dedicated mobile application.
- Real-time payment details, credit card configurations, and transfer logs.
- Loan portfolios, interest matrices, and asset valuations.
- Account statements, wire transfers, deposit proofs, and audit histories.

FinSecure Bank may face threats such as sophisticated database hacking, targeted phishing emails, ransomware, stolen credential attacks, dishonest internal employees, and distributed denial-of-service (DDoS) attacks that make the online platform unavailable.

The institution must make sure that private financial records are only seen by authorised people. It must also keep information completely correct and ensure that its transaction systems are available whenever customers and operational teams need them.

| To improve security, FinSecure Bank should use:

- Complex, strong password policies.
- Multi-factor authentication (MFA) including biometric or hardware keys.
- End-to-end data encryption for stored records and data-in-transit.
- Advanced network firewalls and automated endpoint antivirus software.

- Regular automated system updates and vulnerability patching.
- Immutable, secure offline cloud backups.
- Role-based access controls for internal banking staff.
- Continuous cybersecurity awareness training for all employees.

Incident Response & Business Resilience

The bank should also have a strict plan for dealing with security incidents immediately. For example, if customer account passwords or debit card pins are stolen, it should immediately lock the affected accounts, reset the authentication credentials, thoroughly investigate the root cause of what happened, and quickly inform the impacted customers.

Good security helps FinSecure Bank protect customer wealth, prevent severe financial loss, keep its online infrastructure running perfectly, and maintain lifelong client trust.