1.0 Allegro worksheets

1.1 ATM Skimming

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk	**Threat**	Information Asset	ATM card, customers who use ATM cards, ATM machines		
		Area of Concern	ATM Skimming		
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder		
		(2) Means *How would the actor do it? What would they do?*	Intruder will fix external devices to the ATM machine and skim the data from the cards when customers enter it to the machine and also record the password when the customer types it in the key board using a hidden camera.		
		(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud)		
		(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?*	Only the owner of the ATM card should be able to withdraw money from his/her account using the ATM card		
		(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**
	If money from customers' accounts are stolen, bank is responsible of investigating and giving the money back to protect the reputation of the bank. This might bring massive financial losses to the bank. In addition to that, customer will be disappointed and be discouraged to use ATM card service, which will finally lead to a negative impact on the brand name		Reputation & Customer Confidence	3	2.25
			Financial	5	3.75

	Investigating the crime might take excessive hours of effort, analysing the evidence gathered through CCTV and analysing the transactions happened. A special task force might be needed for the investigation and the cost of it will be high	Productivity	3	2.25
		Safety & Health	0	0
	If the customers take legal actions against the banks, even though the bank is not directly responsible for the theft of their money, it might cost some amount of resources for justifications and legal services (example – Hiring Lawyers)	Fines & Legal Penalties	2	1.5
		User Defined Impact Area	0	0
			Relative Risk Score	**9.75**

(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?*
Break the single authority processes.	Rotate the ATM hardware providers, which will ensure that just one person will not handle the operations exclusively for a machine over a specified point.
Surveillance	Organize ATM cash audit programs where machines will be randomly inspected onsite and also acknowledge the security officers as well as the customers to report any unusual devices or people immediately.
Set standards	The branch/terminal or the bank should be aware of what the ATM look like. After installing the ATM hardware and software there should be proper documentation and visual presentation (photographs) ready to be crosschecked whenever a suspicious device is been identified.
Share Experience	The past and present experience should be properly documented with evidence for future reference. Sharing the Risk experience will help the institutions to increase the security in the future and to improve the process.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	Probability is high because the attackers has been successful in replicating the same appearance to the trackers enabled devices. Since it is a physical attack and currently there are less controls the chances of attack is high.
Reputation & Customer Confidence	3	Reputation of the company will be damaged and the customer confidence about the company will reduce in a comparatively low value since this will affect only to a specific section of customers (ATM card users). Customers might lose their confidence in using ATM cards, but the reputation of the company will highly unlikely to be fully damaged. Therefor a low value is given (3/10)
Financial	5	Financial loses will occur to the customer as well as the institute. Customer might lose their funds from the attack and due to the legal processes institute might have to recover the customer loses. Therefore, an average value is given (5/10)
Productivity	3	Productivity of the employees of the customers might reduce due to additional task arouse due to investigation and prevention of the damage. However, the impact on productivity is for a short time. Once the solution is identified the productivity of the employees will go back to a stable state. Therefor a low value is given (3/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	2	Since the attack is an external attack the chances of getting fines are less. There is a possibility for being charged with penalties for insufficient risk mitigation methods which leads to loss of money from customer’s account. Therefore, a low value is given (2/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.2 Customer personal data breach

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk		Information Asset	Customer, customer details, bank details		
		Area of Concern	Customer personal data breach		
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Internal staff member		
		(2) Means *How would the actor do it? What would they do?*	Internal staff member who might or might not aware of the company or country's rules and compliances might expose sensitive data of a customer, which is also referred to as insider data to a third party.		
		(3) Motive *What is the actor's reason for doing it?*	Can be Intentional (Fraud) or accidental		
		(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?*	Customer's personal data should only be accessed by the relevant stakeholders in the bank and only be given to other responsible parties if the government regulations forces to do so. Sensitive data of the customer, in the wrong hands can cause major financial loses.		
		(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**
		If customer's personal data is leaked, bank is responsible of investigating it to protect the reputation of the bank. This might bring massive financial losses to the bank. In addition to that, customer will be disappointed and be discouraged to use services of the bank, which will finally lead to a negative impact on the brand name	Reputation & Customer Confidence	8	6
			Financial	5	3.75

