Sri Lanka Institute of Information Technology

Information Assurance & Security (IT3070)

Assignment 1

3rd Year, 1st Semester

Selected Asset	Name	IT Number
Core Banking System	Dasanayake N.G.H.B (Leader)	IT22118622
ATM Network	Liyanage S.D	IT22083128
Customer Mobile Banking Application	Kahingala D.L	IT22113054

Group Leader's Batch and Lab Group Y3. S1. WD.IT.0102

Table of Contents

Introduction

Bank of Ceylon (BOC) is state-owned commercial bank in Sri Lanka, founded in 1939. As one of the country's largest and most trusted financial institutions, BOC offers a wide range of banking services, including retail, corporate, and investment banking. The bank manages critical IT- related assets, such as Core Banking System, ATM network, and Customer Mobile Banking Application, which are essential providing seamless banking services. With over 600 branches and strong digital banking options, BOC serves millions of customer both in Sri Lanka and Internationally. BOC is a key player in supporting the nation's economic growth by offering secure and innovative financial solutions. Its focus on modern technology, financial stability, and great customer service has made BOC a leader in Sri Lanka's banking sector.

Asset 01- Core Banking System

01.1 Allegro Worksheet 08 for Core Banking System

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Core Banking System	The Core Banking System is very important for daily banking operations. Such as managing customer accounts, processing transactions, and maintain financial records. It is essential for the bank's functionality and customer service.	The Core Banking System is a comprehensive software platform used by the bank to manage and process financial transactions, customer account information, and other critical banking functions. It supports various banking services and integrates with other financial systems.
(4) Owner(s) *Who owns this information asset?*		
The IT Department of the Bank		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, such as IT staff and senior management with specific roles.	
❑ **Integrity**	Only authorized personnel can modify this information asset, including system administrators and designated IT personnel.	
❑ **Availability**	This asset must be available for these personnel, including customer service representatives and banking operations staff. This asset must be available for __24___ hours, ___7__ days a week, __365___ days a year.	
❑ **Other**	This asset has special regulatory compliance protection requirements with financial and data protection laws.	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
✓ Confidentiality	❑ Integrity	❑ Availability ❑ Other

01.2 Allegro Worksheet 10 for Core Banking System

01.2.1 Malware Infiltrating the Core Banking System

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Core Banking System		
		Area of Concern	Malware Infiltrating the Core Banking System		
		(1) Actor *Who would exploit the area of concern or threat?*	Outside Attacker		
		(2) Means *How would the actor do it? What would they do?*	An outside attacker might carry out a malware attack by using several techniques. They could send deceptive phishing emails containing malicious links or attachment, tricking recipients into downloading and installing malware. They might also find and exploit software flaws that haven't been fixed yet to sneak in malware and gain unauthorized access. Additionally, hackers might set up malicious websites that automatically download malware to any visiting computer without the user knowing		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate: Attacker aim to steal sensitive financial data (such as account numbers, passwords) to commit fraud or sell the information on the dark web.		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Customer data being stolen without permission compromises confidentiality. And also malware changes financial records, affecting transaction accuracy. This will violate Integrity. System outages caused by malware make banking services inaccessible, impacting availability.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	A data breach can seriously damage a bank's reputation and customer confidence, as customer may lose trust in the bank's ability to protect their information. And also, the bank might face financial losses due to fraud, the costs of responding to the incident	Reputation & Customer Confidence	9	6.75
		Financial	9	6.75
	Malware can lead to downtime as the infected may need to be cleaned and restored. This downtime can result in lost productivity and core banking system could disrupt operations, causing delays in customer service and daily banking activities.	Productivity	8	6
		Safety & Health	3	2.25
	Regulatory bodies may impose penalties for data protection violations. And also a breach can disrupt daily operations, reduce efficiency, cause delays in transactions, and lead to a loss of business. Long-term effects might include higher operational costs and damage to customer relationships.	Fines & Legal Penalties	9	6.75
		User Defined Impact Area	8	6
			Relative Risk Score	**34.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	• Employees training on recognizing phishing emails and social engineering attacks. • Limit access for all users and regularly check their permission.
Technical Controls	• Regularly update and patch software to close known as vulnerabilities. • Implement advanced malware detection system. • Use encryption for all sensitive data in transit and at rest.
Physical Controls	• Protect data centers with limited access and physical security measures like cameras and guards. • Use secure backups for important data to recover from ransomware attacks.

