15	Internet Source	
16	img1.wsimg.com Internet Source	
17	patents.justia.com Internet Source	
18	www.doi.gov Internet Source	
19	Dietmar P. F. Möller. "Cybersecurity for Network and Information Security", Springer Science and Business Media LLC, 2026 Publication	

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

Table of Contents

Executive Summary **4**
1.0 System & Asset Identification **5**
1.1 System Overview 5
1.2 High-Level Architecture Diagram 6
1.3 Critical Information Assets & Sensitivity Rating 7
1.4 Mapping 10
Key Stakeholders 11
2.0 Threat and Vulnerability Identification **12**
2.1 STRIDE Threat Analysis 12
2.2 Threat-Actor Analysis 15
2.3 Assumptions and Out-of-Scope Items 17
2.3.1 Assumptions 17
2.3.2 Out-of-Scope Items 17
3.0 Risk Analysis: Likelihood & Impact **18**
3.1 Selected Risk Analysis Methodology 18
3.2 Likelihood and Impact Rating 18
3.3 Likelihood Assessment of Identified Risks 20
3.4 Impact Assessment of Identified Risks 22
3.4.1 Justification of Impact Assessment 24
4.0 Risk Assessment Matrix **27**
4.1 Five-by-Five Risk Assessment Matrix 27
4.2 Risk Score and Priority Ranking 29
4.3 Risk-Tolerance Threshold 30
5.0 Mitigation Strategies & Recommendations **33**
5.1 Recommended Controls Following ISO/IEC 27001 (2022) Annex A 33
5.2 Feasibility, Costs and Residual Risk of Each Control 36
5.3 Implementation Roadmap 37
6.0 Conclusion **39**
References **40**
Appendices **43**
Appendix A: DFD Diagram 43
Appendix B: SSS task 4.0.xlsx 43
Appendix C: ITS68504_ SSS_Assignment 43

Executive Summary

This report provides a cyber security threat assessment for a proposed Mobile Banking App that includes Biometric Authentication. Customer information, authentication data, biometric data, financial information and transactions are among the most critical data elements maintained by the system, for which confidentiality, integrity, and availability are essential.

The assessment defines the most important system assets and trust boundaries, data flows and stakeholders. Using the STRIDE framework, the researchers found 12 major threats such as account takeover, bypass of biometric authentication, tampering with API requests, breach of customer database, interception of OTPs, disruption of core banking services, administrative privilege escalation and abuse of third-party access.

To perform risk analysis and measure the likelihood of and impact on the operations, NIST SP 800-30 was chosen as the methodology. The risk matrix indicated that the majority of the risks identified were rated as 'High' and audit log modification and transaction dispute were rated Moderate. The top three risks are account takeover, modification of customer accounts and transactions, exposure of customer account data and outage of core banking functions.

These risks have been mitigated using strategies targeted at the controls of the ISO/IEC 27001:2022 Annex A. Some of these controls are recommended: MFA, encryption, access control, database monitoring, secure communication, database backups, and DDoS protection, vendor agreements, and incident response planning. In summary, the report highlights the need for robust security measures and ongoing surveillance to ensure the trust of customers and to safeguard banking functions.

1.0 System & Asset Identification

This section will analyse the critical asset of the system in order to determine their sensitivity rating and implement security mechanisms in a proper, orderly manner for vulnerable areas.

1.1 System Overview

One of the earliest organizations to utilise the advantage of using mobile phones in businesses are financial organizations. As mentioned by (Avdic, 2019), financial institutions utilise mobile apps as a way to communicate directly with consumers and speeds up the whole tedious process of generating savings in their businesses. Nevertheless, with the advancement of technology, it also comes with the great question of whether security is up to par with the development of technology. (Parusheva, 2015) states that a reliable confirmation of the identification of users through the authentication process is one of the biggest challenges in order to prevent financial fraud. This is where biometric authentication comes into the frame as a security defense mechanism. Based on (Burge, 2023), physical biometrics is an individual's distinct physiological traits that is utilised for identification purposes. Popular examples include fingerprint, facial recognition, and retina scanning. Now, biometric authentication is used for all mobile banking applications in order to ensure the user's identity in accessing the assets and functionalities of the application.

Circling back to banking applications in mobile phones, the application serves many purposes to ease an individual's financial routine in their daily lives. A person can make money transactions, check account balance, oversee budget tracking and inspect cash flows in less than a minute. (Barber & Steere, 2026) stated that 88% of adults in the UK use any form of online banking which is equivalent to 48 million people in the country alone. From this statement, it is clear that banking app users range from adults for personal use, all the way to businesses all over the globe. Besides that, we also need to consider those who are involved in the backend and the stakeholders of the banking app such as operation teams, frontline staff, product owners, compliance officers and third-party service providers. Finally, banking applications operate on multiple environments, the technical foundation consists of Cloud-native and API-first architecture which also includes mobile devices, mobile networks and firewalls (Backbase, 2026).

1.2 High-Level Architecture Diagram

The diagram below shows the relationship between major components, external entities, and data storage.

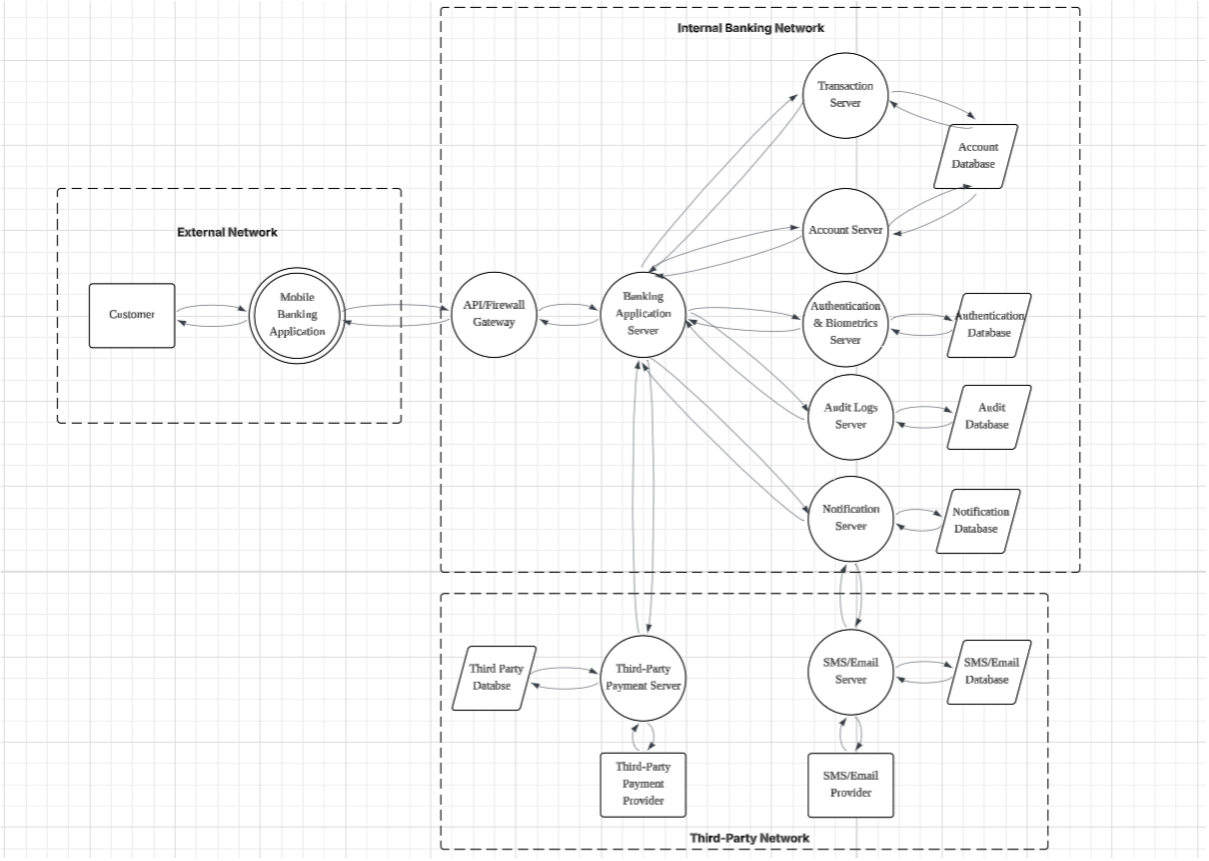


Figure 1.1: *High-Level Architecture Diagram*

Justification

Based on the diagram above, there are 3 trust boundaries within the system. The first boundary would be the external boundary which primarily focuses on the main consumer, customers such as personal users and businesses. The major component involved in the boundary is where the customer will be utilising the mobile banking application which consists of multiple processes within the app itself.

