Allegro - Worksheet 10	Information Asset Risk Worksheet			
Information Asset Risk — **Threat**	Information Asset	Banking details		
	Area of Concern	*Mobile banking trojans*		
	(1) Actor *Who would exploit the area of concern or threat?*	Malicious actor		
	(2) Means *How would the actor do it? What would they do?*	Mobile trojans delivered as smart home apps carrying keyloggers and more sophisticated malwares		
	(3) Motive *What is the actor's reason for doing it?*	Financial gain		
	(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?*	Confidentiality and integrity breached		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☐ **Medium**	☑ **Low**

(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**
Compromised account can be emptied by malicious actor	Reputation & Confidence	M	8
	Financial	H	15
Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments.	Productivity	M	6
	Safety & Health	H	18
	Fines & Legal Penalties	H	3
	User Defined Impact Area	L	2
		Relative Risk Score	**44**

(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?*
People	Raise awareness in household members. Train them to verify legitimacy of new apps and download only from reliable sources.
Endpoint devices	Keep devices up to date. Never disable the device's security features.
Accounts	Enable 2FA and OTP codes.
Accounts	Enable activity notifications to quickly detect suspicious operations.

Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Banking details		
		Area of Concern	*Unsafe processing and storing of bank details*		
		(1) Actor *Who would exploit the area of concern or threat?*	Advanced threat actors		
		(2) Means *How would the actor do it? What would they do?*	Banking details are required to access certain IoT platforms. Data Centers where those informations are stored may be located in areas subject to lighter cybersec regulation, exposing user's data in case of an incident.		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain		
		(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?*	Confidentiality and integrity of the asset breached		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☐ **Medium**	☑ **Low**

(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**
Compromised bank account can be emptied by malicious actor	Reputation & Confidence	M	8
	Financial	H	15
Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments.	Productivity	M	6
	Safety & Health	H	18
	Fines & Legal Penalties	H	3
	User Defined Impact Area	L	2
		Relative Risk Score	**44**

(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?*
Accounts	Enable 2FA and OTP codes.
Accounts	Enable activity notifications to quickly detect suspicious operations.

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Banking details	
		Area of Concern	*Unsafe processing and storing of bank details / trojans - Residual risk*	
		(1) Actor *Who would exploit the area of concern or threat?*	Advanced threat actors	
		(2) Means *How would the actor do it? What would they do?*	Acquiring information about payment cards using trojans or breaching service providers.	
		(3) Motive *What is the actor's reason for doing it?*	Financial gain	
		(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?*	Confidentiality of the asset breached	
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☐ **Medium** ☑ **Low**

(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**
2FA and OTP codes will prevent the attacker from using the card.	Reputation & Confidence	M	8
	Financial	L	5
If the attacker succeeds and makes a transaction, a notification will be sent to the owner, which can immediately block the card/account.	Productivity	M	6
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	L	2
		Relative Risk Score	**28**

(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?*