Justification of probability and severity values

Attribute	Value	Justification
Probability	75%	The high probability is set at 75% because the core banking system holds sensitive information and is very appealing to hackers. Cyber-attacks on banks happen often and are very sophisticated showing that there's a serious risk of malware getting into the system
Reputation & Customer Confidence	9	A server impact on reputation and customer confidence is expected if malware compromises the core banking system. Customers expect their banks to be very secure. Any breach might make many customers leave because the they no longer trust the bank to keep their information safe.
Financial	9	The financial stakes are extremely high in the event of malware attack on the core banking system. This includes money lost from fraud, the expenses to fix the problem, and possible fines from regulators.
Productivity	8	Malware infections typically result in system downtime while the malware is contained and systems are restored. This can disrupt daily banking operations significantly, affecting overall productivity and service delivery.
Safety & Health	3	A cyber-attack usually doesn't directly harm people's physical safety or health. However, the stress and mental strain it puts on employees who have to handle the situation are important and should not be overlooked.
Fines & Legal Penalties	9	The risk of legal trouble is high. Banks must follow strict rules, and if they break them because of malware, they could face heavy fines and be forced to fix the problem by law.
User Defined Impact Area	8	The user-defined impact area reflects long-term operational costs, such as recovery efforts, security improvements, and policy changes.

01.2.2 Unauthorized internal users in the bank accessing sensitive information for steal data.

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	Core Banking System		
	Area of Concern	Unauthorized internal users in the bank accessing sensitive information for steal data.		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Employees(Insider)		
	(2) Means *How would the actor do it? What would they do?*	Unauthorized internal users might misuse their access to steal sensitive data from the core banking system. They could bypass security and take confidential information.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate or Accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Destruction** ✓ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Sensitive information being stolen without permission compromises confidentiality. And also they do unauthorized modifications or deletions. This will violate Integrity. Misuse of data could affect system availability.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
A sensitive information breach can significant damage a bank's reputation and customer confidence, as customer may lose trust in the bank's ability to protect their information. And also, the bank might face financial losses due to fraud, legal fees, and regulatory fines.	Reputation & Customer Confidence	9	6.75
	Financial	9	6.75

	Reduced efficiency and potential disruptions. And also minimal direct impact for safety & health, though stress for staff.	Productivity	7	5.25
		Safety & Health	2	1.5
	Heavy fines for breaking regulations.	Fines & Legal Penalties	8	6
		User Defined Impact Area	6	4.5
			Relative Risk Score	**30.75**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	• Implement strict access controls, regular audits, and user activity monitoring. • Conduct background checks and training for employees.
Technical Controls	• Use data encryption, access management systems, and intrusion detection system. • Enforce strong authentication methods.
Physical Controls	• Limit access to important systems and secure server rooms with cameras and access records.

Justification of probability and severity values

Attribute	Value	Justification
Probability	75%	The likelihood of internal users misusing their access to steal or modify sensitive information is high due to potential vulnerabilities in security controls. We assign a high chance rating of 75% based on this threat.
Reputation & Customer Confidence	9	A breach of sensitive data could greatly harm the bank's reputation. Customers may doubt the bank's ability to protect their personal information, resulting in a major decline in trust and customer confidence.
Financial	9	The unauthorized access could result in financial losses due to fraud, legal fees, and possible compensation to customers. The financial impact of this breach is substantial.
Productivity	7	The misuse of sensitive data could lower efficiency and disrupt system operations. Employees may become distracted or lose confidence, which would result in a drop productivity.
Safety & Health	2	There is minimal direct impact on safety and health, though the stress on staff could be considered a small factor.
Fines & Legal Penalties	8	Regulatory agencies could issue substantial fines for violating confidentiality and security regulations, so we assign high rating for legal consequences.
User Defined Impact Area	6	Potential damage in other areas such as internal policies and compliance might lead to internal risks.