The next trust boundary is the internal banking network. This is where all the processes in the mobile banking application are executed based on a customer's request. Each request will be filtered by API and Firewall gateway. While API ensure all data exchange are communicated, Firewall acts as a defense mechanism by blocking unauthorized access and filter network traffic. After a request is authorised by API and Firewall gateway, then only it will reach the

banking server. The banking server is further broken down into a few smaller sub-servers based on their functionality. Then each server will have their on database to store data.

The first sub-server is the transaction server. It handles all the transaction flow made by the customers. It works very closely with the second sub-server, which is the account server because they will be sharing the same database which is the account database. The difference between transaction server and account server is the type of data they are handling. As mentioned before, the transaction server handles cash flow while the account server handles critical information such as customer data (NRIC, phone number, address, etc.) and account information like card linked, account balance and loan details. The third sub-server is the crucial server in our topic which is the authentication and biometrics server. It handles authentication and biometrics data which is stored in the authentication database. The fourth sub-server is the audit log server which handles all the activity logs within the application to ensure accountability within the system. The last sub-server would be the notification server which works closely with a server from a third-party network.

The last trust boundary is the third-party network. It is not part of the internal banking network because it belongs to external entities who provide service to the banking company. It consists of 2 types of external entities that each will have their respective server and database. The first external entity is the third party payment provider. Their server acts as a sub-server for the mobile banking application server. This is because a transaction from or to a third-party is a very common process in a banking application. The next external entity will be the SMS/Email provider. Their server acts as a sub-server for the notification server as they work together directly compared to the other servers. Both third-party servers consist of their own database to store data which are not to be disclosed to the internal banking network.

1.3 Critical Information Assets & Sensitivity Rating

As quoted by NIST, asset means anything of value to the stakeholders, may be tangible (hardware, device, firmware, etc) or intangible (software,service, data, etc). An asset's value is determined by specific stakeholders in consideration of loss concerns in the entire system life cycle. In terms of mobile banking applications, listed below are the critical assets of a mobile banking application and its sensitivity ranked by CIA.

Table 1.3: *Critical asset and their CIA category*

Asset	Category	Justification
Account Database	Confidentiality	Customer's personal data such as their name, NRIC, phone number, etc. are sensitive information that should not be disclosed with unauthorized individuals. Exposure of these data could lead to identity theft and privacy violation and could cause the company to face a serious lawsuit.
Authentication Database	Confidentiality	Credentials such as password, pin number, OTP, etc. were also the type of information that is usually exploited by unauthorized individuals to gain control over a customer's account.
API Gateway	Confidentiality	APIs handle sensitive data at all times. Thus, every request sent from an app to the banking server through API should be protected from attackers who will attempt to intercept the request and steal customer's information or their authentication tokens.
Banking Database	Confidentiality	The database stores all of the highly sensitive information of each stakeholder that must be protected from data breaches. Unauthorized access to the database would cause a significant problem, as it is the central hub of information storage and exchange.
Transaction records	Integrity	Transaction data must be accurate at all times to ensure that it is not tampered with because it visualises the cash flow within an account. This is to prevent fraud and financial disputes from occurring that can lead to loss of trust. This also assist in audit verifications and cases investigations.
Account Information	Integrity	Account informations such as linked cards, loan details, account balance, etc must be consistent at all times. Changes made by unauthorised personnel will lead to fraudulent transactions, operational disturbance and incorrect banking decisions.
Audit Logs	Integrity	Logs serves as an official record of system usage and user activities. Logs are also important to ensure accountability, detect cyberattacks and tracing suspicious activities. If attackers are able to tamper with the logs, banking company may lose evidence to malicious activities thus complicating the whole investigating process.
Firewall Gateway	Availability	Firewall is a network security system that controls the network traffic based on predefined rules. If a firewall is not available, it also means that the system is losing one of its important defense mechanisms against the attackers.

Authentication & Biometrics Server	Availability	The authentication server must remain available at all times to verify customer's identity and control access to services. Unavailability of authentication server will lead to loss in customer's trust, disruption of operations, and backlash in business continuity. Basically, authentication is an entry point of access and maintaining high availability is critical.
Mobile Banking Application	Availability	The application itself must remain available to provide service to users. System downtime within the app will lead to customers frustration as it disrupts them from accessing their account and completing urgent financial transactions.
Third-Party Payment Gateway	Availability	Third-party payment gateway processes services with external merchants or financial company. Unavailability of third-party payment gateway will cause a major problem as customers have multiple types of account in different banking company.
Database Service	Availability	The database service must remain accessible at all times because the database stores critical information. All banking operations relies heavily on real-time access to the database in order to keep the transaction going.

1.4 Mapping

Based on figure 1.1, (Data Flow Diagram) here are a structured mapping of data flows and trust boundaries with each key stakeholders identified. The purpose of the mapping is to comprehend how data moves through the system and where sensitive information is expose and finally, where security controls are needed.

Table 1.4: *Mapping of data flows within the system*

Source	Destination	Type of Data
Customer	Mobile Banking App	Login credentials, biometric authentication, transaction request, account information
Mobile Banking App	API/Firewall Gateway	Authentication request, transaction request, account information request
API/Firewall Gateway	Banking App Server	Validated customer request
Banking App Server	Authentication Server	Login credentials, MFA request, biometric request
Authentication Server	Authentication Database	User credentials, authentication log, session information
Banking App Server	Account Server	Account balance request, profile data request
Account Server	Account Database	Customer account information, balances, transaction history, account detail
Transaction Server		
Banking App Server	Transaction Server	Fund transfer request, bill payments, transaction processing request
Banking App Server	Audit Log Server	User activities, system events, security events
Audit Log Server	Audit Log Database	Audit logs and activity records
Banking App Server	Notification Server	OTP request, transaction notifications, event notification
Notification Server	Notification Database	Notification records and delivery status
Notification Server	SMS/Email Server	OTPs request, notification messages request
Banking App Server	Third-Party Payment Server	Payment authorisation request
Third-Party Payment Server	Third-Party Payment Database	Authorised transactions
Third-Party Payment Server	Banking App Server	Transaction response

Key Stakeholders

A. Asset Owners

Asset owners are the personnel that are responsible to manage and protect the assets. Based on the trust boundaries that were discussed in section 1.2, it is clear that each asset such as servers and databases responsibility falls upon the owner of the boundary itself. For example, all the assets under internal banking network boundary will be protected by the bank itself and all the asset under third-party network boundary will be the third-party owner's responsibility.

B. Data Subjects

Data subjects are the individual whose personal data is protected by the system. Customers are the main data subject as their data processed such as personal information, biometric data and authentication credentials belongs to them. This is because their personal and financial informations are collected, processed ad stored within the banking system.

C. Regulators and External Authorities

Regulators are the ones who ensures that the bank compliances with cybersecurity regulations, privacy, and operational requirement. For example, Bank Negara Malaysia (BNM) is responsible for banking regulations, security requirement and operation management while Personal Data Protection Department (JPDP) is responsible to enforce Personal Data Protection Act (PDPA)

2.0 Threat and Vulnerability Identification

The purpose of this section is to identify and analyze potential security threats that may affect the proposed Mobile Banking Application with Biometric Authentication.

2.1 STRIDE Threat Analysis

The STRIDE threat modeling framework developed by Microsoft was used to evaluate the security risks associated with the major system components. Each component was analyzed to determine how it could be exploited by potential threat actors and what impact such attacks could have on the banking system. The identified threats were categorized according to the six STRIDE categories to ensure comprehensive threat coverage across the application.

