2023 Marco Chinello, Kate Michael

SMART HOMES CYBER RISK ASSESSMENT USING OCTAVE ALLEGRO FRAMEWORK.

Introduction

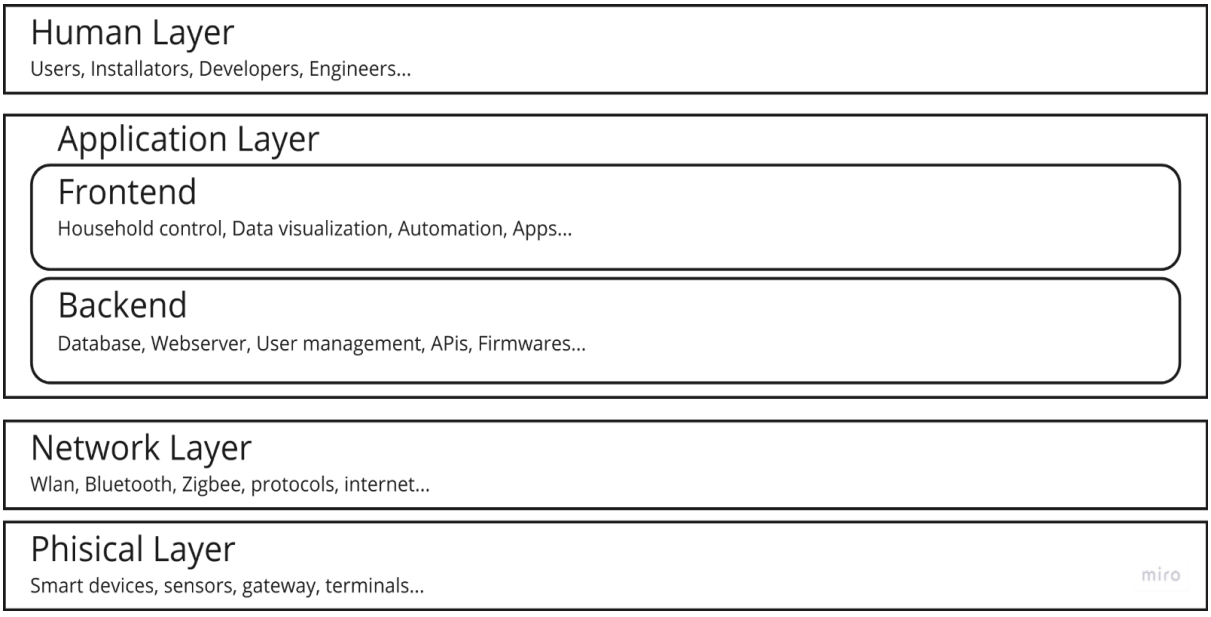
In the **consumer market, IoT technology is associated with "smart home"** devices that can be controlled through connected devices such as smartphones and smart audio systems. IoT devices can be used for home automation to control lighting, heating and cooling, media, and security systems, leading to **energy savings and improved convenience**. IoT can also have a significant **impact on technology and modern society**, connecting physical and virtual devices and enabling more advanced services.

The IoT environment deals with a lot o**f heterogeneous devices which might be vulnerable to cyber attacks and notably increase household's attack surface**. Those factors may lead to privacy breaches, data exfiltration, ransom and IoT botnets, just to name some recent documented incidents.
This complexity and the vast amount of articles and news about incidents related to IoT devices in smarthomes may be **difficult to interpret for entry level users** to whom the products are addressed, potentially leading to unsafe deployments, or excessive fear and difference for this promising technology, thereby **mandating the need for a structured risk assessment process** that is usually part of risk assessment frameworks.

Components and architecture of smart home systems

Smart homes can be established on **platforms or central points that control various devices and appliances** *(Gateway or Hub).* **Manufacturers can create dedicated apps or use existing ones** like Siri and Google Assistant to control their smart home products.
The structure of a smart home includes **five building blocks**: devices under control, sensors and actuators, network connectivity, home automation controller, and user interfaces.

The **architecture** of IoT-based smart home control systems can be divided in layers as follows:



IoT technology presents some uniqueness which cybersecurity specialists must consider:

- IoT systems can undergo **rapid changes** due to **interoperability** of devices, requiring continuous assessment;
- **Interconnected devices** bring new risks and device compromise;
- IoT devices themselves can be the **basis for attacks**;
- **Traditional cyber risk assessment process needs to be tailored** for IoT systems;
- IoT deployment is different from traditional IT;
- IoT environment deals with various connectivity models and **devices which may not support the CIA triad**;
- IoT devices **increase the attack surface**, and firmware updates, protocol updates, and applications further increase it.

Risk Assessment frameworks

Cybersecurity literature provides a **few popular RAP** (Risk Assessment Process) **frameworks** like **NIST, ISO/IEC, TARA and OCTAVE** to support the specialist in conducting **documented, objective and effective assessments**. Each of them presents unique aspects, like the nature of the approach and the methodology adopted to measure the risk. During the research on smart homes security, we investigated the characteristics of each RAP, its suitability to assess IoT risks, and previous examples of Cyber Risk studies for Smarthomes, **identifying OCTAVE Allegro as the most flexible and easily adaptable RAP for smart households**.

OCTAVE Allegro key principles are:

1. **Establishing objective risk measurement criteria**, specific for the organization's goals and agreed by all organization's members is a fundamental step in the assessment. Those criteria form the **foundation** to measure the extent to which the organization is impacted if a risk is realized;
2. Organization's information **assets must be mapped** and the **critical ones should be selected**. To concentrate available risk management resources **risk assessment should be performed only on those assets that are critical to accomplishing goals and achieving the organization's mission**;
3. All the places where those assets can be found (containers) should be mapped. **Threats to containers are inherited by the assets contained**;
4. Threats must be evaluated from a **strategic point of view** (who would exploit this vulnerability? How? Why? How likely?) and their **impact should be quantified** according to the previously agreed objective measurement criteria;
5. **Risk score = Impact severity * Probability**
6. Risks should be ranked according to their score. **Ranking determines the mitigation strategy**, concentrating available resources on the relevant ones.

Objectives

The scope of this assessment is to **propose a method to objectively score threats to Smart Homes** maintaining a **brand and technology agnostic** point of view. We will then try to deduct **general best practices** (mitigations) which can be applied and customised by any smart home enthusiast. Lastly, we will **qualitatively score the effectiveness** of proposed mitigations.

Compatibly with the resources available for this project, we do not commit to comprehensively analyse all threats to a smart home, but rather we will focus on their **main trends and categories**. We will provide a walkthrough of our assessment which our readers can follow through, **completing or replicating it according to their situation, needs and choices**. Our r**ecommendations should be tailored** to specific cases and **complemented with mitigations targeting the characteristics of their systems**.

Coongruently with the scope, we decided to base the assessment on the following **premises**:

Average European Household
The organization subject of our study will be an **average European household localised in Germany**, wich, using data from *Eurostat's 2021 surveys* we can imagine as follow:

- Composed by **2 adults**;
- Living in a **3.7 rooms** flat;
- Total **income 88744 €/year**;
- Spending 18.9% of income in housing costs;
- At least one of the members performs **Home Office** or occasionally works from home.

Smart Home specific
We will intentionally leave out the assessment threats which are not specifically related to IoT, like risks affecting any household equipped with WiFi or performing Home Office. Although considering those risks and mitigating them is the first fundamental factor for a safe smarthome, plenty of literature is available on the topic, and re-discussing them would fall outside of the **scope of our assessment, which is limited to Smart Homes security**.

Threat trends
Instead of analysing vulnerabilities for specific platforms or devices, we will **focus on the trends regarding IoT threats** and incidents, which applies to Smarthomes independently from their technology choices.