Asset 02- ATM Network

02.1 Allegro Worksheet 08 for ATM Network

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
ATM Network	The ATM network is a critical asset for Bank of Ceylon as it enables customers to access banking services such as cash withdrawals, deposits, balance inquiries, and funds transfers 24/7, ensuring customer	The ATM network is made up of machines located in different places that are connected to the bank's main system. It allows real-time processing of transactions, providing essential banking services to customers outside regular banking hours.
(4) Owner(s) *Who owns this information asset?*		
IT Department of the Bank		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, such as the IT staff and ATM service technicians.	
❑ **Integrity**	Only authorized personnel can modify this information asset, including IT Administrators, bank management (with special permission) and network engineers.	
❑ **Availability**	This asset must be available for IT manager, Operation manger, Network manager and Finance officer to do their jobs. This asset must be available for _24____ hours, ___7__ days a week, _365____ days a	
❑ **Other**	The ATM network must comply with financial industry regulations such as **PCI DSS (Payment Card Industry Data Security Standard)** to protect cardholder data and ensure the security of electronic transactions.	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	✓ Availability ❑ Other

02.2 Allegro Worksheet 10 for ATM Network

02.2.1 Cybersecurity vulnerabilities of the ATM network

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	ATM Network		
		Area of Concern	Cybersecurity vulnerabilities of the ATM network		
		(1) Actor *Who would exploit the area of concern or threat?*	Outside Attacker		
		(2) Means *How would the actor do it? What would they do?*	The outside attacker could exploit vulnerabilities in the ATM network by launching attacks such as malware injections, tricking people into giving up information, using devices to steal card information, or brute force attacks. They might compromise the ATM software, intercept data transmitted between the ATM and the bank servers, or take advantage of poor security settings.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate: The attacker aims to steal personal and financial information from customers to commit fraud, withdraw money without permission, or sell the stolen data. Attacker does these things for attacker's financial gain.		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Modification**	✓ **Destruction** ✓ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Unauthorized access to customer data compromises Confidentiality. Change or mess with the data being sent between the ATM and the bank affects Integrity. ATM services are interrupted or shut down by an attack, customers won't be able to use them, which impacts **Availability.**		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	A successful attack on ATMs could lead to a loss of trust in the bank's ability to secure customer funds and personal information. Customers may feel unsafe using the ATMs, leading to a loss of confidence and reputation damage for the bank. And also, the bank might face financial losses from unauthorized withdrawals. Additionally, the bank might have to spend money to investigate the attack, fix or replace damaged ATMs, and pay back customers who were affected.	Reputation & Customer Confidence	9	6.75
		Financial	9	6.75
	If the ATM network is disrupted, it could lead to downtime, resulting in customers being unable to access their funds. The downtime would require technical teams to fix the issues, affecting the bank's operational efficiency.	Productivity	9	6.75
		Safety & Health	2	1.5
	If customer data is stolen, the bank could be fined by regulators for not protecting the data properly. The bank might also get sued by customers whose information was exposed. Repeated attacks on the ATM network could disrupt daily operations, and over time, the bank may have to spend more money on extra security measures and dealing with these incidents.	Fines & Legal Penalties	9	6.75
		User Defined Impact Area	9	6.75
			Relative Risk Score	**35.25**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Administrative Controls	• Regularly train staff to spot phishing scams, tricks used by attackers (social engineering), and any suspicious activity around ATM security. • Limit access to important ATM systems to only trusted and authorized people, and check regularly to make sure the right people have access. • Create and update a clear plan to quickly handle cyberattacks and reduce damage if an attack happens.		
Physical Controls	• Install surveillance cameras, alarms, and tamper-resistant locks on ATMs to prevent unauthorized access.		
Technical Controls	• Keep ATM software updated with the latest fixes to prevent security weaknesses. • Use strong security methods to protect data sent between ATMs and the bank, and for any sensitive data stored on the ATMs. • Set up advanced systems to watch for any unusual activity on the ATM network and stop attacks before they cause harm.		

Justification of probability and severity values

Attribute	Value	Justification
Probability	75%	The likelihood of a cyber-attack on the ATM network is high due to external attackers exploiting vulnerabilities such as malware injections and brute force attacks. Given that ATM networks are often targeted for financial gain, there's a 75% chance of such threats materializing.
Reputation & Customer Confidence	9	An attack on the ATM network could severely impact customer confidence in the bank's ability to secure their personal and financial information. Customers might lose trust in using ATMs, leading to significant reputational damage for the bank.
Financial	9	Financial consequences are significant; as unauthorized withdrawals can result in considerable losses. Additionally, the bank would incur costs for investigations, repairing/replacing ATMs, and compensating affected customers, making the financial impact high.
Productivity	9	A disruption in the ATM network would lead to downtime, impacting customers' ability to access funds and creating operational inefficiencies. The technical teams would need to address the issues, leading to a productivity drop for the bank.
Safety & Health	2	While a cyber-attack on the ATM network does not directly affect physical safety or health, the stress and strain on employees handling the situation can be considerable. However, the overall impact on safety and health is low.
Fines & Legal Penalties	9	The bank faces the risk of heavy fines and legal penalties if customer data is compromised. Non-compliance with data protection laws can lead to significant penalties, and the bank may also face lawsuits from affected customers, making this a high-risk area.
User Defined Impact Area	9	This area reflects the long-term impact of the attack, including costs related to recovery efforts, security upgrades, and policy adjustments. The bank may need to invest in stronger security measures to prevent future incidents, which could involve significant resource allocation.