Table 2.1: *STRIDE Threat List*

Threat ID	Threat Name	Target System Component	Threat Scenario
STRIDE Category: SPOOFING			
T01	Account Takeover via Credential Theft	Mobile Banking Application	An attacker uses stolen banking credentials obtained through phishing to impersonate a legitimate customer and access banking services.
T02	Biometric Authentication Bypass	Authentication & Biometrics Server	An attacker uses a fake fingerprint or facial image to bypass biometric authentication and gain unauthorized account access.
STRIDE Category: TAMPERING			

T03	API Request Tampering During Transmission	API/Firewall Gateway	An attacker intercepts communication between the mobile banking application and the API gateway and modifies request parameters before they reach the backend system.
T04	Fraudulent Modification of Transaction Details	Transaction Server	An attacker exploits weaknesses in the transaction processing logic of the Transaction Server to alter transaction details or redirect funds to an unauthorized account.
T05	Audit Log Modification	Audit Logs Server	A malicious insider alters or deletes audit records to conceal unauthorized banking activities.
STRIDE Category: REPUDIATION			
T06	Transaction Dispute	Transaction Server	A customer performs a transaction and later denies having performed the action, while insufficient audit evidence prevents the bank from proving accountability.
STRIDE Category: INFORMATION DISCLOSURE			
T07	Customer Account Data Exposure	Account Server	Unauthorized users gain access to customer account information such as balances, linked cards, and loan details.
T08	Customer Database Breach	Account Database	An attacker accesses sensitive customer records including NRIC numbers, addresses, phone numbers, and transaction histories.
T09	OTP Interception	SMS/Email Server	An attacker intercepts OTP messages through SIM-swapping or email compromise to facilitate fraudulent transactions.
STRIDE Category: DENIAL OF SERVICE			

T10	Core Banking Service Outage	Banking Application Server	A DDoS attack overwhelms the banking server, disrupting account access and transaction processing.
STRIDE Category: ELEVATION OF PREVILEGE			
T11	Administrative Privilege Escalation	Banking Application Server	An attacker exploits a software vulnerability to obtain administrator privileges and gain unauthorized control over banking operations.
T12	Third-Party Access Abuse	Third-Party Payment Server	A compromised third-party payment provider abuses its integration privileges to access banking resources beyond its authorized scope

Based on the identified threats, several underlying vulnerabilities were observed across the banking system. These include weaknesses in authentication mechanisms, insufficient transaction validation controls, excessive user privileges, insecure communication channels, and exploitable software flaws. If left unaddressed, these vulnerabilities may provide opportunities for threat actors to compromise sensitive customer information, manipulate financial transactions, disrupt banking services, or gain unauthorized access to critical system resources. Therefore, addressing these vulnerabilities is essential to maintaining the confidentiality, integrity, and availability of the mobile banking system.

2.2 Threat-Actor Analysis

Understanding the potential threat actors is important in determining how each identified threat may be carried out. The analysis categorizes threat actors into external attackers, insiders, and supply-chain actors. External attackers refer to unauthorized individuals attempting to compromise the banking system from outside the organization *(Jimmy, 2024)*. Insider threats originate from employees or privileged users who misuse their authorized access *(Favour, 2024)*. Supply-chain threats involve third-party service providers or vendors whose compromise may indirectly impact the banking system *(Saikrishna, 2021)*. ***Table 2.2*** maps each identified threat to its most likely threat actor and provides a brief justification.

Table 2.2: *Threat-Actor Analysis*

Threat ID	Threat Name	Threat Actor	Justification
T01	Account Takeover via Credential Theft	External Attacker	The mobile banking application is publicly accessible through the Internet, allowing unauthorized individuals to target customer credentials without requiring access to internal banking systems.
T02	Biometric Authentication Bypass	External Attacker	Biometric authentication serves as the first access control layer for customers, making it an attractive target for unauthorized individuals seeking account access.
T03	API Request Tampering During Transmission	External Attacker	The API gateway handles communication between the mobile application and backend systems. Since these communications pass through external networks, they may be targeted by unauthorized parties.
T04	Fraudulent Modification of Transaction Details	External Attacker	The Transaction Server handles fund transfers and payment processing. Any weakness in this component could be exploited to manipulate transaction outcomes for financial gain.
T05	Audit Log Modification	Insider	Since audit logs are mainly managed by administrators, there is a higher risk of misuse by employees with privileged access compared to external users.
T06	Transaction Dispute	Customer/ Insider	Since customers and authorized users perform banking transactions, they are the parties most likely to deny actions that cannot be clearly verified.

T07	Customer Account Data Exposure	External Attacker/ Insider	Both external attackers and employees with excessive privileges may access confidential customer information.
T08	Customer Database Breach	External Attacker	The account database stores sensitive customer and financial information, which makes it an attractive target for attackers seeking valuable data.
T09	OTP Interception	External Attacker	OTP messages travel through external communication providers, creating opportunities for interception outside the bank's direct control.
T10	Core Banking Service Outage	External Attacker	Organized threat actors may target core banking infrastructure to cause operational disruption.
T11	Administrative Privilege Escalation	External Attacker	Unlike administrators who already have privileged access, external attackers must exploit system vulnerabilities to obtain higher privileges and gain control of banking operations.
T12	Third-Party Access Abuse	Supply-Chain Attacker	A compromised third-party payment provider may be used as an entry point into the banking environment.

The analysis indicates that most threats originate from external attackers due to the Internet-facing nature of the mobile banking application. However, insider threats remain a significant concern, particularly for systems involving audit logging and privileged administrative access. In addition, the reliance on third-party payment and notification services introduces supply-chain risks that may affect the security of the overall banking ecosystem.

2.3 Assumptions and Out-of-Scope Items

Threat modeling is performed based on available system information and therefore requires several assumptions regarding the system architecture and operating environment. The assumptions listed below were used throughout the threat identification process. In addition, several areas were intentionally excluded from the scope of this assessment to maintain focus on the logical and technical security risks associated with the mobile banking application.

2.3.1 Assumptions

1. The mobile banking application is accessible through the Internet and supports remote customer access.
2. Biometric authentication is implemented using fingerprint and facial recognition technologies.
3. OTP verification messages are delivered through trusted third-party SMS and email providers.
4. Customer account information and transaction records are stored within centralized banking databases.
5. Third-party payment services communicate with the banking system through secured API integrations.

2.3.2 Out-of-Scope Items

1. Physical theft, vandalism, or destruction of banking hardware and infrastructure.
2. Natural disasters, environmental incidents, and utility failures that may impact system availability.
3. Security vulnerabilities associated with customer-owned devices that are outside the control of the banking organization.
4. Regulatory compliance assessments and legal requirements that are not directly related to technical cybersecurity risks.
5. Source code review and vulnerability scanning activities are not included within the scope of this assessment.

The assumptions and scope limitations defined above provide the basis for the threat analysis conducted in this report. While not all possible risks can be evaluated within the scope of this assessment, the identified threats represent the most relevant security concerns affecting the proposed mobile banking application and its supporting infrastructure.

3.0 Risk Analysis: Likelihood & Impact

This section involves analysing the identified risks through the use of the selected risk assessment methodology. The goal is to determine the severity of the potential consequences of each risk if it ever materializes and the likelihood of it happening. The analysis is based on the threats identified in **Section 2** and will be used to support the risk matrix and prioritization in the next section.

3.1 Selected Risk Analysis Methodology

For this assessment, NIST SP 800-30 was chosen as the risk analysis methodology, as it offers a structured and systematic way to identify, analyze, and assess cybersecurity risks ***(McCarthy & Harnett, 2014).*** It helps to evaluate the probability of a threat to occur and the damage it can cause to an organization's resources. This is directly related to the purpose of this assessment, since the proposed mobile banking application handles sensitive data of the customer, financial transactions, authentication documents, and biometric information. Specifically designed for risk assessment and prioritization, NIST SP 800-30 was chosen over other frameworks. The NIST Cybersecurity Framework emphasizes the management of cybersecurity activities through five core functions: Identify, Protect, Detect, Respond, and Recover, whereas ISO/IEC 27001 is about the implementation and maintenance of an Information Security Management System. MITRE ATT&CK primarily emphasizes on attacker tactics and techniques instead of assigning likelihood and impact ratings. Therefore, NIST SP 800-30 is the most suitable methodology for assessing and prioritizing the identified risks in the proposed mobile banking application.