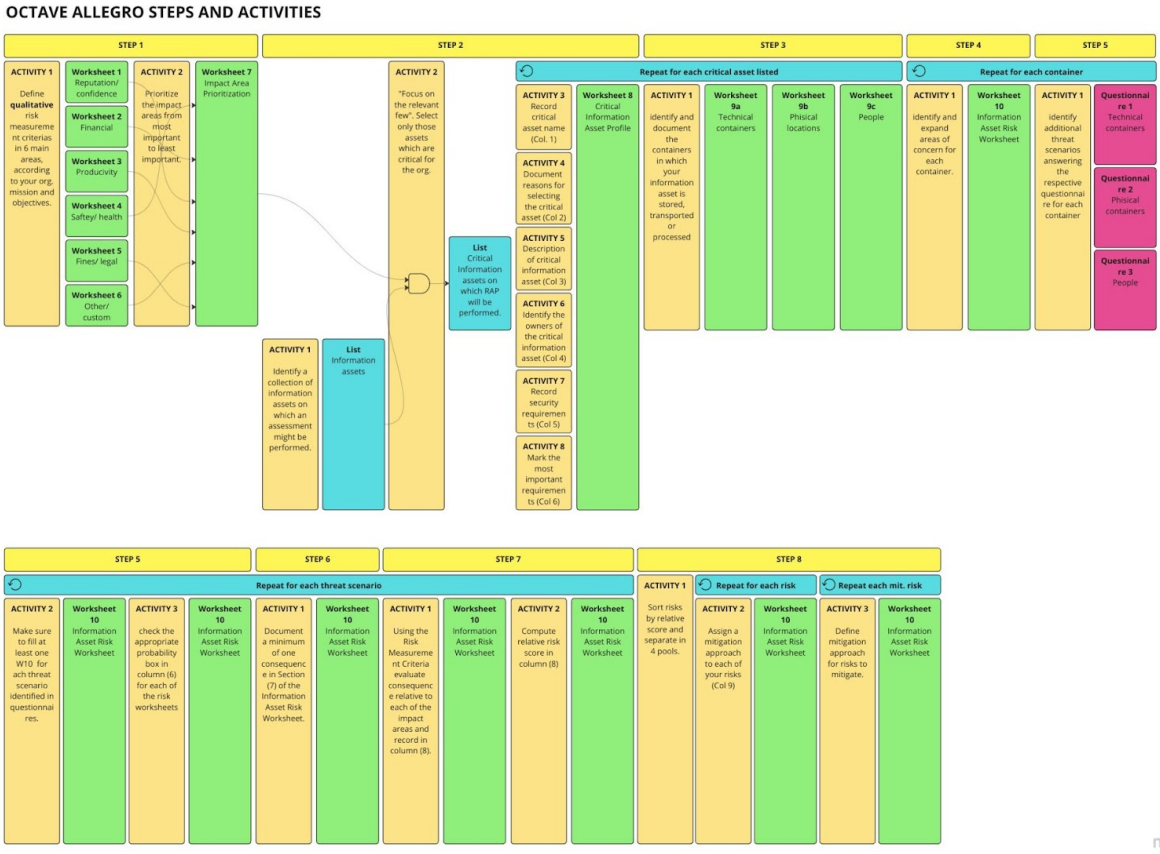
Strategic Threat Intelligence
We collected many different potential threats during our research on smart homes vulnerabilities. For the assessment, we considered the amount of **time and effort an actor should invest to exploit a vulnerability against the potential gain he can foresee**. Given the average position of our household, attackers definitely can't expect the same advantages they would get from breaching industrial or healthcare IoT systems.
Documented episodes suggest that Smart Homes are mostly targeted with **automated and simple attacks**. If many devices can be infected quickly and without excessive efforts, i.e. to spread **ransomware** or transform them into elements of a **botnet**, the law of big numbers makes the practice convenient. Advanced techniques would instead require investing a noticeable amount of time on a target which does not present specific attractivity.
At the same time, if an advanced threat actor or ATP decides to target a Smart Home, possibilities of successful defence with consumer grade equipment are very limited, while the **cost of deploying enterprise security solutions would outweigh the benefits** and the value of the protected assets.
This statement does not apply to any Smart Home. Households of politicians, entrepreneurs or other prominent figures may definitely appear more promising and give threat actors additional reasons to invest resources on exploiting it. **The enthusiast who prepares to replicate our assessment should review our threat intelligence according to its specific conditions.**

Octave Allegro assessment

The OCTAVE Allegro methodology is focused on creating strength in results, allowing for **exhaustive risk assessment and concentrating on data protection**, helping to find out various security vulnerabilities of IoT-based smart homes, present the risks to home inhabitants, and propose approaches to mitigate the identified risks.
OCTAVE **involves eight steps that are organised into four levels**. **Worksheets** are provided by the methodology to capture outputs from each step in the risk evaluation and use them to input into the following step, which enables continuous awareness throughout the process and makes it easier to explore problematic situations.

OCTAVE considers four levels as follows:

1. **Establish drivers phase**: This phase develops criteria for measuring risk which is the foundation for risk assessment
2. **Profile assets phase**: This phase establishes limits for assets and identifies security requirements
3. **Identify threats phase**: This phase identifies security threats from the assets where the information asset is stored, transported, or processed
4. **Risk mitigation phase**: This phase determines and executes a risk mitigation strategy for the identified assets.



In this chapter we describe the execution of each assessment phase.

Establish drivers phase

Background and definitions:

- **Impact** – The effect of a threat on an organization's mission and business objectives.
- **Impact value** – a qualitative measure of a specific risk's impact to the organization (high, medium, or low).
- **Risk measurement criteria** – a set of qualitative measures against which the effect of each risk on an organization's mission and business objectives is evaluated. Risk measurement criteria define ranges of high, medium, and low impacts for an organization.

Step 1 Activities 1 - 2

The first step of the methodology is establishing the drivers that will be used to evaluate the effect of a risk on your organization's mission and business objectives. These drivers are reflected in a **set of risk measurement criteria that will be developed**. Those criteria form the **foundation** to measure the extent to which the organization is impacted if a risk is realized.

It is important to create a consistent set of risk measurement criteria that can be used for all information assets, focused at an organisational level, and reflecting management's awareness of the risk. This ensures that decisions about how to mitigate risk will be consistent across multiple assets and units.

To create a set of risk measurement criteria, **OCTAVE identifies a range of impact areas that are important and unique to the organization**. These impact areas can include health and safety of customers and employees, financial, reputation, and laws and regulations.

The second activity in this phase is **prioritising the impact areas** from most important to least important, using the Impact Area Ranking Worksheet (Worksheet 7, Appendix B). The most important category should receive the highest score and the least important the lowest.

- ➢ Worksheets 1 to 7 support this phase, and are collected with our comments in Appendix 1.

Profile assets phase

Background and definitions:

- **Asset** – An asset is something of value to the enterprise. Assets are used by organizations to achieve goals, provide a return on investment, and generate revenue.

- **Critical information asset** – Critical information assets are the most important assets to an organization. The organization will suffer an adverse impact if
    - a critical asset is disclosed to unauthorized people
    - a critical asset is modified without authorization
    - a critical asset is lost or destroyed
    - access to a critical asset is interrupted
- **Information asset** – An information asset can be described as information or data that is of value to the organization, including such information as patient records, intellectual property, or customer information. These assets can exist in physical form or electronically (stored on databases, in files, on personal computers).
- **Information asset profile** – A representation of an information asset describing its unique features, qualities, characteristics, and value.
- **Information asset owners** – Owners of information assets are those individuals who have primary responsibility for the viability, survivability, and resiliency of an information asset.
- **Information asset custodians** – Custodians of information assets refers to the individuals in the organization who have the responsibility to protect information assets that are stored, transported, or processed in containers.
- **People** – In the structured risk assessment, people are a type of container for information assets. They may possess specialized or important information and use it in their jobs, such as intellectual property.
- **Security requirements** – The requirements that characterize how an information asset is to be protected. These are also often referred to as “security objectives.”
    - Confidentiality – Ensuring that only authorized people (or systems) have access to an information asset.
    - Integrity – Ensuring that an information asset remains in the condition that was intended by the owner and for the purposes intended by the owner.
    - Availability – Ensuring that the information asset remains accessible to authorized users.
- **Technology assets** – Technology assets typically describe electronic containers in which information assets are stored, transported, or processed. These assets generally include hardware, software, application systems, servers, and networks.
- **Information asset container** – An information asset container is where information assets are stored, transported, or processed. It is a place where an information asset “lives.” Containers generally include hardware, software, application systems, servers, and networks (technology assets), but they can also include items such as file folders (where information is stored in written form) or people (who may carry around important information such as intellectual property). They can also be both internal and external to an organization.

Step 2 Activities 1 - 8

In this phase the **focus is on identifying and defining the organization's information assets**. This includes identifying the **containers and custodians** of those assets **to determine vulnerabilities**.

A profile is created for each asset, which includes its boundaries, security requirements, and possibly a quantitative value. Information asset profiling is important for consistency and ensuring that assets are adequately defined and secured. **The profile will form the basis for identifying threats and risks in subsequent steps**

The **first activity in Step 2** involves **identifying a collection of information assets on which an assessment might be performed**. The assessment provides the most utility when it is focused on the information assets that are most important to the organization.

Considering the following questions we conducted a brainstorm to **list the assets that are important to our household** and on which and on which a structured risk assessment might be performed**:**

- What information assets are of most value to your organization?
- What information assets are used in day-to-day work processes and operations?
- What information assets, if lost, would significantly disrupt your organization's ability to accomplish its goals and contribute to achieving the organization's mission?
- What other assets are closely related to these assets?

"Focusing on the critical few" is an essential risk management principle. Structured **risk assessment should be performed only on those assets that are critical to accomplishing goals and achieving the organization's mission**, as well as those that are important because of such factors as **regulatory compliance**.

For each item in the list created during the brainstorming session, we considered the following question:

- Which assets on list, if compromised, would have an adverse impact on the organization (as defined by your risk evaluation criteria) if one or more of the following occurred?
    - The asset or assets were disclosed to unauthorized people.
    - The asset or assets were modified without authorization.
    - The asset or assets were lost or destroyed.
    - Access to the asset or assets was interrupted.

Assets that meet one or more of these criteria are considered critical and should have a structured risk assessment performed on them. For time constraints we limited our selection to the most critical ones, which will be analysed in our example.

ASSETS AND CRITICAL ASSETS (in red):

- Banking and payment credentials and codes
- Personal accounts credentials
- Internet connection responsibility / ownership
- Network performances
- Work/company/customers accounts credentials (may be critical for freelancers, less for employees)

- Work/company/customers sensible data
- Privacy
- Smart Home appliances and IoT devices efficiency
- Private properties
- PII household members (medical files etc...)
- “Kids well-being” (exposing kids to information which doesn't suit their age, abusing their ingenuity...)
- Important files (work related, documents, memories…)

The next activities in step 2 (3-8) are about gathering information on each critical asset, necessary to begin the assessment process.