	Investigating on the data breech might take excessive hours of effort, analysing the evidence gathered through history of specific systems, archives and analysing the transactions happened. A special task force might be needed for the investigation and the cost of it will be high	Productivity	3	2.25
		Safety & Health	0	0
	If the customers take legal actions against the banks, even though the employee’s action was not intentional for the theft of their data, it might cost some amount of resources for justifications and legal services (example – Hiring Lawyers)	Fines & Legal Penalties	6	4.5
		User Defined Impact Area	0	0
			Relative Risk Score	**16.5**

(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?*
Conduct workshops, awareness sessions and conferences	The employees should be given a proper induction on data security and it’s risk. Even after the initial training sessions it is important to keep the employees updated about the possible attacks and new risks.
Surveillance	Organize internal and external audits on all the communication channels and other data transformation methods frequently. Restrict inappropriate files sharing with external parties examples - set limits for the shareable files size, control external mail channels
Set standards	Set internal standards for customer information managements inside the organization. Create timely compliance documents and update the existing agreements, rules and regulations with the employees, about internal data security.
Share Experience	The past and present experience should be properly documented with evidence for future reference. Sharing the Risk experience will help the institutions to increase the security in the future and to improve the process.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	Probability is high because the company is not checking the outside emails sent by the employees of the company. Since sending emails to outside of the organization cannot be controlled. Monitoring tools to check on the size and content of the emails is not implemented at the moment and employees can use external devices such as flash drives to copy data from their computers. Additionally, employees are allowed to use cloud data storages (example – Google drive) and also personal emails and social media. Since the controls are less, there is a high probability for this risk.
Reputation & Customer Confidence	8	Reputation of the company will be damaged and the customer confidence about the company will reduce in a high rate, since customers believe that their personal information is safe but failure to do so will reduce their confidence on the company. Customers might lose their confidence in using company products. Therefor a high value is given (8/10)
Financial	5	Financial loses will occur to the company if the customer is aware of the breech and if the customer takes a legal action against the company. Customer might lose their trust and due to the legal processes institute might have to recover the customer loses. Therefore, a medium value is given (5/10)
Productivity	3	Productivity of the employees of the customers might reduce due to additional task arouse due to investigation and prevention of the damage. However, the impact on productivity is for a short time. Once the solution and possible controls are identified the productivity of the employees will go back to a stable state. Therefor a low value is given (3/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	6	Since the attack is an internal attack the chances of getting fines are high. There is a possibility for being charged with penalties for insufficient risk mitigation methods which leads to loss of customer data. The company might have to pay lawyer fees, law court fines and also penalties for the customer. Therefore, a high value is given (6/10)

User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.3 Phishing attacks

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	**Threat**	Information Asset	Customer, customer details, bank details
		Area of Concern	Phishing attacks
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder
		(2) Means *How would the actor do it? What would they do?*	Intruder will create an exactly similar User interface to the Banking application. Then this will be sent via emails as advertisements, promotions, or paying links. (spams). When user clicks on these links and tried to logged in, Intruder gets all the sensitive information user entered on that fake user interface. This may be user's credit card number, cvv, account number, name etc. Intruder keeps collecting information like these. So afterwards intruder can logged in to these accounts using steal credentials.
		(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud)
		(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?*	By having customer's sensitive bank details intruder can easily impersonate to be the customer and use customer's money for his/her benefit. Customer's personal data should only be accessed by the relevant stakeholders in the bank and only be given to other responsible parties if the government regulations forces to do so. Sensitive data of the customer, in the wrong hands can cause major financial loses.
		(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**
	If intruder did any sort of modification to the account (changing passwords, transferring money, making a payment using the account, viewing history of transactions, etc), bank is not responsible for investigating on the security threat and data breach happened. Bank should be able to trace all the transactions done by intruder with details.	Reputation & Customer Confidence	2	1
		Financial	5	2.5
	Investigating on the attack might take excessive hours of effort, analysing the evidence gathered through different channels and analysing the transactions happened. A special task force might be needed for the investigation and the cost of it will be high	Productivity	0	0
		Safety & Health	0	0
	If the customers take legal actions against the banks, even though the bank is not directly responsible for the theft of their money, it might cost some amount of resources for justifications and legal services (example– Hiring Lawyers)	Fines & Legal Penalties	1	0.5
		User Defined Impact Area	0	0
			Relative Risk Score	**4**

(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?*
Keep customer informed about the phishing attack types	New phishing scams are being developed all the time and it is important to keep information about those up to date. The risks of different phishing scams should be informed to the customer whenever possible.
Install an Anti-Phishing Toolbars	Advising the customers to Install an Anti-Phishing Tools will control the phishing attacks that can happen to the customer. If the customer uses a malicious site those tools will give warnings before customer clicks on any of the links available in the fraud sites.