3.2 Likelihood and Impact Rating

For consistency in the risk assessment process, a five-point rating scale was used to assess the likelihood and effect of each threat identified. The likelihood rating indicates the probability that the threat will occur, and the impact rating indicates the severity of the impact if the threat actually happens. The higher the ratings the higher the risk exposure and the higher the priority in risk treatment.

Table 3.2.1: *Likelihood Rating*

Rating	Level	Justification
1	Very Low	The likelihood of this happening is very low, and there is little historical evidence that this is likely.
2	Low	The threat is unlikely to occur but remains possible under limited conditions.
3	Moderate	The threat may occur under certain conditions or circumstances and has occasionally been observed in similar systems.
4	High	The threat would be likely to materialize as a result of known vulnerabilities or through common attack patterns.
5	Very High	High probability of occurrence and often seen in similar systems.

Table 3.2.2: *Impact Rating*

Rating	Level	Justification
1	Very Low	Minimal impact on system operations, assets, or users.
2	Low	Minimal disturbance, causing minor operational or financial impact.
3	Moderate	Evident effect on operations, data, or services that needs management attention.
4	High	Operational disruption or financial loss, regulatory issues, or reputational damage that is significant.
5	Very High	An impact that causes significant financial damage, significant data loss, legal issues or extended service disruption.

All of identified threats will be assigned with the likelihood and impact ratings in the proposed mobile banking application. These scales give a uniform standard for gauging the severity of risks and give a basis for prioritizing what risks to treat and what risks to mitigate.

3.3 Likelihood Assessment of Identified Risks

Table 3.3: *Likelihood Assessment of Identified Risks*

Threat ID	Threat Name	Threat Actor	Likelihood Rating	Justification
T01	Account Takeover via Credential Theft	External Attacker	**4**	A typical issue on the mobile banking side is credential theft, in which an outside entity can trick customers into compromising their accounts via phishing, social engineering attacks, and leaked credentials ***(Castell, 2013).*** The approaches don't always involve superior technical expertise and have often been seen in banking-related cybercrime attacks. But biometric authentication, OTP verification, and account monitoring of the situation can cut down the likelihood of a successful takeover.
T02	Biometric Authentication Bypass	External Attacker	**3**	Research and actual incidents have shown that biometric spoofing, including spoofing using fake fingerprints and face images, is possible ***(Banga & Pillai, 2021).*** Unlike credential theft attacks, however, these attacks typically involve special tools and technical abilities.
T03	API Request Tampering During Transmission	External Attacker	**3**	API request tampering can happen when there is interception or alteration of the API communication between the mobile banking app and backend system. Such an attack can be possible if the encryption is weak or weak session protection occurs, or even if the server-side request validation is weak. The attacker, however, will generally need technical knowledge, access to the communications channel, and some kind of vulnerability to exploit.
T04	Fraudulent Modification of Transaction Details	External Attacker	**4**	Financial systems are good targets, as an attacker can make a direct monetary return. Transaction information is often hijacked via application vulnerabilities or from a compromised account. Such attacks have been seen in online banking situations.
T05	Audit Log Modification	Insider	**2**	Access to internal systems or resources normally is privileged in order to modify audit logs. However, external attackers are unlikely to be able to access audit logs directly, and the external attack isn't as worrisome as an insider or admin attack.

T06	Transaction Dispute	Customer/Insider	**3**	Customers can choose to deny transactions or inner persons can take advantage of weak processes in record-keeping. They happen from time to time in financial institutions, particularly where audit trails or evidence may be inadequate.
T07	Customer Account Data Exposure	External Attacker/ Insider	**4**	Customer data is valuable and often a desired target for the attackers. Both external attackers and insiders may attempt to access sensitive account information. It is not unusual for data exposure incidents to be happening throughout the financial sector ***(Huang & Wang, 2021)***.
T08	Customer Database Breach	External Attacker	**3**	Databases are a big source of cybersecurity concerns as they contain large amounts of valuable customer data ***(Gowda & Gowda, 2021; Huang & Wang, 2021).*** While the large amount of valuable information stored in financial databases probably makes them more attractive to attackers than other targets, the level of security they employ diminishes the ease with which such attacks can occur.
T09	OTP Interception	External Attacker	**3**	OTP interception can be done via SIM-swapping, phishing, email compromise, or access to device of the customer ***(Okafor et al. 2025)***. These attacks are made in the financial sector, but typically demand more information about the target, effective social engineering, or breaching a communication medium.
T10	Core Banking Service Outage	External Attacker	**4**	Given that banking services are publicly available and depend upon availability, financial institutions are often targets of Distributed Denial-of-Service (DDoS) attacks. History tells us that banks are a favorite target for service disruption attacks ***(Sachdeva et al. 2010).***
T11	Administrative Privilege Escalation	External Attacker	**3**	In privilege escalation attacks, the attacker can only exploit software flaws to gain higher privileges after first accessing the system. These attacks can be severe, but typically take more technical expertise than phishing or credential theft does.
T12	Third-Party Access Abuse	Supply-Chain Attacker	**3**	Third-party service providers are increasingly targeted by attackers as part of supply-chain attacks. However, the attacks against trusted third parties happen less often than direct attacks against banking systems, but there have been several major cybersecurity incidents that show the risks involved in trusted third-party access ***(Kolo et al. 2025).***

3.4 Impact Assessment of Identified Risks

The effect of each identified risk was evaluated on six dimensions: confidentiality, integrity, availability, financial, regulatory and reputational impact. The five point impact scale outlined in section 3.2 was used to rate each dimension from Very Low to Very High. The overall impact rating was the mean of six dimension scores of impact rounded to the nearest whole number. Using this approach ensures a balanced assessment and that one dimension does not automatically dictate the overall rating of the impact.

$$\text{Impact Rating} = \frac{C + I + A + F + R + RP}{6}$$

Where: C: Confidentiality, I: Integrity, A: Availability, F: Financial, R: Regulatory, and RP: Reputational.

Table 3.4: *Impact Assessment of Identified Risks*

Threat ID	Threat Name	Confidentiality	Integrity	Availability	Financial	Regulatory	Reputational	Average	Impact Rating
T01	Account Takeover via Credential Theft	**5**	**4**	**2**	**5**	**4**	**4**	**4**	**4**
T02	Biometric Authentication Bypass	**5**	**4**	**2**	**4**	**4**	**4**	**3.83**	**4**
T03	API Request Tampering During Transmission	**4**	**5**	**3**	**4**	**4**	**4**	**4**	**4**

T04	Fraudulent Modification of Transaction Details	**3**	**5**	**2**	**5**	**4**	**5**	**4**	**4**
T05	Audit Log Modification	**2**	**5**	**2**	**3**	**5**	**4**	**3.50**	**4**
T06	Transaction Dispute	**2**	**4**	**2**	**3**	**3**	**3**	**2.83**	**3**
T07	Customer Account Data Exposure	**5**	**3**	**2**	**4**	**5**	**5**	**4**	**4**
T08	Customer Database Breach	**5**	**5**	**4**	**5**	**5**	**5**	**4.83**	**5**
T09	OTP Interception	**4**	**4**	**2**	**5**	**4**	**4**	**3.83**	**4**
T10	Core Banking Service Outage	**1**	**2**	**5**	**5**	**3**	**5**	**3.50**	**4**
T11	Administrative Privilege Escalation	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**
T12	Third-Party Access Abuse	**5**	**4**	**4**	**4**	**5**	**5**	**4.50**	**5**

3.4.1 Justification of Impact Assessment

T01 – Account Takeover via Credential Theft

If the account takeover is successful, the attacker can get access to personal confidential details of the customer and carry out unauthorized activities from the account. It's also possible to change account settings or contact information. This not only can have a considerable legal impact but also a financial as well, as the bank might have to compensate the impacted customers and carry out investigation to the incident. Yet, typically, it targets the individual accounts and not the entire banking system.