➢ Worksheet 8 supports those activities and are collected in Appendix 2.

Step 3 Activity 1

Places **where an information asset is stored, transported, or processed can be points of vulnerability and threats, but they are also places where controls can be implemented to protect the information asset**.

Containers, which can be physical, people or technical, must be considered when profiling risks to the information asset, and controls must be implemented at the container level to protect the information asset. **Any vulnerabilities or threats to the containers in which the information asset lives are inherited by the asset. Identifying containers is essential to identifying risks to the information asset** in an information security risk assessment. Information assets can reside in containers that are not in the direct control of the organization, such as those managed by service providers, and must be identified to gain an adequate risk profile of the information asset.

Worksheet 9 (**Information Asset Risk Environment Map)** is used to identify and document the containers. **Whenever possible, the owner of the container should be documented.** The owner of the container often takes custody of the asset.

➢ Worksheets 9 support this phase, collected in Appendix 3.

Identify threats phase

Background and definitions:

- **Area of Concern** – A descriptive statement that details a real-world condition or situation that could affect an information asset in your organization.
- **Threat** – A threat is an indication of a potential undesirable event. A threat refers to a situation (or scenario) in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization’s email server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization’s

information technology hardware). A threat is created when a threat actor exploits a vulnerability.

- **Threat scenario** – A threat scenario is a situation in which an information asset can be compromised. It generally consists of an actor, a motive, a means (access), and an undesired outcome. Threat scenarios are simplified ways to determine if a risk exists that could affect your information asset.
- **Threat trees** – A tree structure used to visually represent a range of threat scenarios. Threat trees help you to ensure that you consider a broad range of potential threats to your information asset as the basis for determining risk.

Step 4 Activity 1

In Step 4 the focus is on **addressing the threat component of the risk equation**. Risk is the combination of a threat and the resulting impact of the threat if acted upon. The goal of this step is to brainstorm **possible conditions or situations that can threaten the information asset, which are referred to as areas of concern**. These areas of concern may represent unique threats to the organization and its operating conditions. The purpose is **not to capture a complete list of all possible threat scenarios but to quickly capture those situations that come to mind** that could affect the asset and record them. When developing these scenarios, it is important to consider the various actors, motives, and outcomes inherent in the area of concern, be specific, and keep in mind the security requirements set for the information asset and how they might be compromised due to a threat.

To perform this activity, we will use the Information **Asset Risk Environment Maps for reference** and **fill the Information Asset Risk Worksheets (Worksheet 10)** to record the areas of concern.

The following steps help identify areas of concern:

1. Using the Information Asset Risk Environment Maps, r**eview each of the containers listed to seed a discussion** about potential areas of concern.
2. **Document each area of concern** on an Information Asset Risk Worksheet. On the worksheet, record the name of the information asset and document the area of concern in as much detail as possible. **Complete the columns labelled “Information Asset” and “Area of Concern”** on the worksheet and **remember to use a separate worksheet for each area of concern** that you identify.
3. **Expand your areas of concern to create threat scenarios.** A threat scenario is a more detailed expression of the properties of a threat. For each area of concern recorded on an Information Asset Risk Worksheet, **complete columns (1) through (4) by recording the actor, means, motive, and outcome.** If some of those fields can't be filled,leave them blank.
4. In **column (5) document how this threat would affect the security requirements that have been set for the information asset.**

5. **Proceed through each of the containers listed** on the Information Asset Risk Environment Maps and document as many areas of concern as possible. **A single container may result in the identification of one or more areas of concern**.

Each worksheet 10 will uniquely capture a single risk, several of these worksheets will be completed throughout the risk assessment.

Step 5 Activity 1 - 2

In this step, **areas of concern are expanded into threat scenarios that further detail the properties of a threat**. To expand areas of concern into threat scenarios, we must first understand the **basic components of a threat**. A threat has the following properties:

- **Asset** – something of value to the enterprise
- **Access/means** – how the asset is accessed by an actor (technical means, physical access, social engineering). Access applies only to human actors.
- **Actor** – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- **Motive** – the intent of an actor (e.g., deliberate or accidental). Motive applies only to human actors.
- **Outcome** – the immediate result (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset.

➢ The excellent *Threat Mind Map* (Appendix 5) released by ENISA helped us during those steps, although OCTAVE released standardised questionnaires.

Step 5 Activity 3

Probability is optional in OCTAVE, but if used it should be estimated for every risk profile. Probability helps to determine which of the scenarios are more likely given the organization unique operating contexts. This will be useful later in determining how to prioritise your risk mitigation activities.

Because it is often very difficult to accurately quantify probability (especially with respect to security vulnerabilities and events), probability is expressed in this risk assessment qualitatively as **high, medium, or low** in the probability box in column (6**)** for each of the risk worksheets that were created.

Mitigate risks phase

Background and definitions:

- **Impact statement** – A descriptive statement that details how the organization is impacted when a threat scenario is realized. The impact statement is the consequence of the realization of a threat scenario.
- **Risk** – A risk is the possibility of suffering harm or loss. Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence. A risk is composed of
    - an event,
    - a consequence, and
    - Uncertainty
- **Impact value** – A qualitative value assigned to describe the extent of impact to an organization when a threat scenario and resulting impact is realized. The impact value is derived from the risk measurement criteria.
- **Mitigation approach** – The way that an organization intends to address a risk. An organization has the following options: accept, mitigate, or defer.
    - **Accept** – A decision made during risk analysis to take no action to address a risk and to accept the stated consequences. Risks that are accepted should have little to low impact on the organization.
    - **Mitigate** – A decision made during risk analysis to address a risk by developing and implementing controls to counter the underlying threat or to minimize the resulting impact, or both. Risks that are mitigated are those that typically have a medium to high impact on an organization.
    - **Defer** – A situation where a risk is neither accepted nor mitigated based on the organization's desire to gather additional information and perform additional analysis. Deferred risks are monitored and re-evaluated at some point in the future. Risks that are deferred are generally not an imminent threat to the organization nor would they significantly impact the organization if realized.
- **Residual risk** – Residual risk is the risk that remains when a mitigation approach has been developed and implemented for the range of risks that affect an information asset. Residual risk that remains must be acceptable to the organization.

Step 6 Activity 1

In this activity, we **determine how the threat scenario recorded on each Information Asset Risk Worksheet could impact the household.**

1. For each threat scenario documented on an Information Asset Risk Worksheet, determine how the organization would be impacted if this threat scenario was realized. This is the consequence of the threat and completes the risk equation.
2. **Document a minimum of one consequence in Section (7) of the Information Asset Risk Worksheet.** Additional consequences can be documented as necessary,

as specifically as possible and considering the impact areas of the risk evaluation criteria and the “outcome” noted in Step 5.

Step 7 Activity 1 & 2

In Step 7, **we qualitatively measure the extent to which the organization is impacted by a threat computing a relative risk score for each risk**. The score is derived by **considering the extent to which the consequence of a risk affects the organization as compared to the relative importance of the impact areas established in step 1**. By using these criteria, we ensure that **risks are scored in the context of the organisational drivers**. These activities **must be performed for each Information Asset Risk Worksheet**.

Activity 1 begins **by reviewing the Risk Measurement Criteria** created in Step 1. Using the Criteria as a guide, **evaluate the impacts of consequence statements** (or statements) relative to each of the impact areas, and **record a value of “high,” “medium,” or “low”** in the “Value” area of Worksheet 10 column 8.

In Activity 2 **a relative risk score will be computed. Perform this step in the “Score” area of column (8) on each of the Information Asset Risk Worksheets**.

1. **Compute the score** for each impact area **by multiplying the impact area rank by the impact value.** (Refer to the Impact Area Ranking, Worksheet 7) Record the result in the “score” column. Impact values are assigned quantitative values as follows: **High – 3, Medium – 2, and Low – 1.** Keep these values consistent throughout the risk worksheets.
2. **Multiply the sum of impact values in the different areas by the probability**, using the same scale (High – 3, Medium – 2, and Low – 1). **This value is the total relative risk score.**

The scores generated in this activity **are only meant to be used as a prioritisation tool. Differences between risk scores are not considered to be quantitative.**

Step 8 Activity 1 - 3

In Step 8, we **prioritise and mitigate risks by considering organisational factors and developing a strategy based on asset value and location.**

When deciding whether to accept, reduce, or delay a risk, **we need to consider many factors**, like how important the asset is and how likely the risk is. If a risk could really harm the organization but it's unlikely to happen, we may not want to reduce it. However, **there's no one right way to decide which risks to reduce.** Usually, it's a decision made by the people involved in the risk assessment and their knowledge of the organization.

Containers often hold multiple assets with varying security requirements. In this case the information asset with the most extensive security requirements rules the security requirements applied to the container.

To mitigate risk appropriately, we must consider a **balanced approach**.

- **Avoiding risks** by implementing appropriate controls to prevent threats and vulnerabilities from being exploited.
- **Limiting risk** by implementing strategies that contain the adverse impact on the organization if a risk is realized.

In most cases, it is appropriate that mitigation strategies **address both avoiding and limiting risk**. However, it is also important to **consider the cost** of mitigation strategies. **The cost of avoiding and limiting risk must be commensurate with the value of the asset being protected and the potential impact on the organization i**f the asset is compromised.