02.2.2 Internal Employee Misuse of ATM Network

Allegro - Worksheet 10			INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Threat	Information Asset	ATM Network		
		Area of Concern	Internal Employee Misuse of ATM Network		
		(1) Actor *Who would exploit the area of concern or threat?*	Employee (Insider)		
		(2) Means *How would the actor do it? What would they do?*	Internal employee could abuse their authorized access by manipulating software, modifying transaction records, or intercepting sensitive data. They could use system credentials to carry out unauthorized withdrawals, alter account balances, or disable security features.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate or Accidental.		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	The misuse of privileged access by an internal employee threatens ATM network security. It can compromise **confidentiality** by exposing sensitive customer data, **integrity** by causing inaccurate or fraudulent transactions through system modifications, and **availability** by disrupting ATM services, leading to operational downtime and customer inconvenience.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value**	**Score**

	Internal misuse of the ATM network could severely damage the bank's reputation, as customers lose confidence in the bank's ability to secure their personal and financial information. This may result in reduced ATM usage, further affecting the bank's credibility. In addition to reputational damage, the bank could suffer direct financial losses due to unauthorized transactions and withdrawals.	Reputation & Customer Confidence	9	6,75
		Financial	9	6.75
	If the ATM network is disrupted, the resulting downtime could prevent customers from accessing their funds. This downtime negatively impacting operational efficiency and leading to further customer	Productivity	8	6
		Safety & Health	2	1.5
	If sensitive customer data is compromised, the bank may face regulatory fines for failure to protect that data in compliance with legal requirements. In addition, customers whose information is exposed may pursue legal action against the bank, leading to further financial penalties and damage to the bank's reputation.	Fines & Legal Penalties	8	6
		User Defined Impact Area	8	6
			Relative Risk Score	**33.0**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	✓ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	• Limit employee access to the ATM network based on role and need, using principles of least privilege. • Implement regular security awareness training for employees on ethical practices and legal consequences of misuse.
Physical Controls	• Restrict physical access to ATM servers or terminals to only authorized personnel.
Technical Controls	• Implement role-based access controls (RBAC) to limit what employees can access within the ATM network. Require employees to use multi-factor authentication when accessing sensitive ATM systems or databases. This adds an extra layer of security beyond just passwords and reduces the risk of unauthorized access.

Justification of probability and severity values

Attribute	Value	Justification
Probability	75%	There is a high chance (75%) that an internal employee could misuse the ATM system because they have access to sensitive data.
Reputation & Customer Confidence	9	If an employee misuses the system, customers may lose trust in the bank's ability to keep their money safe. This could lead to fewer people using the bank's ATMs and hurt the bank's reputation.
Financial	9	Misuse could lead to unauthorized withdrawals or transactions, causing financial losses for the bank. The bank might also need to spend money on investigations and compensations.
Productivity	8	Misuse of the system could cause downtime for ATMs, preventing customers from accessing their money and reducing the bank's efficiency.
Safety & Health	2	While this doesn't directly impact physical safety, it can create stress for employees dealing with the issue. However, the overall risk to safety and health is low.
Fines & Legal Penalties	8	If customer data is compromised, the bank could face fines from regulators and might be sued by affected customers, leading to financial and reputational losses.
User Defined Impact Area	8	The bank may have to spend money in the long term to recover from the incident, improve security, and prevent future misuse. This includes costs for new security measures and employee training.