T02 – Biometric Authentication Bypass

It might be possible for an unauthorized party to access a customer's account through a method that does not require the customer's biometric authentication, and potentially allow the customer to be exposed to certain personal or financial information. The attacker might be able to make fraudulent transactions or to change the details of the account. The incident could cause customers to lose trust in the bank's authentication mechanisms. But it is expected that it would not impact the entire banking system, only customers' accounts selected for this implementation.

T03 – API Request Tampering During Transmission

The API interfaces could be susceptible to tampering, which could enable a hacker to alter the data that is sent between the smartphone app and banking servers. The quantity of the transactions, the numbers of the accounts to which funds are to be transferred or any of the specified request parameters can be altered. This has a significant impact on the integrity of data and can lead to loss of money, regulatory issues, and loss of reputation. Services may also be impacted, but potentially not an outage.

T04 – Fraudulent Modification of Transaction Details

Any manipulation of transaction information directly has impact on the integrity of financial transactions. Attacker can alter the transfer amount or transfer to another account. The result could be monetary damages, customer grievances, regulatory investigation and devastating reputation. Confidentiality and availability are affected minimally since the aim of the attack is to alter the information of a transaction.

T05 – Audit Log Modification

The attacker or insider can mask unauthorized activity by altering or removing audit trails. This can make it difficult for the bank to know what happened when a security incident occurs, and weaken the usefulness of evidence in investigations. The major impacts are on integrity and regulatory compliance as financial institutions have been expected to keep accurate and reliable audit records. But the threat does not generally compromise or reveal customer details or prevent banking.

T06 – Transaction Dispute

A transaction dispute might happen if the customer challenges that the transaction occurred and the bank can't find enough evidence to dispute the claim. Can result in refunds, investigative expenses and customer complaints. There is doubt over the integrity of the records of the transactions as well. But the event typically involves only one customer or transaction and is not necessarily systemic, that is, involving the entire banking system.

T07 – Customer Account Data Exposure

The information exposed by customer accounts can provide a wide range of sensitive data, including account balances, associated cards, transaction history, loan details and personal data. This raises some significant confidentiality and privacy issues. The consequences can also include identity theft, regulatory fines, loss of customer trust and financial loss. The threat does not cause a stoppage of the banking service, but mainly brings the data to the forefront, therefore availability is less affected.

T08 – Customer Database Breach

Any breach in a customer database could lead to the exposure, modifications or even deletion of a mountain of sensitive customer and financial data. However, it is unlike a single account incident, it could be affecting many customers simultaneously. It can result in severe breaches of privacy and security, financial loss, regulatory fines, litigation issues, breach notification expenses and ongoing reputational damage. The database can also be down during incident analysis and recovery operations.

09 – OTP Interception

If an OTP is intercepted, it could be used by an attacker to skip an extra authentication process and authorize access or fraudulent transactions. It can compromise confidentiality of company accounts and the integrity of financial transactions. The bank can suffer financial losses, provider payouts to customers, regulatory issues and loss in customer confidence in

their banking system's authentication. The incident, however, would typically impact specific users not the entire system.

T10 – Core Banking Service Outage

Core Banking Service outage primarily impacts system availability. It may not be possible for customers to log into their accounts, transfer funds, pay bills or do any urgent transactions. Extended downtimes can lead to business disruption, lost profits, and even grievances by their customers, and significant damage to reputation. An outage of the service, however, doesn't normally lead to exposure of confidential information or have a significant impact on the information stored.

T11 – Administrative Privilege Escalation

Access, as part of administrative privilege escalation, can grant the attacker access to banking servers, databases, customer accounts, banking security, and transaction services. The intruder can use his access to the system to obtain confidential data, alter data, open up new accounts, stop security measures or interfere with banking services. The threat can have significant financial, regulatory and reputational impacts throughout the system.

T12 - Third-Party Access Abuse

Third-party access abuse is when a third party accesses banking systems and abuses them for the purposes of the attacker or service provider. Based on the type of access it has, the incident can result in the exposure of customer information or changing of transactions, disruption of connected services or impact multiple customers. Also, it can result in regulatory, contractual and reputational implications as the bank is still held accountable to safeguard the consumer information that is accessed through third-party integration.

The findings show that the majority of the identified risks are in the high-impact category, as the **mobile banking application** handles sensitive financial activities and information of the customer. Customer Database Breach, Administrative Privilege Escalation, and Third-Party Access Abuse were rated **Very High** to impact multiple customers, system components, and business operations. The impact ratings will be multiplied by the likelihood ratings from **Section 3.3** to obtain the risk ratings in the risk assessment matrix.

4.0 Risk Assessment Matrix

This section combines the likelihood and impact ratings of **Section 3** into a **risk assessment matrix.** The aim of the matrix is to indicate the relative positioning of each individual risk and facilitate risk prioritization. The risk scores are calculated according to the formula Likelihood x Impact, and the results indicate the level of risk, urgency of treatment and the need for action or continuous monitoring of each risk.

4.1 Five-by-Five Risk Assessment Matrix

The five-by-five risk assessment matrix was created to display the location of each risk identified in Section 3 according to their likelihood and impact ratings. The horizontal axis for this matrix is the likelihood rating, and the vertical axis is the impact rating. The threat IDs are plotted based on their assigned threat values for ease of comparison and identification of which threats should have a higher priority. The closer to the upper right hand corner of the matrix the position, the more concerned one should be, since they have a high likelihood and a high impact. This matrix is therefore used to prioritize the process prior to determining the final risk scores and treatment decisions.

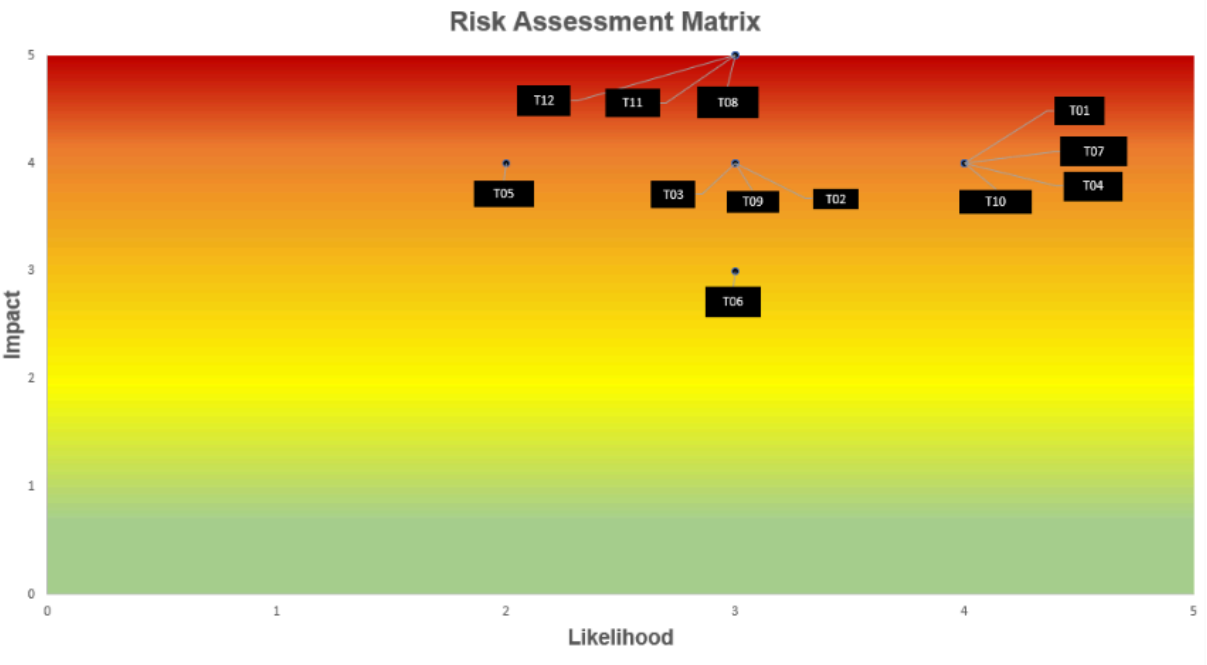


Figure 4.1: *Risk Assessment Matrix Plot for Identified Risks*

Further to this, in order to clearly pinpoint the location of the risk factors in the five-by-five risk assessment matrix, Table 4.1 presents the positioning of the threats according to their respective likelihood and impact values. This table supplements the graphical representation of Figure 4.1, indicating the actual risk level area for each threat.