N**ot all risk can be eliminated.** Mitigation strategies may result in **residual risk**, which can be accepted or further mitigated.

In Activity 1 & 2 **risks are sorted according to their relative scores** and a **mitigation approach is assigned to each of them.** As a rule of thumb, Worksheets 10 separated into 4 pools containing a similar number of risks.Pool 1 with the highest scores should be Mitigated, pool 2 mitigated or deferred, pool 3 deferred or accepted and pool 4 accepted, but the final decision must consider the organization's unique operating circumstances. **Any risks that could have serious consequences on the organization should not be accepted.**

In Activity 3 a mitigation strategy is developed for all of the risk profiles requiring mitigation.

1. **Note the container** in which the control will be implemented. (These containers can be found on the Information Asset Risk Environment Maps.)
2. **Describe the control** to be implemented **and any residual risk** to the asset once the control is implemented.

➢ Appendix 4 collects the Worksheets 10 we compiled and the selected mitigations. As we concentrated our study on a few most critical assets, we decided to apply mitigations to all of them. For risks that could not be completely eliminated we computed the residual risk score.

Outcomes

We analysed 5 critical assets:

- Personal account credentials;
- Banking credentials;
- Archived files;
- Smart home efficiency;
- Internet connection responsibility.

A total of **16 risks were documented**, leading to a cumulative relative score of 1097.

After mitigation we documented **5 residual risks**, with a cumulative score of 137.

In this chapter we present the mitigations strategies selected grouped by the containers they apply to.

Network

Network segmentation

Connecting **smart and personal devices to the same network exposes the household to huge security risks**, besides easily overloading the home router connecting an excessive number of clients and compromising its functioning.
The problem is easily solved using a **cascade router,** which connects to the main one for internet access and deploys a second WiFi network exclusively used for IoT devices. Once Home and IoT network segments are created, this **router's firewall can be configured to only expose the needed services to the home network, and allow only strictly required traffic from IoT to Home network**. Cost of the mitigation can be contained utilising an old router, as most IoT devices still function with 2.4GHz WiFi and no DSL interface is required.

Selective internet access for Smart Devices

The cascade router's firewall should also be configured to **prevent IoT devices from connecting to the internet**, except for the ones which rely on cloud services for control, the home gateway which needs to receive user inputs, and occasionally for updating devices firmware or their first configuration. **This prevents a hijacked device from being able to communicate with malicious C2C servers, taking part in botnets or exfiltrating data**.

IoT WiFi Clients Isolation

Most routers can **isolate WiFi clients by blocking network discovery and cross-talking**. Normal smart home devices only need to communicate with the home gateway, which is also in charge of proxying commands from the endpoints. By connecting the gateway to a LAN port of the cascade router,we can apply client isolation to **prevent malwares from spreading** and **limit network reconnaissance** attempts.

Network mapping, clients identification and traffic monitoring

Assuming the good habit of regularly checking which clients connect to our networks and the volume / type of traffic generated allows us to **quickly detect anomalies and unidentified new devices**.

HTTPS

Deploying HTTPS can be complicated for an entry level user, but the market is evolving and many new products provide simple and guided procedures to issue certificates and enable HTTPS web interfaces. This should be preferred over HTTP whenever possible, as it **prevents eavesdropping of administrative credentials** and other sensitive information.

Tunnels/VPN instead of open ports

Being able to reach the Home Gateway or other Smart Home services from the internet is often required to control the smart home from the internet. Some gateways use cloud services and webhooks to achieve this safely, while others require the user to deploy its solution autonomously. The most diffused practice of **forwarding an open port on our home router to the gateway makes it discoverable by anyone on the internet**, including crawlers and malicious actors.
This solution exposes the gateway to various types of attacks and we recommend avoiding it. **VPNs or services like Cloudflare tunnels allow remote access to the gateway without exposing it to the internet**, a much safer alternative. Cloudflare in addition is also a WAF, which can filter traffic according to custom rules even before it reaches our network.

- ➔ The websites shodan.io and its Chinese counterpart en.fofa.info continuously scan the internet looking for exposed services and devices. They can give you precious insights about how your smart household looks from the internet (The less you appear, the better).

WAF / Firewall IP bans

Gateways and WAF like Cloudflare can keep track of the amount of requests and login attempts generated by every client. A rule which automatically blocks a source IP address after too many failed login attempts (**IP bans**) or too many requests sent in a short amount of time (**rate-based rules**) helps **prevent brute force and dictionary attacks to our login pages**.

- ➔ Cloudflare
- ➔ Wireguard, an user-friendly VPN tunnel supported by new domestic routers.

Smart Home system

Investigate reviews of smart devices before purchase, look for vendor reputation, platform compatibility, design faults, user complaints, security incidents and service terms (privacy, data collection, cloud servers location…)

The Smart home IoT market is really huge and constantly evolving, products with similar functions may differ in price, brand, compatible gateways, control protocols, brand, hardware quality, failsafe design and other factors. **We recommend research on those key points before selecting a brand or device**, especially when purchasing low cost devices which may come with limited compatibility, design flaws, unlawfully terms and conditions and security vulnerabilities.

Carefully plan ahead on which gateway type and brand to build your system

The **Home Hub will be the hearth of the smart home and will dictate any further addition to the system**. For those reasons it is vital to select the solution which better meets the household needs and favours and ensures the maximum compatibility. Discussing every solution available would quickly become a time consuming tasks, but we can identify **three categories in the market**:

- **Commercial consumer Hubs** (i.e. *Google Home, Amazon Alexa* and *Apple*) are cheap, easy to configure and only works with the vendor's cloud services and apps. Simplicity and cheapness come with a trade off on customizability, advanced functions, compatibility and control over personal data.
- **Open Source Hubs** (i.e. *Home Assistant* and *OpenHAB*) are cheap or free, offer the maximum compatibility and can be customised in every aspect, but requires IT skills or the passion for learning them;
- **Professional Hi-End Hubs** (i.e. *JoshAI* or *BTCINO MHSERVERKIT*) combines all the advantages, but are much more expensive and are normally distributed by installation companies which take care of set-up and configurations.

There is not a best or worst solution, every household should make an informed decision according to factors like budget, privacy and customizability concerns, and available IT skills.

Local network controlled smart devices (Matter, Zigbee, ESP-Home…)

Another important factor in smart devices selection is the control protocol they use. The various solutions available can be distinguished in **two categories**:

- **Cloud controlled devices** (i.e. *Tuya*) those are usually the cheapest devices and introduces huge issues: They can't function without an active internet connection and they lock the customer to install a vendor's specific app. This makes it impossible to block internet access for the devices, and often result in the need of installing a multitude of apps to control each specific brand. **We recommend avoiding those products**, unless being ready to venture in jailbreaking procedures where tools like *Tuya-Cloudcutter* are used to overwrite their original firmware, freeing the devices from the vendor's cloud and obtaining control on them;

- **Local control devices** (i.e. Matter, Zigbee, ESP-Home…) those devices require an active internet connection only on rare occasions, like the first configuration. They are safer, put the user in control, and continue functioning even in case of Internet connection failure.

Follow best practices and configure devices properly since the beginning

In many cases, enthusiasts start experimenting with a limited number of devices and a simple system, which is later expanded over time. **Even during the first steps, it is important to configure the devices safely, securing them with strong passwords and connecting them to the proper network**. Failure to do so may result in forgotten bad configurations, which will represent a vulnerability when the system is scaled up. Reconfiguring the system mid-way can become a time consuming and tedious task, so we highly recommend following a safe approach from the beginning.

Software updates

Firmwares and softwares updates are released frequently to address new vulnerabilities and improve the devices security. We recommend **making system backups and updating as quickly as possible everytime a new version is released**. The backups will help us revert the system to the previous state in case the update goes wrong or breaks important functions.

Automations and hardware controls to manage critical devices if user input becomes unavailable

We will face occasions where our system can't receive user inputs or communicate with the internet, i.e. in case of a network failure. Having a **backup strategy for those situations** is fundamental, in example:

- Always preserve mechanical switches or control methods, at least for critical devices.
- Program automations to switch off lights and heating when the home is empty, so you won't have to worry about energy wastes if remote control becomes unavailable due to internet failure or similar events.

Have physical switches, privacy positions, and covers to hard-disable cameras and microphones when not in use

Not only cameras and voice assistants can capture video and sound from the surrounding environments. Appliances like robot-vacuum and similar may use computer vision systems to navigate the space or identify objects and obstacles. Plenty of documented incidents demonstrates the **unreliability of software switches**, those devices may always record even when they appear to be disabled. Instead of relying on easily hijackable softwares, we recommend using **physical switches, hard covers and other mechanical methods to make it impossible for the devices to capture any sound or image when not needed**.

Critical Smart Devices check routine

Devices like door locks and thermostats are critical for their functions and for energy saving. We recommend **periodically checking their health, battery levels, their configurations and testing that everything works as expected.** This will help identify issues before they grow into actual problems.

Smart Devices low battery notifications

Battery operated devices may become unusable if the battery level falls too low. Some, like thermostats, can fail in open valve position, leading to huge energy waste. To avoid this make sure to **configure and receive notifications when the batteries need replacement**.