Checking Online Accounts Regularly	It is important to advise the customer to check their accounts regularly. If the customer doesn’t visit an online account for a while, intruder’s task will be easy. To prevent bank phishing and credit card phishing scams, customer should be advised to personally check their statements regularly. Bank should suggest them Get monthly statements for their financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without their knowledge.
Changing Passwords	Customer should be advised to get into the habit of changing their passwords regularly. Even if the customer is not following the requested good practices, bank can reset the customer passwords and ask them to create new passwords every 6 months or depending on bank’s choice.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	Probability is average since most of the browsers supports anti-virus and scam prevention tools and recommend users to use when they login to a financial application. But there are customers who are not aware of using the tools and not aware of the risks, therefore a medium chance of a phishing attack is there.
Reputation & Customer Confidence	2	Reputation of the company is not at high risk since the large portion of controls are in the customer’s hand. Customers are highly responsible on their actions and there is a possibility that customer will lose their confidence about the bank if a phishing attack happens due to bank not advising the customer properly. Therefore, a low value is given (2/10)
Financial	5	Financial loses will occur to the customer when they lose their sensitive account data, but it will not give and big impact on the profit of the bank since customer is responsible of their actions. Bank might have to spend on investigation purposes and improving mitigation controls. Therefore, a medium value is given.
Productivity	0	There is no impact on productivity. Therefore, no value is given (0/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)

Fines & Legal Penalties	1	There is a lesser chance of getting legal fines since the possible controls using firewalls and other methods are used. But due to the possibility of undiscovered loophole a lesser value is given (1/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.4 DDoS Attacks using Botnets

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	**Threat**	Information Asset	Bank, Customer
		Area of Concern	DDoS Attacks using Botnets
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder who uses Botnets
		(2) Means *How would the actor do it? What would they do?*	Botnets are group of computers with installed malware and showing malware behaviour. These are controlled by hackers in large amounts to attack a server and stopping the service provided by it. These are also designed to steal data, and some are in form of ransomware. These are self-propagating and keeps continuously attacking a server pointed. These can be also trained to exploit website vulnerabilities and crack weak authentications, or incorrect authentications flows (e.g.: Incorrectly architecture of SAML flows). These botnets request to the same service at single time and make the service incapable of providing response at once. Hence server stops, that's called Denial of service attack or DDoS attack.
		(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud)
		(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?*	Online banking system will be inaccessible causing total system failure.

(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?

If bank website has weak authentications or incorrectly configured auth flows, botnets may crack the vulnerability and data will be bleached. If happens, bank should be responsible for loss of customer data.

Under GDPR regulations bank have to pay a fine after estimating the type of attack (DDoS attacks are 3 types; volumetric attacks, application attacks, protocols attacks) and its damage.

Customers won't be able to log in to system. Hence Bank will be lost it reputation due to loss of productivity.

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	**Value**	**Score**
Reputation & Customer Confidence	8	6
Financial	5	3.75
Productivity	7	5.25
Safety & Health	0	0
Fines & Legal Penalties	4	3
User Defined Impact Area	0	0
	Relative Risk Score	**18**

(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?*
Buy more bandwidth	This enables the server to handle spikes in traffic. This traffic may be due to actual legitimate user increase or malicious botnet networks. By the way if the server has more bandwidth it will be able to handle the TPS (Transactions per second).