Table 4.1: *Placement of Identified Risks Based on Likelihood and Impact*

Likelihood ↓ / Impact →	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
5 Very High	-	-	-	-	-
4 High	-	-	-	**T01, T04, T07, T10**	-
3 Moderate	-	-	**T06**	**T02, T03, T09**	**T08, T11, T12**
2 Low	-	-	-	**T05**	-
1 Very Low	-	-	-	-	-

As can be seen from Table 4.1, the majority of the risks is placed in the High-risk section of the matrix. Such risks as T01, T04, T07, and T10 belong to the High likelihood and High impact section. It can be said that these risks are very likely to happen and will cause considerable damage to the mobile banking application. These risks should be considered with great care due to the fact that they have to do with account takeover, transactions manipulation, data leakage, and availability problems. Moreover, the risks of T08, T11, and T12 have Moderate likelihood but Very High impact. Although these risks are less likely to happen than some other risks, they still need special attention because their consequences will be very bad due to the fact that they have to do with databases, administrative privileges, third-party access, multiple customers, and multiple system components. Also, such risks as T02, T03, and T09 belong to the High-risk area since although their likelihood is moderate, their impact is high.

4.2 Risk Score and Priority Ranking

The risks identified were plotted in the risk assessment matrix, and a risk score calculated for each risk based on the formula Likelihood × Impact. The likelihood rating is from Section 3.3, and impact rating is from Section 3.4. The objective of the risk score is to prioritize the risks and identify which ones need to be treated first. Higher scores indicate more urgent risks, as they have a higher likelihood and impact. If there are multiple risks with the same score, their priority order was based on their relevance to mobile banking operations, potential financial impact, and likelihood to impact customer trust and services continuity.

Table 4.2: *Risk Score and Priority Ranking of Identified Risks*

Priority	Threat ID	Threat Name	Likelihood	Impact	Risk Score	Risk Level
1	**T01**	Account Takeover via Credential Theft	**4**	**4**	**16**	**High**
2	**T04**	Fraudulent Modification of Transaction Details	**4**	**4**	**16**	**High**
3	**T07**	Customer Account Data Exposure	**4**	**4**	**16**	**High**
4	**T10**	Core Banking Service Outage	**4**	**4**	**16**	**High**
5	**T08**	Customer Database Breach	**3**	**5**	**15**	**High**
6	**T11**	Administrative Privilege Escalation	**3**	**5**	**15**	**High**
7	**T12**	Third-Party Access Abuse	**3**	**5**	**15**	**High**
8	**T02**	Biometric Authentication Bypass	**3**	**4**	**12**	**High**
9	**T03**	API Request Tampering During Transmission	**3**	**4**	**12**	**High**
10	**T09**	OTP Interception	**3**	**4**	**12**	**High**
11	**T06**	Transaction Dispute	**3**	**3**	**9**	**Moderate**
12	**T05**	Audit Log Modification	**2**	**4**	**8**	**Moderate**

4.3 Risk-Tolerance Threshold

The level of risk tolerance would be the line between acceptable risk and treatable risk. Risk tolerance is the level and kind of risk that an organization is willing to take. The proposed system is a mobile banking application, therefore, the tolerance level for the risk is low, as the system is handling sensitive information of the customer, authentication data, and financial transactions. Hence, any risks that could impact confidentiality, transaction integrity, service availability, regulatory compliance or customer trust should not be ignored.

We used the following formula to calculate the risk score:

Risk Score = Likelihood x Impact

The threshold was determined by using the risk matrix (5 × 5) and the calculated risk score. The first matrix indicates the qualitative risk level according to the likelihood and impact of the risk, and the second matrix indicates the numeric risk score based on the results of the multiplication of both the likelihood and the impact. Low scoring risks can be accepted but monitored, moderate risks should be controlled by a review of the risks. High and Very High risk levels are not acceptable and may result in financial loss, disruption of service, legal problems or damage to reputation, and must be treated as such. This is in line with the idea of risk assessment in terms of likelihood and impact which is used to determine whether to avoid, mitigate, transfer or accept the risk.

		Impact				
		Insignificant (1)	Minor (2)	moderate (3)	Major (4)	Catastrophic (5)
Likelihood	Almost Certain (5)	Moderate	High	High	Very High	Very High
	Likely (4)	Low	Moderate	High	High	Very High
	Possible (3)	Low	Moderate	Moderate	High	High
	Unlikely (2)	Very Low	Low	Moderate	Moderate	High
	Rare (1)	Very Low	Very Low	Low	Low	Moderate

Figure 4.3.1: *Risk Level Matrix Based on Likelihood and Impact*

Figure 4.3.1 shows that depending on the various likelihoods and impacts that have been identified, there arise various levels of risks from very low up to very high.



Figure 4.3.2: *Risk Score Matrix Based on Likelihood x Impact*

Figure 4.3.2 shows the risk score matrix in numeric form according to the Likelihood × Impact formula. The scale ranges from 1 to 25, and the higher the number, the higher the risk exposure.

Based on these two matrices, the *Risk-Tolerance Threshold* was identified. As shows below in table 4.3.1.

Table 4.3.1: *Risk-Tolerance Threshold*

Risk Score Range	Risk Level	Tolerance Decision	Required Action
1-5	**Very Low / Low**	Acceptable	Monitor periodically and maintain existing controls
6-9	**Moderate**	Tolerable with control review	Review current controls, monitor regularly, and improve control if needed
10-16	**High**	Unacceptable without mitigation	Mitigation plan is required before the risk can be accepted
20-25	**Very High**	Unacceptable / Immediate action required	Immediate treatment, management escalation and strong security controls are required

Because this is a mobile banking application, High and Very High risks are grouped as unacceptable risks that require treatment. Very high risks, however, call for quicker response, and faster escalation of management, than high risks. Moderate risks should be accepted for a short period of time, provided that they are closely monitored and reviewed regularly.

Table 4.3.2: *Application of Risk-Tolerance Threshold*

Threat ID	Risk Score	Risk Level	Tolerance Decision	Required Action
T01	**16**	**High**	Unacceptable without mitigation	Mitigation plan required
T02	**12**	**High**	Unacceptable without mitigation	Mitigation plan required
T03	**12**	**High**	Unacceptable without mitigation	Mitigation plan required
T04	**16**	**High**	Unacceptable without mitigation	Mitigation plan required
T05	**8**	**Moderate**	Tolerable with control review	Monitor and review controls
T06	**9**	**Moderate**	Tolerable with control review	Monitor and review controls
T07	**16**	**High**	Unacceptable without mitigation	Mitigation plan required
T08	**15**	**High**	Unacceptable without mitigation	Mitigation plan required
T09	**12**	**High**	Unacceptable without mitigation	Mitigation plan required
T10	**16**	**High**	Unacceptable without mitigation	Mitigation plan required
T11	**15**	**High**	Unacceptable without mitigation	Mitigation plan required
T12	**15**	**High**	Unacceptable without mitigation	Mitigation plan required

Application of the threshold indicates that the majority of the identified risks are in the High-Risk classification. The following tests are not acceptable without mitigation: T01, T02, T03, T04, T07, T08, T09, T10, T11 and T12, which could impact customer data, transaction integrity, the availability of service, regulatory compliance, and customer trust. T05 and T06 are at a Moderate level and are subject to control review and ongoing monitoring to ensure levels do not rise to more than this.