Regularly review logs to spot errors, misconfigurations or suspect activities

Regularly checking devices and hub logs looking for errors, failures, misconfiguration and suspect activities is a good practice and enables quick resolution of problems or investigation of threats.

Periodically assess and review the system configuration

Periodic review of configuration helps to **identify errors or spot misconfigured devices which may accumulate with time** due to system expansions and modifications. It is also a good occasion to refresh and improve the system to improve it and keep it updated.

Collect feedback from household members to improve user experience

When administering a Smart Home system, it is important to **hear the needs and preferences of every household member.** Receiving **feedback from the users will help you achieve better efficiency, prevent their mistakes, and acknowledge issues** much faster.

Accounts and credentials

Individual accounts

Provide **each household member a personal account** to interact with the system, and give each account **only the privileges it needs**. This allows to relate actions in the system to the user who initiated them, and it makes it much simpler to reset or block the account if compromised.

Strong passwords

Choose a **good password manager and generator,** use it to generate **long random passwords unique for every account and device**. Password reuse must be avoided. This practice will make brute force and dictionary attacks innocuous, and will limit lateral movement of threat actors if an account is compromised.

- ➔ Websites like passwordmonster.com can be used to estimate the time required to brute force your password.

2FA AND OTP

Always **enable Two-Factor Authentication for user accounts and to access administrative interfaces**.

Bank accounts activity notifications

Enable **notifications for activities on your bank accounts, payment cards and payment services** (i.e. Paypal or crypto wallets) to immediately acknowledge suspect or unrecognised operations.

File Archives

Map file archive locations

Over time, important files may accumulate in different devices and hard drives, making it very difficult to keep track of their location and protect them. **A clear definition of where and which files are archived will help you secure those locations**.

Cloud backups & Offline backups

Backing up relevant files in a **cloud service is a good way to transfer the risks** associated with their custody, while backing up files into **Hard Drives that will be disconnected from the system when not in use adds a second layer of redundancy**. The two practices should be **combined to mutually mitigate each other's vulnerabilities**, granting the maximum security.

Endpoints

Control mobile apps permissions, zero-trust model

Smart phones contain a lot of sensitive data. When installing new apps, especially from unknown or untrusted vendors, be sure to **grant the minimum necessary permissions** to operate.

AV solutions

Installing **Antivirus solutions** on personal devices and Home servers ensures protection against known malwares.

- ➔ ClamAV is an open source multiplatform antivirus developed by Cisco Talos, one of the biggest cybersecurity solutions providers.

Secure mail clients

Modern mail clients like GMail **recognize and block most of phishing attempts and malicious attachments** even before they reach our inbox.

People and strategic

Check terms and agreements from cloud service providers

When deciding to use a cloud provider for file storage, home control or other services, be sure to **check and understand its usage terms and conditions** first. Remember that most providers can change those agreements at their will. Consider the effort and issues which you may face in case those terms are changed in a way that you cannot accept, forcing you to leave the service.

- ➔ The website tosdr.org monitors and presents a simplified form of the Terms and Conditions of most popular services, highlighting good and negative clauses.

Household members awareness training

Different sources report that **80% to 95% of cybersecurity incidents are originated by human mistakes**. There is little you can do to keep your home safe if you miss to address this factor by diffusing **awareness and training the other household members**.

Incident response plan

Even the best security measures cannot completely eradicate risks. In the case one of the threats realises, you should **always have a response plan ready.** This may include a backup method to enter your home, a neighbour who can step in if you are travelling and the heating switches on without reason, spare parts to quickly replace compromised devices and many more. **Imagining in advance what you would do in case of an incident will help you to be ready and act tempestively**.

Conclusions

OCTAVE Allegro has proven to be an agile and flexible method that **can be adapted to the study of a smart home** and can be **executed in relative simplicity and with limited resources**.
Even if we had to stretch a few definitions to apply them to our subject, this is permitted and provided for by the framework itself.

Th**e cumulative relative risk score** of our average household went from 1097 prior to mitigations to 137 in residual risks. Although those scores are qualitative and OCTAVE recommends to not consider the numbers relevant, a **reduction of 88%** definitely indicates some effectiveness of the proposed mitigations.

We demonstrated that, despite the wide, various and constantly changing IoT market represents a challenge to securing and trusting smart devices, **generic controls and mitigations can be implemented in other containers and to our smart home infrastructure**, preventing and mitigating the consequences of an incident involving IoT technologies.

Finally, we hope we have provided our readers with a useful **starting point for approaching cyber risk assessment and protecting their smart homes effectively and rationally.** OCTAVE Allegro involves frequent revisions and expansion of the assessment, which readers will be able to develop on their own **by repeating the illustrated process**, **objectively assessing the extent of the threats they are exposed to, and their possible consequences.**

Appendix 1: Worksheets 1 to 7

Allegro Worksheet 1	**Risk Measurement Criteria – Reputation and Customer Confidence**		
Impact Area	**Low**	**Moderate**	**High**
Reputation (Neighbors…)	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Workplace (relation with employers and colleagues of household members)	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Privacy	Privacy is minimally breached, no tangible consequences. (i.e. data collection for marketing…), little or no effort or expense is required to recover.	Privacy is breached, consequences are possible, some effort or expense is required to recover.	Privacy is irrevocably breached, with consequences.

For a commercial organisation this impact area represents relationships with employees, customers and other entities. For our household we adapted the definition to cover relationships with Neighbors, Employers and colleagues and privacy.

Allegro Worksheet 2	**Risk Measurement Criteria – Financial**		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs (utility bills etc…)	Increase of less than 10% in yearly operating costs	Yearly operating costs increase by 10 to 20%.	Yearly operating costs increase by more than 20%.
Revenue - income (Ability of household members to earn money)	Loss of less than 2.5% in yearly net income.	Loss of less than 5% in yearly net income.	Loss of more than 5% in yearly net income.
One-Time Year Financial Loss (Costs for damages, repairings….)	One-time financial cost of less than 2180€ (2.5% income)	One-time financial cost of 2180€ to 4372.2€ (5% income)	One-time financial cost greater than 4372.2€

Similarly to commercial organisations, our household experiences financial risk in relation to its income.

Allegro Worksheet 3	**RISK MEASUREMENT CRITERIA – PRODUCTIVITY**		
Impact Area	**Low**	**Moderate**	**High**
Essential domestic activities (cooking, washing, heating…)	regular activities are disturbed but can be carried out anyway and without delays.	Regular activities become more complicated. Activities require additional effort and time.	Regular activities are interrupted and can't be carried out.
Home office:	Office activities are disturbed but not compromised, the solution takes less than 5 minutes.	Office activities become more complicated. Activities require additional effort and time. Solution requires between 5 and 30 min.	Office activities are interrupted and can't be carried out. Solution takes more than 30 min.
Non essential activities and entertainment.	regular activities are disturbed	activities are interrupted and can't be carried out, the problem lasts one day or less.	activities are interrupted and can't be carried out, the problem lasts more than one day.

Productivity of our smart home refers to the essential and non-essential functions it should provide to its inhabitants.

Allegro Worksheet 4	**Risk Measurement Criteria – Safety and Health**		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to household members' lives.	Household members' lives are threatened, but they will recover after receiving medical treatment.	Household members' death.
Health	Minimal, immediately treatable degradation in household members' health with recovery within three days.	Temporary or recoverable impairment of household members' health.	Permanent impairment of significant aspects of household members' health.
Safety	Safety questioned.	Safety affected.	Safety violated.
Wellbeing:	Wellbeing questioned.	Wellbeing affected.	Wellbeing violated.

This area applies to households and their members in close similarity with commercial organisations.

Allegro Worksheet 5	**Risk Measurement Criteria – Fines and Legal Penalties**		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than 2186,1 € (2.5% DE avg. household income) are levied.	Fines between 2186,1 € to 4372.2€ (5% income) are levied.	Fines greater than 4372.2€ are levied.
Lawsuits	Frivolous lawsuits filed against the household members, requiring little or no attention, efforts and expenses.	Non-frivolous lawsuits are filed against the organization. Require attention, effort and expenses below 4372.2€ (5% income).	Non-frivolous lawsuits are filed against the organization. Requires attention, effort and expense and may have serious consequences.
Investigations	No reasons for queries from government or other investigative organizations	Government or other investigative organization may request information or records (low profile).	Government or other investigative organization initiates an investigation into household practices.

This area applies to households and their members in close similarity with commercial organisations, although our household has much lower risk thresholds.

Allegro Worksheet 6	**RISK MEASUREMENT CRITERIA – SMART HOME / IOT**		
Impact Area	**Low**	**Moderate**	**High**
Functionality and usability	No disruption or minimal temporary disruption solving autonomously once the cause is removed. Controls are easily accessed.	Temporary disruption of specific devices or requiring less than 2 hours to restore. Control requires complicated procedures preventing usage of all members.	Disruption of the vast majority of devices functionalities, or requiring more than 2 h to recover, or expenses.
Efficiency	Devices functioning at their optimal efficiency and helping energy saving.	Devices efficiency compromised, invalidating energy saving advantages.	Devices become so inefficient that they increase the energy requirements for the household instead of reducing it.
Devices health	No threats to devices hardware and software	Device is compromised but can be repaired.	Device replacement is the only solution.

We introduced the smart home impact area as a custom category to add emphasis to risks impacting the smart devices.