Network Traffic Analyzer with spike detection.	This enables the bank to identify DDoS attacks to server. Perfect monitoring system can clearly separate an actual user from a botnet. Human intervention is also highly needed to monitor this traffic and mitigate immediately once detected. So, Network engineers need to be engaged in this work 24*7.
API throttling	Throttling is done to limit the request count and set permissions on requests to validate the API request to check whether its valid or not. You can define this API level as well as application level.
Set Concurrent Connections Limit	This will automatically control DDoS attacks. This sets amount of pool for users. It can be configured region wise, IP wise etc. This will mitigate DDoS attacks automatically.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	75%	Probability is high because there are many DDoS attacks around and cost for initiating this type of attack is very low. One person can control botnets and completely breaks a system temporally.
Reputation & Customer Confidence	8	Reputation of the company will be highly damaged. Due to the down time of systems, customer will lose the faith about the bank and it's systems. Therefore, the high impact value is given (8/10)
Financial	5	Financial loses will occur to the customer as well as the institute. Customer might lose their funds from the attack and due to the legal processes institute might have to recover the customer loses. Therefore, an average value is given (5/10)
Productivity	7	Productivity of the banking application goes down with this. This will result in complete system failure. No one will be able to log in until the server restarts. There for the impact on productivity is high (7/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	4	Bank might be fined under GDPR for data breach. Therefore, a medium value is given (4/10)

User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)

1.5 Fund transfers using CSRF attacks

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	**Threat**	Information Asset	Banking customer, customer’s sensitive information
		Area of Concern	Fund transfers using CSRF attacks
		(1) Actor *Who would exploit the area of concern or threat?*	Intruder
		(2) Means *How would the actor do it? What would they do?*	CSRF (Cross-Site Request Forgery) is most popular attack among banking applications. These attacks are state changing operations. This forces the user to execute actions where user is authenticated. (transfer money from user account to another one).
		(3) Motive *What is the actor’s reason for doing it?*	Intentional (Fraud)
		(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?*	User will experience change in state changing operation like reduced account balance, logout suddenly, automatic money transfers.
		(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**
If bank website has this CSRF vulnerability, hacker can easily execute unwanted commands using a legitimate user. These CSRF attacks may be used to transfer funds etc. So, bank should be responsible for it.	Reputation & Customer Confidence	3	1.5
	Financial	5	2.5
	Productivity	3	0

	Hacking Admin account can compromise security of all accounts. Creation, deletion, update of accounts can happen without the knowing of bank.	Safety & Health	0	0
	Bank will quickly erode the websites credibility after these types of attack. So, customer might close their accounts on the bank by withdrawing money or they may stop using online banking as a result.	Fines & Legal Penalties	2	1
		User Defined Impact Area	0	0
			Relative Risk Score	**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?*
Web Application Firewall	These types of application are designed to scan and filter all types of incoming website traffic to the website. As CSRF is a risk arising with web applications using a firewall will minimize the risk.
Implementing Synchronizer Token Pattern	It’s a technique where a token, secret and unique value for each request, is embedded by the web application in all HTML forms and verified on the server side.
Implementing Double submit cookie pattern	If storing the CSRF token in session is problematic, an alternative defence is use of a double submit cookie. It is defined as sending a random value in both a cookie and as a request parameter, with the server verifying if the cookie value and request value match.

Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	Probability of a CSRF attack is medium since there are many controls when using banking applications. Most of the latest browsers and security/malware protection software supports CSRF prevention. Even though there are controls CSRF stands in top security threats, therefore 50% chance of CSRF attack is there.
Reputation & Customer Confidence	3	Reputation of the company will be damaged. Since the company has taken controls to reduce the probability of occurrence, a relatively less impact value is given. (3/10)
Financial	5	Financial loses will occur to the customer as well as the institute. Customer might lose their funds from the attack and due to the legal processes institute might have to recover the customer loses. Therefore, an average value is given (5/10)
Productivity	0	Productivity of the company is not affected. Therefore, no value is given (0/10)
Safety & Health	0	There is no impact on safety and health. Therefore, no value is given (0/10)
Fines & Legal Penalties	2	There is a minor impact on legal penalties as customers might complain and if proper mitigation plan is not there, company will be subjected to fines. Since some of the mitigation methodologies are time consuming or expensive, company might not be able to fully control the risk. Therefor a less impact value is given (2/10)
User Defined Impact Area	0	There are no User Defined Impact Areas. Therefore, no value is given (0/10)