5.0 Mitigation Strategies & Recommendations

Every risk of threats to the system must be mitigated to prevent any further losses to the organization. For a mobile banking service, it is important that their services on the application have constant uptime. In addition to the uptime, customer personal information must remain confidential and not compromised as this is a breach of trust and rights of users. For example, an EU regulatory framework named Digital Operational Resilience Act (DORA), mandates that financial entities and ICT third-part service providers to follow a set of rules regarding risk management and mitigation and failure to comply may be penalized according to the law. (Digital Operational Resilience Act (DORA) | Freshfields, n.d.). This shows that security is an important basis in any running organizations to protect the users as well as the personnels in the company.

5.1 Recommended Controls Following ISO/IEC 27001 (2022) Annex A

For this mobile banking application example, standards such as the ISO/IEC 27001 Annex A will be implemented, which helps provide proper guidelines to apply various mitigation methods for each specific risk that has been identified previously.

Table 5.1: *Mapping of Mitigation Controls*

No.	Risk	Mitigation Control	Mitigate/Transfer/ Accept/Avoid	ISO/IEC 27001 (2022) Annex A
T01	Account Takeover via Credential Theft (High)	Implement multifactor authentication (MFA): Enforce MFA on higher risk actions or data such as approving large transactions and modifying account information.	Mitigate	A.8.5 (Secure authentication)
		Phishing Awareness Training: Frequent gentle reminders to users about phishing as they use the banking mobile app.	Mitigate	A.6.3 (Information security awareness, education and training)
T04	Fraudulent Modification of Transaction Details (High)	Apply Database Activity Monitoring: Tracks activities or actions being done onto the database in real time.	Mitigate	A.8.15 (Logging) A.8.16 (Monitoring activities)
		Use of cryptography: Encrypt the transaction details using algorithms such hash functions (e.g. SHA-256) to hold integrity of the data.	Mitigate	A.8.24 (Use of cryptography)

T07	Customer Account Data Exposure (High)	Use of cryptography: Encrypt customer personal information with algorithms such as using block ciphers and stream ciphers.	Mitigate	A.8.24 (Use of cryptography)
T10	Core Banking Service Outage (High)	Outsource from a DDoS protection services group: Consult cloud providers and alike for their services to cover for any service disruption such as DDoS.	Transfer	A.5.24 (Information security incident management planning and preparation)
		Disaster recovery roadmap: Have a set of instructions and actions that align with global security standards in the scenario where services are disrupted.	Mitigate	A.5.26 (Response to information security incidents)
T08	Customer Database Breach (High)	Enforce restrictive access control: Apply role-based access control (RBAC) or zero-trust policy to prevent access by unauthorized personnel.	Mitigate	A.5.15 (Access control)
		Apply Database Activity Monitoring: Tracks activities or actions being done onto the database in real time.	Mitigate	A.8.15 (Logging) A.8.16 (Monitoring activities)
T11	Administrative Privilege Escalation (High)	Enforce restrictive access control: Apply role-based access control (RBAC) or zero-trust policy to prevent access by unauthorized personnel.	Mitigate	A.5.15 (Access control)
		Unusual behaviour detection: Detect any differences in user behaviour such as location of user receiving privilege and login time.	Mitigate	A.8.16 (Monitoring activities)
T12	Third-Party Access Abuse (High)	Formalize policies and agreements in vendor contracts: Allow the third-parties to sign contracts with the terms and policies to follow concerning security of the system and data.	Mitigate	A.5.20 (Addressing information security in supplier agreements) A.6.2 (Terms and conditions of employment)
T02	Biometric Authentication Bypass (High)	**Deploy strong sensor systems:** Strong verification sensors prevent attackers from bypassing using deepfake biometrics.	Mitigate	A.8.5 (Secure authentication)

T03	API Request Tampering During Transmission (High)	**Mandate TLS:** The encryption and integrity aspect of TLS prevents the data from being eavesdropped and modified.	Mitigate	A.8.24 (Use of cryptography)
T09	OTP Interception (High)	**Install firewall at critical points:** Install firewalls in critical parts in the network as a way to monitor traffic coming in and out of the network for suspicious activities.	Mitigate	A.8.20 (Network security)
		Replace OTP with other authentication methods: Completely remove OTP requests as a way to authenticate and replace them with authentication methods such as with passkeys and in-app approvals.	Avoid	A.8.5 (Secure authentication)
T06	Transaction Dispute (Moderate)	**Set terms and conditions for transaction disputes:** Customers must provide sufficient evidence to support their case; The banking system must also maintain audit trails for verification.	Mitigate	A.5.31 (Legal, statutory, regulatory and contractual requirements)
		Accept certain disputes: Some disputes root from human error and behaviour which cannot be avoided. Acceptance is fair when the cost of mitigation is more than potential loss.	Accept	-
T05	Audit Log Modification (Moderate)	**Ensure immutable backup:** Store an extra audit log backup with read-only mode that prevents changes done except for when creating new records.	Mitigate	A.8.13 (Information backup) A.5.33 (Protection of records)

5.2 Feasibility, Costs and Residual Risk of Each Control

Before carrying out any mitigation techniques, it is important to review whether or not the method is feasible financially and in terms of the impact post-application of the method. Mapping these considerations are required to be carried out to prevent unnecessary financial losses and to consider scenarios where fast responses are needed to prevent losses of assets.

The majority of the mitigation control methods proposed for the identified risks is to mitigate and reduce the impact of the potential risks as these risks are risks that cannot be overlooked as they will affect the operations of the application. This control method offers high feasibility as some proposed methods are easily executable and low in cost such as the implementation of MFA, access controls and encryption methods. However, some other methods require an extra step in the process such as the methods that involve legal authorities and extra manpower such as in disaster response scenarios. Residual risks of these methods are minimal however as technology advances, more variations of cyber attacks are developed, requiring constant monitoring and gradual improvement of the current security system to address them.

Transfer mitigation controls are only done to control the effect of the risk but does not completely eliminate the risk. The transfer of risk to relevant and trusted third-parties is done only when the organization does not have enough internal expertise to tackle the issue. That said, taking this mitigation control will be one of the biggest financial burdens for the company, affecting feasibility of this control method. For example, relying on cloud services to prevent DDoS attacks requires a timely subscription-like payment that may be costly, depending on the plan chosen by the organization. However, these services are mostly done by well-established and trusted companies hence it is safe to conclude that the residual risk of this control is minimal and will become a low priority risk in the future.

Accepting risk mitigation method refers to accepting the risk after considering other possible ways to mitigate those risks. This method measures the feasibility of a mitigation method where if said mitigation method does not seem feasible in terms of time, money and resource, the organization may choose to accept the risk. For example, it is suitable to accept some of the transaction disputes, such as in scenarios where mitigating the problem has a bigger financial cost compared to accepting the risk. The residual risk of this method is that the risk is still present however this is only permissible if the company has come to terms with the risk.

Avoiding the risk method is the method of eliminating the threat by removing the feature in the system that arises that risk. This method is fairly easy to implement but may cause risk of affecting other features in the system such as poor integration of the new system after deleting the old system, hence feasibility is medium-level for removing the OTP requests feature. The cost of this operation may cause significant loss in revenue and sunk costs from building the deleted feature. However, the residual risks of the original problem are solved this way.

5.3 Implementation Roadmap

After deciding on which mitigation methods to implement, the organization must plan out an implementation roadmap to follow to ensure a structured and proper implementation of the security methods. The roadmap is to be separated into multiple phases based on priority of risks to be addressed. Frameworks such as the NIST Cybersecurity Framework emphasize under the Govern function, that it is crucial to understand the problem and roles of the personnel involved to strategize how to carry out this risk management.