Allegro Worksheet 7	**IMPACT AREA PRIORITIZATION WORKSHEET**
PRIORITY	**IMPACT AREAS**
6	**Safety and Health**
5	**Financial**
4	**Reputation and Confidence**
3	**Productivity**
2	**Smart Home / IoT**
1	**Fines and Legal Penalties**

Appendix 2: Worksheets 8

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?*
Personal Accounts credentials	This asset is critical because it allows access and use of accounts like Social networks, emails etc.	The assets consist of username and password pairs, sometimes combined with OTP codes.
(4) Owner(s) *Who owns this information asset?*		
Owner of the accounts are owners of access credentials		
(5) Security Requirements *What are the security requirements for this information asset?*		
☐ **Confidentiality**	Only account owners should know the access credentials.	
☐ **Integrity**	Only account owners should modify the access credentials. Service providers may be able to reset them in exceptional situations.	
☐ **Availability**	This asset should be available for accessing emails and other accounts.	
	This asset must be available for _8___ hours, ___7__ days/week, __365___ weeks/year minimum.	Unavailability can have critical consequences if it is longer than a few hours.
☐ **Other**		
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
☑ Confidentiality	☐ Integrity	☐ Availability ☐ Other

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?*
Archived Files	The asset is critical for bureaucratic reasons. If destroyed it can hardly be recovered. It contains sensitive and personal data of household members.	The asset consists in digital copies of contracts, health records, pictures and other medias, legal acts and other relevant documents

(4) Owner(s) *Each household member is the owner of its accounts, except for those in the name of kids which are managed by parents.*
File owner / File archives admin

(5) Security Requirements *What are the security requirements for this information asset?*		
☐ **Confidentiality**	Only authorized personnel can view this information asset.	**Secret to everybody except the owner and authorized household members.**
☐ **Integrity**	Only authorized personnel can modify this information asset, as follows:	**Only owners of files are authorized to modify.**
☐ **Availability**	This asset must be available for these personnel, as follows:	Asset is not accessed regularly, but needs to be available anytime circumstances require it.
	This asset must be available for _8___ hours, ___7__ days/week, __365___ weeks/year.	Interruptions under 2 days can be handled.
☐ **Other**		

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
☐ Confidentiality	☑ Integrity	☐ Availability	☐ Other

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?*
Banking details	This asset is critical for the household as it allows operations on member's bank accounts.	Bank information are credit card numbers, CVV, authorization codes, Web-banking logins, OTP generators.

(4) Owner(s) *Each household member is the owner of its accounts, except for those in the name of kids which are managed by parents.*
Banking account owner

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset.	**Secret to everybody except the owner.**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	**Only owners and bank institutes are authorized to modify the info.**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Bank info must be available to owners to purchase necessary items and pay bills, ensuring supplies to households.
	This asset must be available for _8___ hours, ___7__ days/week, __365___ weeks/year.	Short interruptions, under 2 days, can be handled.
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Owners are responsible towards banks for correct custody of their bank accounts.

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
☑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

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?*
Internet connection	This asset is critical as it ensures internet connectivity in the household. The network owner is responsible for actions carried out through it.	The asset consists of connection bandwidth, public IP and MAC addresses identifying the connection, ISP contract and admin credentials.
(4) Owner(s) *Who owns this information asset?*		
The household member who owns the contract.		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Public IP and MAc addresses are of public domain. Information transmitted on the net must be confidential. Admin credentials must be secret.	Administrative credentials must be known only to asset owners. Traffic must be confidential.
❑ **Integrity**	The assets Integrity requires only the network owner, ISP, and NIC vendors being able to use and control the asset, preventing unauthorized use and modifications.	Compromise of integrity leads to impersonation, identity theft and potential breach of confidentiality.
❑ **Availability**	This asset must be available to household members and authorized guests.	Disruption leads to inability to perform activities and control cloud IoT devices.
	This asset must be always available.	Interruptions during day and evening time are more likely to cause inconveniences.
❑ **Other**	Misuse of this asset can lead to legal consequences for the network owner.	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
☑ Confidentiality	☐ Integrity	☑ Availability ☐ Other

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?*
Smart Home	Smart Home devices (IoT) functioning is critical, as our household relies on them for many needs like lighting to heating, door opening and entertainment.	The asset consists of hardware, software and proper functioning of IoT devices like lightbulbs, thermostats, door locks, gateway and the softwares/firmwares controlling those.
(4) Owner(s) *Who owns this information asset?*		
In most cases one of the household members is in charge of implementing and configuring IoT devices.		
(5) Security Requirements *What are the security requirements for this information asset?*		
☐ **Confidentiality**	IoT devices data may reveal sensitive information on the household. They normally store account credentials.	Only household members should access the asset.
☐ **Integrity**	The asset is considered integer when only legitimate users can interact with it.	Compromise of integrity leads to threat actors being able to tamper devices, breach privacy and exfiltrate data.
☐ **Availability**	This asset must be available to household members and authorized guests.	Disruption leads to inability to perform activities in the household, and loss of efficiency.
	This asset must be always available.	Proper operation of devices is critical anytime of the day, independently from household members' presence.
☐ **Other**		
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
☐ Confidentiality	☑ Integrity	☐ Availability ☐ Other

Appendix 3: Worksheets 9

Allegro Worksheet 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)**
Account credentials	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Local Smart devices (Lightbulbs, thermostats….) controlled locally.	Device owner
Home gateway (Computer system controlling devices and providing user interaction)	Gateway owner / Smarthome enthusiast
Endpoint devices used to control smart homes (Smartphone apps, web-apps, card readers…)	Endpoint owner
Home network	

EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Cloud connected Smart devices (Lightbulbs, thermostats….) relying on cloud services.	Device owner
	Cloud service provider
Internet network	-

Allegro Worksheet 9b	**INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)**
Account credentials	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Paper backup copies	Account owner

EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
	Providers

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Account credentials	

Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
Household members (users)	Household
Smarthome enthusiast (admin)	Household

External Personnel	
Contractor, Vendor, Etc.	**Organization**
Household guests	

Allegro Worksheet 9a	**ARCHIVED FILES RISK ENVIRONMENT MAP (TECHNICAL)**
Important files	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Personal devices (Pc, laptops, tablet, smartphones)	Device owner
NAS	Admin
Home Network	Admin

EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Cloud storage	Account owner
	Cloud service provider

Allegro Worksheet 9b	**INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)**
Important files	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Offline backup drives	Admin

EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Important files	

Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
Household members (users)	-
Backup admin	

External Personnel	
Contractor, Vendor, Etc.	**Organization**

Allegro Worksheet 9a	**BANKING DETAILS RISK ENVIRONMENT MAP (TECHNICAL)**
Bank credentials	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Home Network	Admin
Smart phones	Owner
Laptop, Tablets, PC	Owner
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Cloud services subscriptions	Service Provider
	Contract owner
Internet connection	ISP
Payment systems (POS, ATMs…)	Service Provider

Allegro Worksheet 9b	**INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)**
Bank credentials	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Payment cards	Owner
Printed copies of PIN codes, OTP etc…	Owner
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Bank credentials	

Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
Bank account owner	

External Personnel	
Contractor, Vendor, Etc.	**Organization**

Allegro Worksheet 9a	**INTERNET CONNECTION RISK ENVIRONMENT MAP (TECHNICAL)**
Internet connection	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Networks (WiFi, Bluetooth, Zigbee, wired…)	Admin
Network devices admin credentials (Router configuration, NAS, smart devices…)	Admin
Network access credentials (WiFi passwords, pairing keys, encryption keys….)	Admin
Exposed ports for Home Gateway or other services	Admin
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Internet service	Internet Service Provider
	Contract owner

Allegro Worksheet 9b	**INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)**
Internet connection	
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Router labels and QR codes with WiFi access credentials	Network contract owner
Wired connection	Network contract owner
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
DSL / Cable / Optical line	ISP

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Internet connection	

Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
Household members / Responsible for their actions on the network and for keeping the access credentials safe	-
Network contract owner/ Besides sharing the same responsibilities of other members, he is also responsible for correct configuration and monitoring of network devices, and for custody of admin credentials.	
External Personnel	
Contractor, Vendor, Etc.	**Organization**
Household guests / If given access to the network they are responsible for their actions and for custody of access credentials.	

Allegro Worksheet 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)**
Smart Home	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Smart devices (Lightbulbs, thermostats….) controlled locally.	Device owner
Home gateway (Computer system controlling devices and providing user interaction)	Gateway owner / Smarthome enthusiast
Endpoint devices used to control smart homes (Smartphone apps, web-apps, card readers…)	Endpoint owner

EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Smart devices (Lightbulbs, thermostats….) relying on cloud services.	Device owner
	Cloud service provider

Allegro Worksheet 9b	**INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)**
Smart Home	

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**

EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
Utilities (Electricity, heating, Internet, water…)	Providers

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Smart Home	

Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
Household members (users)	-
Smarthome enthusiast (admin)	
External Personnel	
Contractor, Vendor, Etc.	**Organization**
Household guests	
Software and Hardware developers	

Appendix 4: Worksheets 10

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Personal Accounts credentials		
		Area of Concern	Http traffic eavesdropping		
		(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?*	Many smartdevice have a web interface for configuration, which is often served in plain HTTP. An attacker can sniff this traffic and easily retrieve login credentials.		
		(3) Motive *What is the actor's reason for doing it?*	Successful eavesdropping gives the attacker access to the device. The same credentials can be tested to control other devices in the network. The hacked device can serve as a starting point for 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?*	Confidentiality and Integrity of credentials 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**
Compromise of the device	Reputation & Confidence	H	12
	Financial	L	5
If the same password was reused, the attacker can gain access to multiple devices at the same time.	Productivity	H	9
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
	Relative Risk Score		**39**

(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	If the device provides this possibility, enable HTTPS access to configuration page
Passwords	Use a password manager to generate random and unique passwords for devices.
Network	Monitor new devices accessing the home network and verify their identity.