Asset 03- Customer Mobile Banking Application

03.1 Allegro Worksheet 08 for Customer Mobile Banking Application

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Customer Mobile Banking System.	It handles all customer transactions and account information.	A mobile application that allows customers to manage their bank accounts, transfer money, and monitor transactions.
(4) Owner(s) *Who owns this information asset?*		
The IT Department and Bank's Cybersecurity Team.		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Customer account data should only be accessed by authenticated users, system administrators, and authorized bank personnel.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Transaction records and customer data can only be modified by authorized bank employees and system administrators.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The system must be available to customers, bank employees, and system administrators at all times for performing financial transactions and account management.
	This asset must be available for 24 hours, 7 days/week, 52 weeks/year.	This asset should be 99.999%(five nine) availability.
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Lack of security and availability could damage the bank's reputation, leading to loss of trust. Many financial regulations mandate stringent security controls. A system lacking these could face heavy fines and legal consequences.
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	✓ Integrity	❑ Availability	❑ Other

03.2 Allegro Worksheet 10 for Customer Mobile Banking Application

03.2.1 Unauthorized access to customer data

Allegro - Worksheet 10			INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Threat	Information Asset	Customer Mobile Banking System		
		Area of Concern	Unauthorized access to customer data		
		(1) Actor *Who would exploit the area of concern or threat?*	Cybercriminals		
		(2) Means *How would the actor do it? What would they do?*	By attempting unauthorized access, installing malware, or phishing attacks.		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain from selling stolen customer data, conducting fraud, or extorting the bank.		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Customer data is exposed to unauthorized actors, violating confidentiality policies.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
A breach of customer data can lead to legal and regulatory penalties. It can cause reputational damage, resulting in customer loss. Financial losses may occur, along with operational disruption.	Reputation & Customer Confidence	5	3.75
	Financial	4	3
A breach of data integrity through the modification of transaction records can lead to financial fraud and losses. It often results in customer dissatisfaction and a loss of business credibility. Additionally, the organization may face increased audits and	Productivity	3	2.25
	Safety & Health	1	0.75
A system outage or service downtime can lead to a loss of revenue and customer dissatisfaction, potentially	Fines & Legal Penalties	4	3

	causing attrition. It may also result in an operational backlog and penalties for non-compliance.	User Defined Impact Area	3	2.25
			Relative Risk Score	**15**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	• Policies and Procedures: Ensure compliance with secure coding standards, privacy policies, and user data protection regulations. • App Development Training: Developers should be trained on secure coding and mobile application security best practices. • Incident Response Plan: Establish a clear procedure for responding to application-level security breaches.
Technical Controls	• Multi-Factor Authentication (MFA): Require MFA for users and admins to access the app. • Encryption: Ensure end-to-end encryption of sensitive data in transit and at rest. • App Vulnerability Testing: Regular penetration testing and code reviews. • Patch Management: Ensure timely updates and patches to address newly discovered vulnerabilities.
Physical Controls	• Secure Data Centers: Ensure that data centers housing backend servers have restricted access with biometric and badge controls. • Environmental Controls: Implement fire suppression, temperature control, and disaster recovery measures. • Device Security: Encourage users to secure their devices with biometric locks or strong passwords.
Residual Risk	• Data leaks from misconfigured databases or servers. • Insider threats from employees with legitimate access to backend systems. • DDoS attacks that overwhelm server capacity, despite firewalls and monitoring. • Zero-day vulnerabilities in the app could still be exploited before patches are available. • Phishing attacks targeting users could lead to unauthorized access. • User misconfiguration (e.g., weak passwords) may persist despite MFA.

Justification of probability and severity values

Attribute	Value	Justification
Probability	75%	Given the high value of financial data, mobile banking systems are frequently targeted by various actors, making the probability of a breach relatively high.
Reputation & Customer Confidence	5	Reputation is critical in banking; a breach can lead to significant loss of trust and customer base. Recovery from reputational damage is challenging and lengthy.
Financial	4	Financial losses can include direct impacts from fraud, costs associated with breach management, potential lawsuits, and compensation payments.
Productivity	3	System downtime or breach response can temporarily disrupt operations and productivity, but this is usually a short- to medium-term impact.
Safety & Health	1	Data breaches typically don't impact physical safety or health directly, though extreme cases may cause psychological stress.
Fines & Legal Penalties	4	Financial institutions face strict regulatory requirements. Non-compliance due to breaches can result in significant fines and legal costs.
User Defined Impact Area	3	Strategic impacts affect long-term growth and market competitiveness, and can be substantial but often less immediate compared to operational and financial impacts.