Table 5.3: *Risk Management Roadmap*

	Objective	Key Initiatives
Short-term (0-3 months)	• Immediately address the high risk and high impact risks. • Tackle issues regarding security of the databases and secure authentication methods.	• Encryption • MFA • Replacing OTP with in-app authentication • Formalize terms and conditions
Medium-term (3-6 months)	• Strengthen the newly applied security measures by applying another layer of security on current systems.	• Network security • Backup logs • RBAC • Security awareness training
Long-term (6-12 months)	• Focuses on implementing security principles and advanced security detection systems. • Continuous monitoring for threats is in this phase.	• Database monitoring systems • Incident response • Execute testing and continuous monitoring

This phased implementation guideline allows the organization to plan out their security measures as well as financially plan the amount of money intended to use per term as established. The early phase of the roadmap focuses on addressing the critical vulnerabilities in the current system and gradually building up and enhancing the security systems in the later phases. The long-term or ongoing phase after the early phases is reserved to develop resilience in the security system with continuous monitoring for detection of threats. This strategy supports continuous improvement and aligns with global cybersecurity standards and expectations.

6.0 Conclusion

This report evaluated Mobile Banking Application with Biometric Authentication for cybersecurity risks. This indicated that the components involve extremely sensitive materials like customer personal information, verification information, biometric data, financial data, transaction information, and system logs. Thus it is essential to ensure the integrity, confidentiality and availability of the system.

Based on the STRIDE framework, problems that can pose a threat to the application were identified and included in the report: Credential theft, Biometric bypass, API tamper, Customer database breach, OTP interception, DDoS attacks, Privilege escalation, and Third-party access abuse. Using NIST SP 800-30 the risk analysis was performed with each threat rated for likelihood of occurrence and impact. The risk matrix revealed that most risks are of High category which cannot be accepted without mitigations being put in place.

The latter were integrated into the ISO/IEC 27001 Annex A controls to help meet cyber security standards. Other controls like multi-factor authentication, encryption, role-based access control, database activity monitoring, secure communication, backup protection, vendor agreements and incident response planning can help mitigate the risks identified.

It may be concluded that only when the identified risks are taken care of the proposed mobile banking application can deliver secure and reliable services. High-risk threats must be treated as a priority and moderate risks monitored continuously and reviewed. Implementing the recommended controls and following a phased rollout approach will help to enhance system security, ensure the protection of customer information, keep the system up and running, and increase trust in the mobile banking system.

References

- Boyle, M. (2024). *Digital banking statistics 2024: How many Brits use online banking?* Finder UK. https://www.finder.com/uk/banking/digital-banking-statistics
- Backbase. (2026). *Banking Operating System: Core to Platform Guide*. Backbase.com. https://www.backbase.com/blog/banking-operating-system
- CSRC Content Editor. (2017). *asset - Glossary | CSRC*. Nist.gov. https://csrc.nist.gov/glossary/term/asset?
- *14 Types of Biometrics & How They Work*. (2023, October 1). https://securityjournaluk.com/types-of-biometrics/
- Parusheva, S. (2015). A comparative study on the application of biometric technologies for authentication in online banking [Review of *A comparative study on the application of biometric technologies for authentication in online banking*]. *Egyptian Computer Science Journal*, *39*(4), 12. https://www.researchgate.net/profile/Silvia-Parusheva/publication/282653501_A_comparative_study_on_the_application_of_biometric_technologies_for_authentication_in_online_banking/links/5616249c08aec62244120e0a/A-comparative-study-on-the-application-of-biometric-technologies-for-authentication-in-online-banking.pdf
- Avdic, A. (2019). Use of Biometrics in Mobile Banking Security: Case Study of Croatian Banks [Review of *Use of Biometrics in Mobile Banking Security: Case Study of Croatian Banks*]. *IJCSNS International Journal of Computer Science and Network Security*, *19*(10), 7. https://www.researchgate.net/profile/Ammar-Avdic/publication/340647644_Use_of_Biometrics_in_Mobile_Banking_Security_Case_Study_of_Croatian_Banks/links/5e96f5554585150839de95df/Use-of-Biometrics-in-Mobile-Banking-Security-Case-Study-of-Croatian-Banks.pdf
- Jimmy, F. (2024). Cybersecurity Threats and Vulnerabilities in Online Banking Systems. International Journal of Scientific Research and Management (IJSRM), 12(10), 1631–1646. https://doi.org/10.18535/ijsrm/v12i10.ec10

- Favour Olaoye, & Axel Egon. (2024, August 30). Insider Threat Detection and Prevention. Journal of Cyber Security; Tech Science Press. https://www.researchgate.net/publication/383565287_Insider_Threat_Detection_and_Prevention
- Saikrishna Boggavarapu. (2021, December 1). The Effect of Third-party Service Providers On Information Security Breaches At Financial Institutions. https://doi.org/10.13140/RG.2.2.21419.62245
- McCarthy, C., & Harnett, K. (2014). National institute of standards and technology (nist) cybersecurity risk management framework applied to modern vehicles. National Institute of Standards and Technology (NIST) cybersecurity risk management framework applied to modern vehicles
- Castell, M. (2013). Mitigating online account takeovers: The case for education. Mitigating Online Account Takeovers: The Case for Education
- Banga, L., & Pillai, S. (2021, July). Impact of behavioural biometrics on mobile banking system. In *Journal of physics: Conference series* (Vol. 1964, No. 6, p. 062109). IOP Publishing. Impact of Behavioural Biometrics on Mobile Banking System - IOPscience
- Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, *96*(3), 261-286. Do Banks Price Firms' Data Breaches? | The Accounting Review | American Accounting Association
- Gowda, P., & Gowda, A. N. (2021). Data breach as a threat in the banking sector and steps to avoid it. *International Journal of Science and Research (IJSR)*, *10*(4), 1412-1415. Data Breach as a Threat in the Banking Sector and Steps to Avoid It
- Okafor, C. M., Oseghale, D. O., & Ayanlaja, S. Enhancing Transactional Security in US Banking Systems by Implementing OTP-Based Two-Factor Authentication to Mitigate Debit and Credit Card Fraud. Enhancing Transactional Security in U.S. Banking Systems by Implementing OTP-Based Two-Factor Authentication to Mitigate Debit and Credit Card Fraud

- Sachdeva, M., Singh, G., Kumar, K., & Singh, K. (2010). DDoS Incidents and their Impact: A Review. *Int. Arab J. Inf. Technol.*, *7*(1), 14-20. https://d1wqtxts1xzle7.cloudfront.net/34877167/3-libre.pdf?1411684637=&response-content-disposition=inline%3B+filename%3DDDoS_Incidents_and_their_Impact_A_Review.pdf&Expires=1781598067&Signature=UI7VOyMwRUrvoP-U7RRq~kR7LlQfECBvtc~89sQS14rCCvDIAvRelJWVDgz9C1qYDQoeWHyFXfq2qkgyHssvfEK72lgJdI2RjEmV3qfE5bHhr6IdbAcl4JmnsIicl9fzKhHUuLFJGB2X69GRp6y55IDTbpJjYCtLghe5d~BFDfOqETTX6yE1WokZxuInwVlvIWnku-UgBLEV-75v4TGXd76TkJ~w9rGjtSqzhNgofTI4XqU7QE6eXt7Or-yJ5wq3c-eNaRTcgx6ubv6UKMVVCVVtVlSFRt5LLW8Os5CVuOaMdQQNDrnaia8QPIC63iH5SZ5VmQxHdivwYPeJEeuprA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
- Kolo, F. H. O., Joseph, S. A., Ogunmolu, A. M., Ejiofor, V. O., & Oyekunle, S. M. (2025). Mitigating cybersecurity risks in financial institutions through strategic third-party risk governance frameworks. *Journal of Engineering Research and Reports*, *27*(5), 173-193. Mitigating-Cybersecurity-Risks-in-Financial-Institutions-through-Strategic-Third-Party-Risk-Governance-Frameworks.pdf
- **18**. Digital Operational Resilience Act (DORA) | Freshfields. (n.d.). https://www.freshfields.com/en/our-thinking/campaigns/tech-data-and-ai-the-digital-frontier/eu-digital-strategy/digital-operational-resilience-act-dora?utm_source=incrypthos.com&utm_medium=referral&utm_campaign=noo-engine.com

Appendices

Appendix A: DFD Diagram

Appendix B: **SSS task 4.0.xlsx**

Appendix C: **ITS68504_SSS_Assignment**