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk — **Threat**	Information Asset	Personal Accounts credentials		
	Area of Concern	Http traffic eavesdropping - residual risk		
	(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?*	Many smartdevice have a web interface served in plain HTTP. An attacker can sniff this traffic and easily retrieve login credentials.		
	(3) Motive *What is the actor's reason for doing it?*	Successful eavesdropping gives the attacker access to the device. The same credentials can be tested to control other devices in the network. The hacked device can serve as a starting point for 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?*	Confidentiality and Integrity of credentials 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**
Compromise of the device	Reputation & Confidence	L	4
	Financial	L	5
	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	L	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	Personal Accounts credentials		
		Area of Concern	Phishing emails		
		(1) Actor *Who would exploit the area of concern or threat?*	External threat actor		
		(2) Means *How would the actor do it? What would they do?*	Phishing emails may impersonate smart devices service providers and trick users into opening malicious links or give away their credentials.		
		(3) Motive *What is the actor's reason for doing it?*	Credentials allow access to smart home controls, and can be tested to login on other websites.		
		(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 credentials 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**
Compromise of the account	Reputation & Confidence	H	12
	Financial	L	5
If the same credentials were reused, the attacker can gain access to multiple services.	Productivity	M	6
	Safety & Health	M	12
	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
	Relative Risk Score		**126**

(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?*
Email clients	Use modern mail clients which provides antispam and antiphishing filters.
People	Raise awareness in household members about phishing and instruct them on verifying emails authenticity and domains of URLs.
Credentials	Use unique and random credentials. Provide every household member a specific account, which can be immediately shut down in case of compromise.
Smarthome	Monitor user activities and investigate suspect or unexpected behaviors.
Logins	Enable 2FA authentication when available, especially for accounts which can access the system from the internet.

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Personal Accounts credentials		
		Area of Concern	Phishing emails - residual risk		
		(1) Actor *Who would exploit the area of concern or threat?*	External threat actor		
		(2) Means *How would the actor do it? What would they do?*	Phishing emails may impersonate smart devices service providers and trick users into opening malicious links or give away their credentials.		
		(3) Motive *What is the actor's reason for doing it?*	Credentials allow access to smart home controls, and can be tested to login on other websites.		
		(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 credentials 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**
Compromise of the account, requiring the admin to reset its password.	Reputation & Confidence	L	4
	Financial	L	5
	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	L	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?*
	t

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Archived Files		
		Area of Concern	*Ransomware attack on personal devices*		
		(1) Actor *Who would exploit the area of concern or threat?*	Malicious actor, most probably organized.		
		(2) Means *How would the actor do it? What would they do?*	Abuse of smart device weakness or misconfigurations to access the home network and spread ransomware targeting other devices like personal computer and NAS.		
		(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?*	Integrity, confidentiality and availability of files are 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**
Payment of ransom or encryption of files contained in the infected device(s)	Reputation & Confidence	M	8
	Financial	H	15
Notable amount of time required to eradicate malware and restore device functionality.	Productivity	H	9
	Safety & Health	M	12
Potential loss of unique files and work.	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	9
	Relative Risk Score		**108**

(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?*
Files	Map relevant archived files and their archive locations to implement AV and security measures..
Files	Identify a trusted cloud backup service and synchronize the backups often. Be sure to have a local copy and a cloud copy for every relevant file. Local copies mitigate risk of availability breaches if the cloud is unreachable.
Network	Segment network to prevent spread of malware.
Offline backups	Use external hard drives to backup relevant files, keep them unplugged except for the short time strictly needed to access files. Unplugged HD can't be accessed by ransomware.

Allegro - Worksheet 10	**Information Asset Risk Worksheet**			
Information Asset Risk	**Threat**	Information Asset	Archived Files	
		Area of Concern	*Residual risk - Ransomware attack on personal devices*	
		(1) Actor *Who would exploit the area of concern or threat?*	Malicious actor, most probably organised.	
		(2) Means *How would the actor do it? What would they do?*	Abuse of smart device weakness or misconfigurations to access the home network and spread ransomware targeting other devices like personal computer and NAS.	
		(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?*	Integrity, confidentiality and availability of files are 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**
Relevant files backed up in cloud and offline drives can be restored. Loss of few recent assets not yet secured.	Reputation & Confidence	L	4
	Financial	L	5
Thanks to network segmentation, the malware can´t spread to all devices, infection is contained to the IoT segment.	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6

Relative Risk Score	**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?*

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?*

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Internet connection		
		Area of Concern	*Abuse of weak WiFi authentication by unauthorized people*		
		(1) Actor *Who would exploit the area of concern or threat?*	External threat actor without advanced skills performing wifi attacks		
		(2) Means *How would the actor do it? What would they do?*	IoT devices have limited resources and rarely support the latest WiFi security standards. They are also an easy target for deauthentication attacks.		
		(3) Motive *What is the actor's reason for doing it?*	abuse of network bandwidth for personal purposes, potentially including illegal 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, confidentiality and availability of the network 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**
If the intruder gets unnoticed, he may perform illegal activities which could lead to the network owner facing legal consequences.	Reputation & Confidence	M	8
	Financial	L	5
Negative impact on network performances, affecting productivity and leading to increased costs.	Productivity	M	6
	Safety & Health	L	6
Confidentiality of data in the network is no longer ensured.	Fines & Legal Penalties	M	2
	User Defined Impact Area	L	2
		Relative Risk Score	**58**

(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?*
Network Access Credentials	Implement strong passwords and a regular password change policy.
Internet connection	Monitor internet traffic counters to detect abnormal traffic.
Networks	Configure router for network segmentation, divide Private network, IoT network and Guest network. Implement firewall rules to allow only necessary traffic.
Internet connection	Selectively allow internet connection only to trusted devices.

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Internet Connection		
		Area of Concern	*Execution of remote unauthorized activities*		
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organised Advanced Threat Actor		
		(2) Means *How would the actor do it? What would they do?*	Exploitation of firmware bugs and vulnerabilities in IoT devices leading to RCE and botnet.		
		(3) Motive *What is the actor's reason for doing it?*	Using IoT devices to proxy malicious traffic to anonymously attack other targets.		
		(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 seriously 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**
If the intruder gets unnoticed, he will perform illegal activities which could lead to the network owner facing legal consequences for the harm caused.	Reputation & Confidence	M	8
	Financial	L	5
Execution of remote activities could lead to increased power consumption, lower battery duration and additional traffic, impacting operative costs and performances.	Productivity	M	6
	Safety & Health	L	6
	Fines & Legal Penalties	H	3
	User Defined Impact Area	H	6
		Relative Risk Score	**34**

(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?*
Networks	Configure router for network segmentation, divide Private network, IoT network and Guest network. Implement firewall rules to allow only necessary traffic.
Network	Selectively allow internet connection only to trusted devices.
Network	Isolate IoT WiFi clients to prevent unnecessary cross-talking.

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Internet Connection	
		Area of Concern	*Execution of remote unauthorized activities - Residual risk*	
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organised Advanced Threat Actor	
		(2) Means *How would the actor do it? What would they do?*	Exploitation of firmware bugs and vulnerabilities in IoT devices leading to RCE and botnet.	
		(3) Motive *What is the actor's reason for doing it?*	Using IoT devices to proxy malicious traffic to anonymously attack other targets.	
		(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 seriously 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**
Execution of malware can lead to increased power consumption and lower battery duration, impacting operative costs and performances.	Reputation & Confidence	L	4
	Financial	L	5
	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	L	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	Internet Connection	
		Area of Concern	*Lateral movement of threat actor in home network*	
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organised threat actor with technical skills.	
		(2) Means *How would the actor do it? What would they do?*	Exploited IoT device used as an entry point, allowing malicious actors to further exploit other devices, analyse network traffic and exfiltrate files.	
		(3) Motive *What is the actor's reason for doing it?*	Accessing sensitive data for financial gain (i.e. stealing credentials or blackmailing).	
		(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 network are 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**
If the attack succeeds and sensitive data like logins are stolen, the threat actor can take control of the accounts, with potentially disastrous consequences for privacy and finance.	Reputation & Confidence	H	12
	Financial	H	15
If the attacker succeeds in exfiltrating personal files, he can use them for blackmailing or asking payment of a ransom to release them.	Productivity	H	9
	Safety & Health	M	12
The attacker may access work devices and files, harming not only the household members but also the organizations they work for.	Fines & Legal Penalties	M	2
	User Defined Impact Area	H	6
		Relative Risk Score	**56**

(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?*
Network	https
Network	strong passwords
Network	password change policy
Network	Network segmentation / Tri-band router
Devices	Software updates

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Internet Connection		
		Area of Concern	*Reaching maximum number of clients / connections supported by router*		
		(1) Actor *Who would exploit the area of concern or threat?*	-		
		(2) Means *How would the actor do it? What would they do?*	Most consumer routers have a practical limit to the number of concurrent hosts or connections supported.		
		(3) Motive *What is the actor's reason for doing it?*	The limit can be easily reached when adding smart devices to home network		
		(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**
Instability and slowness of the network	Reputation & Confidence	L	4
	Financial	L	5
Possible crashes or reboots of router	Productivity	H	9
	Safety & Health	L	6
Inability of new devices to connect to the network	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
		Relative Risk Score	**62**

(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?*
Network	Configure a cascade router for network segmentation, divide Private network, IoT network and Guest network. Implement firewall rules to allow only necessary traffic. Use dedicated WiFi for IoT devices.

