Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**

Information Asset Risk	**Threat**	Information Asset	Smart Home
		Area of Concern	*Device hijacking*
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organized malicious actors
		(2) Means *How would the actor do it? What would they do?*	Exploiting device vulnerabilities to take control of it
		(3) Motive *What is the actor's reason for doing it?*	Motivations can range from disturbance to a wider scheme targeting a specific vendor or device model. Hijacked devices can serve as entry points for further 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?*	Integrity and productivity impacted.
		(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**
Threat actors in control of devices can have serious consequences, from disturbing normal usage, to opening doors and abusing video surveillance systems.	Reputation & Confidence	M - 2	8
	Financial	H - 3	15
Hijacked devices can serve as entry point for further lateral movement in the network;	Productivity	H - 3	9
	Safety & Health	M - 2	12
Hijacked devices can be used as part of botnets to start other attacks arming the household or other organizations.	Fines & Legal Penalties	M - 2	2
	User Defined Impact Area	H - 3	6
		Relative Risk Score	**104**

(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?*
IoT device	*Regularly update devices firmware to latest version*
IoT device	Prefer IoT devices utilizing firmware signatures to prevent installation of compromised firmwares.
IoT devices	Prefer IoT devices not requiring an internet connection to operate (Matter, Zigbee…)
Home Net	Segment Home Network connecting IoT devices to a dedicated subnet and use a firewall to filter traffic
Home Net	Use the firewall to prevent IoT devices from being able to reach the Internet except for the ones which can't be operated without it.
IoT devices	Regularly check router traffic logs and metrics to spot anomalies
Home Net	Configure Host Isolation in the IoT subnet to prevent devices´ cross-talking unless specifically needed.

Allegro - Worksheet 10	**Information Asset Risk Worksheet**		
Information Asset Risk	**Threat**	Information Asset	Smart Home
		Area of Concern	*Residual risk - Device hijacking*
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organized malicious actors
		(2) Means *How would the actor do it? What would they do?*	Exploit device during a firmware update or using wifi techniques. Device cannot communicate with the internet, nor with the rest of the Home Network.
		(3) Motive *What is the actor's reason for doing it?*	Motivations can range from disturbance to a wider scheme targeting a specific vendor or device model. Hijacked devices can serve as entry points for further 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?*	Integrity and productivity impacted.
		(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**
The specific device may become unusable.	Reputation & Confidence	L	4
	Financial	L	5
The device needs to be recovered or replaced.	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	M	2
		Relative Risk Score	**21**

(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?*

Allegro - Worksheet 10		**Information Asset Risk Worksheet**	
Information Asset Risk	**Threat**	Information Asset	Smart Home
		Area of Concern	*Device running out of batteries*
		(1) Actor *Who would exploit the area of concern or threat?*	Smart devices like thermostats are often powered by batteries whose duration range from months to years.
		(2) Means *How would the actor do it? What would they do?*	Most probably forgetting to replace them on time, or missing the notifications.
		(3) Motive *What is the actor's reason for doing it?*	Allowing wireless operation of devices.
		(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 breached, efficiency may be impacted too.
		(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**
Devices can't be operated until batteries are replaced.	Reputation & Confidence	L	4
	Financial	L	5
Many cheap consumer grade devices don't have a good failsafe design. In examples, many thermostat valves open completely when they run out of batteries, resulting in huge wastes of energy.	Productivity	M	6
	Safety & Health	M	12
Many Smart door-locks can not be opened until batteries are replaced.	Fines & Legal Penalties	L	1
	User Defined Impact Area	M	4
		Relative Risk Score	**96**

(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?*
IoT devices	Before purchasing a battery operated device, check data sheets, forums and reviews to acknowledge its low battery behavior, average battery duration and possible design faults. Prefer device designs with fail-safe mechanisms.
IoT devices	Set-up low battery notifications and make sure to receive them.
IoT devices	Implement a regular battery-check routine, especially before leaving the household for extended amounts of time.
IoT devices	Especially for door locks and similar critical devices, plan ahead for a possible battery failure. Make sure to have backup methods to open the lock, and inform all household members.
People	Have a trusted person who can enter the household in case of battery failure while all the household members are away.

Allegro - Worksheet 10	**Information Asset Risk Worksheet**

Information Asset Risk	**Threat**	Information Asset	Smart Home
		Area of Concern	*Internet connection failure*
		(1) Actor *Who would exploit the area of concern or threat?*	Residential internet connections may have temporary faults or interruptions.
		(2) Means *How would the actor do it? What would they do?*	The cause may depend on the ISP, the router, billing issues or problems affecting the physical data lines.
		(3) Motive *What is the actor's reason for doing it?*	Motivation may vary, maintenance, road works, natural disasters, router issues, overcommitment of the network, faults…
		(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 impacted
		(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**
Devices controlled through cloud services become inoperable.	Reputation & Confidence	L	4
	Financial	L	5
Users won't be able to control and monitor the smart devices from outside.	Productivity	M	6
	Safety & Health	L	6
Other aspects of household life impacted, like home office and entertainment.	Fines & Legal Penalties	L	1
	User Defined Impact Area	M	4
		Relative Risk Score	**52**

(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?*
IoT devices	Always purchase devices which don't require an internet connection to operate (Matter, Zigbee, ESPhome, Tasmota..)
Gateway	Program routines to be sure the essential appliances like heating are operated in the most efficient way autonomously and not rely on user inputs, which won't be delivered in the case of an internet failure while every household member is away.
Home Net	Some smart-home gateways and high-end routers provide the possibility to install a SIM card for a backup mobile connection.

