Allegro - Worksheet 10		orksheet 10	Information Asset Ri	SK WORKSHEET				
In fo r m at io n A ss et R is k	T h re at	Information Asset	Banking details					
		Area of Concern	Mobile banking trojans	Mobile banking trojans				
		(1) Actor Who would exploit threat?	it the area of concern or	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✓ 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? Compromised account can be emptied by malicious actor Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments.					Severity evere are these consequences to the ization or asset owner by impact area?		
					Impact Area	Value	Score	
				Reputation & Confidence	М	8		
					Financial	Н	15	
				• •	Productivity	М	6	
					Safety & Health	Н	18	
					Fines & Legal Penalties	Н	3	
					User Defined Impact Area	L	2	
							£	

(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 sec	urity features.				
Accounts	Enable 2FA and OTP codes.						
Accounts	Enable activity notifications to	quickly detect suspicion	as operations.				

In for at a large of Concern at at io a large of Concern at a large of concern or threat? (2) Means How would the actor do it? What would they do? (2) Means How would the actor do it? What would they do? (3) Motive What is the actor's reason for doing it? (4) OutCome What would be the resulting effect on the information asset? (5) Security Requirements How would the information asset security requirements be breached? (6) Probability What is the likelihood that this threat scenario could occur? (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 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 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 Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments.	Allegro - Worksheet 10			Information Asset Ri	SK WORKSHEET				
at a	fo r m at io n A ss et R is	h re		Banking details					
(1) Actor who would exploit the area of concern or threat? (2) Means How would the actor do it? What would they do? (3) Motive What is the actor's reason for doing it? (4) Outcome What would be the resulting effect on the information asset? (5) Security Requirements How would the information asset's security requirements be breached? (6) Probability What is the likelihood that this threat scenario could occur? (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 as a result of the outcome and breach of security requirements? Compromised bank account can be emptied by malicious actor Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments. Advanced threat actors 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. Disclosure Disclosure Destruction Interruption Confidentiality and integrity of the asset breached How severe are these consequences to the organization or asset owner as a result of the outcome and breach of security requirements? Impact Area Value Score Reputation & Confidence M 8 Confidence Financial H 15 Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments.				Unsafe processing and storing of bank details					
C2 Means How would the actor do it? 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. C3 Motive What is the actor's reason for doing it? Modification Disclosure Destruction Interruption					Advanced threat actors				
Confidentiality and integrity of the asset breached would the information asset's security requirements How would the information asset's security requirements be breached? Good Probability What is the likelihood that this threat scenario could occur? High Medium Low					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				
Modification Interruption					Financial gain				
Compromised bank account can be emptied by malicious actor Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments. Fines & Legal H 15			• •						
that this threat scenario could occur? (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? How severe are these consequences to the organization or asset owner by impact area? Impact Area Value Score			would the information asset's security		Confidentiality and integrity of the asset breached				
What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements? How severe are these consequences to the organization or asset owner by impact area?					☐ High	☐ Medium	✓	Low	
Compromised bank account can be emptied by malicious actor Reputation & M 8 Confidence Financial H 15 Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments. Safety & Health H 18 Fines & Legal H 3		What are the consequences to the organization or the info				h asset owner as How severe are these consequences to the			
actor Confidence Financial Financia						Impact Area	Value	Score	
Compromised accounts can be used for illegal purposes like money laundering and processing illegal payments. Financial H 15			romised bank a	ccount can be emptied	by malicious		М	8	
money laundering and processing illegal payments. Safety & Health H 18 Fines & Legal H 3						Financial	Н	15	
Safety & Health H 18 Fines & Legal H 3						Productivity	М	6	
						Safety & Health	Н	18	
1 Chaucs						Fines & Legal Penalties	Н	3	
User Defined Impact Area L 2						1	L	2	

(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	For the risks that you decide to mitigate, perform the following:							
On what container would you apply controls?	What administrative, technical, and p would still be accepted by the organiz	hysical controls would you apply on th ation?	nis container? What residual risk					
Accounts	Enable 2FA and OTP codes.							
Accounts	Enable activity notifications	to quickly detect suspicious o	pperations.					

What would they do? trojans or breaching service providers.	ng			
A A Cquiring information about payment cards using trojans or breaching service providers. (1) Actor Who would exploit the area of concern or threat? (2) Means How would the actor do it? What would they do? (3) Motive What is the actor's reason for doing it? (4) Outcome What would be the resulting effect on the information asset? (5) Security Requirements How would the information asset security requirements be breached? (6) Probability What is the likelihood that this threat scenario could occur? (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 organization or asset owner as a result of the outcome and breach of security requirements? Impact Area Value Reputation & Confidence M Confidence	ng			
(1) Actor who would exploit the area of concern or threat? Advanced threat actors Acquiring information about payment cards using trojans or breaching service providers. Financial gain (3) Motive What is the actor's reason for doing it? (4) Outcome What would be the resulting effect on the information asset? (5) Security Requirements How would the information asset's security requirements be breached? (6) Probability What is the likelihood that this threat scenario could occur? (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 organization or asset owner as a result of the outcome and breach of security requirements? Impact Area Value 2FA and OTP codes will prevent the attacker from using the card.	ng			
(2) Means How would the actor do it? What would they do? (3) Motive What is the actor's reason for doing it? (4) Outcome What would be the resulting effect on the information asset? (5) Security Requirements How would the information asset security requirements be breached? (6) Probability What is the likelihood that this threat scenario could occur? (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 organization or asset owner by impact Impact Area Value 2FA and OTP codes will prevent the attacker from using the card.	ng			
(3) Motive What is the actor's reason for doing it? (4) Outcome What would be the resulting effect on the information asset? (5) Security Requirements How would the information asset's security requirements be breached? (6) Probability What is the likelihood that this threat scenario could occur? (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 organization or asset owner by impact of the outcome and breach of security requirements? Impact Area Value 2FA and OTP codes will prevent the attacker from using the card.	Acquiring information about payment cards using trojans or breaching service providers.			
Confidentiality of the asset breached Gonfidentiality of the asset breached Gonf	Financial gain			
would the information asset's security requirements be breached? (6) Probability What is the likelihood that this threat scenario could occur? (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 organization or asset owner by impact Impact Area Value 2FA and OTP codes will prevent the attacker from using the card.				
that this threat scenario could occur? (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? Impact Area Value 2FA and OTP codes will prevent the attacker from using the card. Reputation & Confidence M	Confidentiality of the asset breached			
What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements? How severe are these consequences to organization or asset owner by impact Impact Area Value 2FA and OTP codes will prevent the attacker from using the card. Reputation & Confidence M	Low			
2FA and OTP codes will prevent the attacker from using the card. Reputation & Confidence M	1 ' '			
card. Confidence Confidence	Score			
	8			
Financial L	5			
If the attacker succeeds and makes a transaction, a notification will be sent to the owner, which can immediately	6			
block the card/account. Safety & Health L	6			
Fines & Legal Penalties	1			
User Defined Impact Area	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	e following:			
On what container would you apply controls?	What administrative, technical, and ph would still be accepted by the organize	ysical controls would you apply on this attion?	container? What residual risk		
1					