03.2.2 Distributed Denial of Service (DDoS) attack on the customer mobile banking system.

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Customer Mobile Banking System		
	Area of Concern	Could be confidentiality, integrity, availability, or other risks.		
	(1) Actor *Who would exploit the area of concern or threat?*	A malicious actor or hacktivist group aiming to disrupt the bank's services.		
	(2) Means *How would the actor do it? What would they do?*	The actor would use a botnet or a network of compromised devices to flood the customer mobile banking system with an overwhelming amount of traffic or requests.		
	(3) Motive *What is the actor's reason for doing it?*	Possible motives include causing disruption to the banking service for financial gain, protesting against the bank or its policies, or attempting to distract the bank from other malicious activities.		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	**Availability:** The DDoS attack would breach the availability requirement of the security triad (Confidentiality, Integrity, Availability), as the system's unavailability would directly affect users' access and functionality.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Frequent or severe disruptions can damage the organization's reputation, leading to lost customer trust and decreased brand value. Financial losses might include transaction processing issues, lost business, and	Reputation & Customer Confidence	9	6.75
	Financial	8	6

	compensation claims. Costs for attack mitigation and operational restoration may also be incurred.			
	Post-attack, the organization would likely need to invest in enhanced security measures to prevent future attacks, including improved DDoS protection solutions, network infrastructure upgrades, and potentially increased staffing for security operations.	Productivity	6	4.5
		Safety & Health	2	1.5
	The organization might face legal or regulatory repercussions if it is found to be non-compliant with industry regulations regarding service availability and data protection. This could include fines or legal actions from regulatory bodies.	Fines & Legal Penalties	5	3.75
		User Defined Impact Area	7	5.25
			Relative Risk Score	**27.75**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Administrative Controls	• Incident Response Plan: Implement procedures for detecting and mitigating DDoS attacks. • Service Agreements: Maintain SLAs with third-party DDoS mitigation service providers. • Training: Train IT personnel on identifying early warning signs of DDoS attacks.
Technical Controls	• Traffic Monitoring: Use tools to detect and respond to abnormal traffic patterns. • Rate Limiting: Implement rate limiting on requests to the banking servers to reduce traffic overload. • DDoS Protection Services: Partner with a DDoS protection provider to absorb malicious traffic. • Load Balancing: Use load balancers to distribute traffic across multiple servers and prevent overloading.
Physical Controls	• Data Center Redundancy: Implement geographically distributed data centers to maintain availability in case of attack on one location. • Restricted Access: Limit physical access to server rooms hosting the mobile banking system's infrastructure.
Residual Risk	• DDoS attacks may still overwhelm resources despite DDoS protection services.

	• Attacks could target third-party providers that are integral to the banking system's operation. • Some latency or downtime might still occur during mitigation, affecting customer access temporarily.

Justification of probability and severity values

Attribute	Value	Justification
Probability	75%	The probability is set at 75% because DDoS attacks are increasingly common and sophisticated, making it likely that an organization, particularly one with a significant online presence like a mobile banking system, will experience such an attack.
Reputation & Customer Confidence	9	A DDoS attack can severely damage the organization's reputation and erode customer confidence. The likelihood of this impact is high because customers may lose trust in the bank's ability to provide reliable services, leading to a substantial impact on reputation.
Financial	8	Financial impacts from a DDoS attack are typically severe. Costs can include lost revenue, mitigation expenses, and compensation for affected customers. The probability of significant financial impact is high due to the direct and indirect costs associated with such attacks.
Productivity	6	The impact on productivity is moderate. While a DDoS attack can disrupt normal operations and reduce productivity by affecting transaction processing and system performance, the impact is generally less severe compared to reputation and financial consequences.
Safety & Health	2	DDoS attacks have minimal direct impact on safety and health. While there might be some stress or operational pressure on employees, the primary effects are operational and financial, making the safety and health impact low.
Fines & Legal Penalties	5	There is a moderate likelihood of facing fines or legal penalties if the DDoS attack leads to regulatory non-compliance or breaches. The severity depends on how well the organization adheres to regulatory requirements and the specific nature of the disruption.
User Defined Impact Area	7	For user-defined impact areas, the value is high if the DDoS attack affects critical business functions or key customer segments. The severity is high due to the potential for significant disruption in these vital areas.

References

https://www.cloudflare.com/learning/ddos/ddos-mitigation/

https://www.rapid7.com/fundamentals/malware-attacks/

https://www.asisonline.org/security-management-magazine/articles/2024/09/banks/ATM-crime-risks/