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	**Threat**	Information Asset	Smart Home
		Area of Concern	*Local network failure*
		(1) Actor *Who would exploit the area of concern or threat?*	Wifi access points
		(2) Means *How would the actor do it? What would they do?*	
		(3) Motive *What is the actor's reason for doing it?*	Technical problems, overloading, misconfiguration, disturbed radio signals.
		(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 impacted
		(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**
All the devices relying on that connection for monitoring and control become unavailable.	Reputation & Confidence	L	4
	Financial	L	5
Other aspects of household productivity impacted, like home office and entertainment.	Productivity	H	9
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
		Relative Risk Score	**31**

(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?*
Home Net	Segment network creating a dedicated subnet for IoT devices
Home Net	Use a dedicated access point / a second router / an high-end home gateway to provide a WiFi network only for IoT devices.

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET

Information Asset Risk

Threat

Information Asset	Smart Home
Area of Concern	*Unauthorized data collection*
(1) Actor *Who would exploit the area of concern or threat?*	IoT device vendor and third parties partners
(2) Means *How would the actor do it? What would they do?*	Most consumer devices are controlled by cloud apps which collect PII of the users and usage data from associated IoT devices.
(3) Motive *What is the actor's reason for doing it?*	Those data may be sold for financial profit, incorrectly handled by the service providers, or exposed when processed by third parties.
(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 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?

In documented cases, sensitive data collected by IoT devices were used for purposes like Ai training and were leaked on the internet due to poor handling.

The informations may be sold without user acknowledgement to marketing and advertising companies

Unauthorized collection and processing of user data is against user's rights, as defined by GDPR.

(8) Severity

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

Impact Area	**Value**	**Score**
Reputation & Confidence	M	8
Financial	L	5
Productivity	L	3
Safety & Health	M	12
Fines & Legal Penalties	L	1
User Defined Impact Area	L	2

Relative Risk Score	**93**

(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?*
IoT devices	Carefully check vendor reputation before purchasing devices. Consider which apps are required to control the device. Avoid suspicious brands selling cheap products operated by uncommon apps. Prefer widespread universal devices which can be integrated with popular gateway.
IoT devices	Check Terms and condition agreements when installing any app or integrating a new device in the system.
Endpoint devices	Carefully review smart home apps permissions, apply zero-trust principles.
IoT devices	Enable video cameras and microphones exclusively when needed. A physical power switch, a lens cover, or a PTZ camera with privacy position pointing at the floor provide an extra safety that the capture device is really disabled.
Gateway	When choosing the gateway system vendor for your smart home (Alexa, Google, Open source, High-end…) remember the rule stating that if a service is free you are the product. It is up to the specific household to set a tradeoff between costs and privacy. Open Source solutions are known for better privacy, come for free, but require more technical skills. Professional and High-End solutions provide similar or better levels of privacy, but may be too expensive for an average household. Google, Alexa and similar provide simplicity at no cost, in exchange for personal data.

Allegro - Worksheet 10	**Information Asset Risk Worksheet**

Information Asset Risk	**Threat**	Information Asset	Smart Home
		Area of Concern	*Abuse of device misconfiguration*
		(1) Actor *Who would exploit the area of concern or threat?*	Threat actor with access to home network
		(2) Means *How would the actor do it? What would they do?*	Abuse of a security flaw caused by bad or weak configuration of smart devices controls and security, or bad integration.
		(3) Motive *What is the actor's reason for doing it?*	Lateral movement in the home network, further exploitations.
		(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**
Exfiltration of data, diffusion of malware, botnets.	Reputation & Confidence	M	8
	Financial	L	5
	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	M	2
	User Defined Impact Area	H	6
		Relative Risk Score	**30**

(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?*
IoT devices	Adopt good practices and plan for system security since the beginning of the smart home project. The first devices are often configured with an experimental approach and later forgotten, while the system grows.
IoT devices	Periodically review configurations, especially before expanding or modifying a part of the system. Look for possible ways to make it more efficient, usable and safe. If better technologies become available, consider the benefits of upgrading your systems against the time and costs required.
Home Gateway	Regularly review gateway logs to spot errors or misconfigurations.
IoT devices	Provide all household members a basic “issue reporting” procedure. Use their feedback to improve device controls and routines, spot malfunctioning and assess their appreciation.