Allegro - Worksheet 10	**Information Asset Risk Worksheet**			
Information Asset Risk	**Threat**	Information Asset	Internet Connection	
		Area of Concern	*Attacks to home gateway*	
		(1) Actor *Who would exploit the area of concern or threat?*	External threat, no specific skills needed	
		(2) Means *How would the actor do it? What would they do?*	After mapping open ports on the router using recon tools and fingerprinting exposed services, the home gateway is attacked using dictionary and brute force techniques or exploiting specific vulnerabilities.	
		(3) Motive *What is the actor's reason for doing it?*	Abusing gateway to exfiltrate data, distribute malware, lateral movement or C2C.	
		(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 Home network 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**
In case of success, tampering of smart-home gateway and devices, including door locks, video cameras and other critical systems.	Reputation & Confidence	M	8
	Financial	L	5
Installation of malware on gateway, lateral movement, remote control and data exfiltration. Potential exposure of accounts and payment details stored on gateway, connected cloud services and iot devices. Attack of other devices in the network.	Productivity	H	9
	Safety & Health	M	10
In any case, abuse of computing resources impacts systems leading to poor performances, potential failures and unavailability.	Fines & Legal Penalties	M	2
	User Defined Impact Area	H	6
		Relative Risk Score	**120**

(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 Gateway	Prefer Cloudflare tunnels or webhook systems which allow external communication without opening ports on the router.
Home Gateway	Enable HTTPS if available
Network	Use WAF or firewall to limit maximum login attempts
Home Gateway	Keep software updated

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 organised 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 utilising 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 organised 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 behaviour, 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.

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.
Smar thome system	Have backup controls to operate critical devices in absence of network connectivity.

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?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
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.	Reputation & Confidence	M	8
	Financial	L	5
The informations may be sold without user acknowledgement to marketing and advertising companies	Productivity	L	3
	Safety & Health	M	12
Unauthorized collection and processing of user data is against user's rights, as defined by GDPR.	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

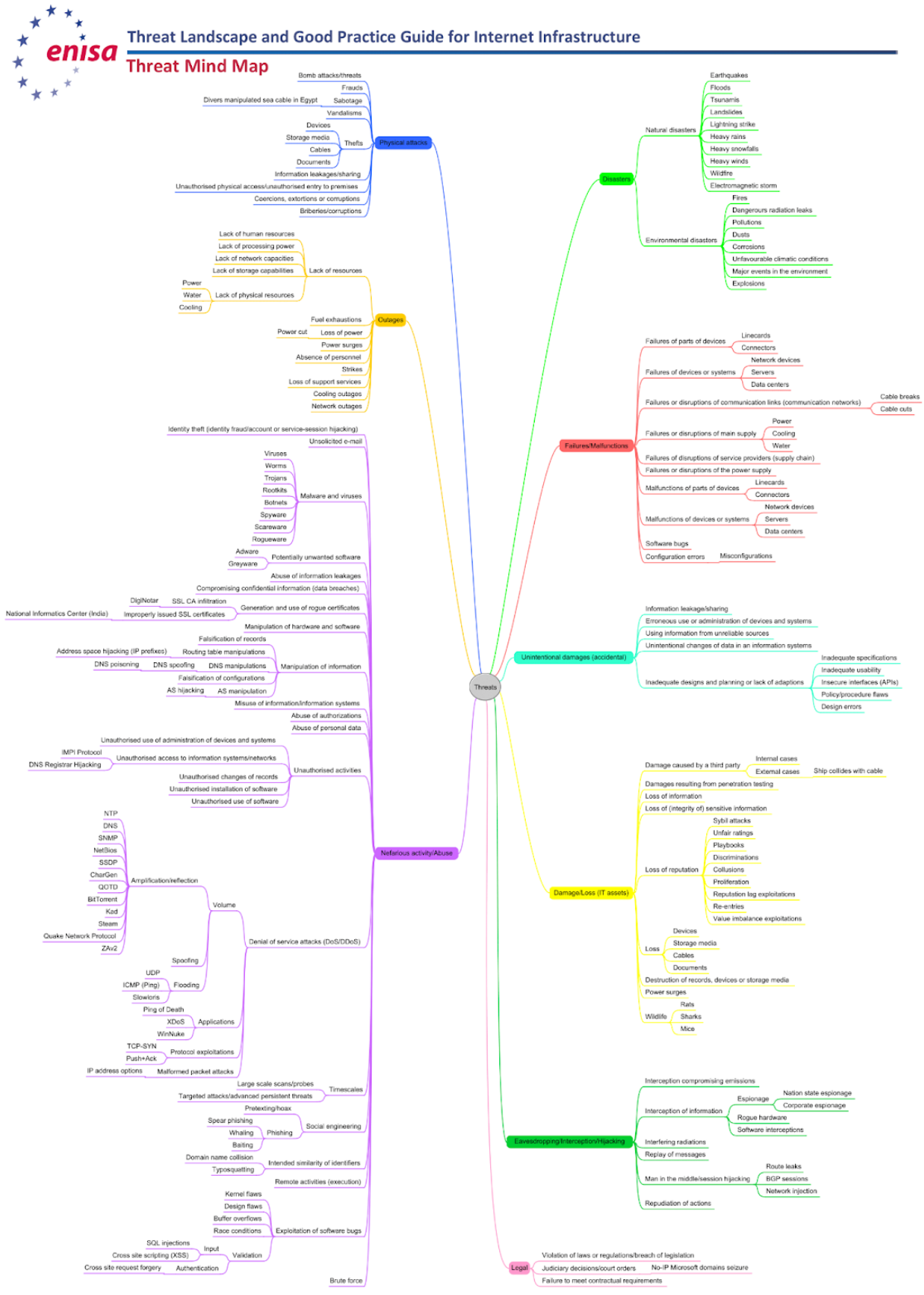
Based on the total score for this risk, what action will you take?

☐ **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.

Appendix 5: ENISA Threat Mind Map


enisa
Threat Landscape and Good Practice Guide for Internet Infrastructure
Threat Mind Map
Threats
Physical attacks
Bomb attacks/threats
Frauds
Sabotage
Divers manipulated sea cable in Egypt
Vandalisms
Thefts
Devices
Storage media
Cables
Documents
Information leakages/sharing
Unauthorised physical access/unauthorised entry to premises
Coercions, extortions or corruptions
Briberies/corruptions
Outages
Lack of resources
Lack of human resources
Lack of processing power
Lack of network capacities
Lack of storage capabilities
Lack of physical resources
Power
Water
Cooling
Fuel exhaustions
Loss of power
Power cut
Power surges
Absence of personnel
Strikes
Loss of support services
Cooling outages
Network outages
Nefarious activity/Abuse
Identity theft (identity fraud/account or service-session hijacking)
Unsolicited e-mail
Malware and viruses
Viruses
Worms
Trojans
Rootkits
Botnets
Spyware
Scareware
Rogueware
Potentially unwanted software
Adware
Greyware
Abuse of information leakages
Compromising confidential information (data breaches)
Generation and use of rogue certificates
DigiNotar
SSL CA infiltration
National Informatics Center (India)
Improperly issued SSL certificates
Manipulation of hardware and software
Manipulation of information
Falsification of records
Routing table manipulations
Address space hijacking (IP prefixes)
DNS manipulations
DNS poisoning
DNS spoofing
Falsification of configurations
AS manipulation
AS hijacking
Misuse of information/information systems
Abuse of authorizations
Abuse of personal data
Unauthorised activities
Unauthorised use of administration of devices and systems
Unauthorised access to information systems/networks
IMPI Protocol
DNS Registrar Hijacking
Unauthorised changes of records
Unauthorised installation of software
Unauthorised use of software
Denial of service attacks (DoS/DDoS)
Amplification/reflection
NTP
DNS
SNMP
NetBios
SSDP
CharGen
QOTD
BitTorrent
Kad
Steam
Quake Network Protocol
ZAv2
Volume
Spoofing
UDP
Flooding
ICMP (Ping)
Slowloris
Applications
Ping of Death
XDoS
WinNuke
Protocol exploitations
TCP-SYN
Push+Ack
Malformed packet attacks
IP address options
Timescales
Large scale scans/probes
Targeted attacks/advanced persistent threats
Social engineering
Pretexting/hoax
Phishing
Spear phishing
Whaling
Baiting
Intended similarity of identifiers
Domain name collision
Typosquatting
Remote activities (execution)
Exploitation of software bugs
Kernel flaws
Design flaws
Buffer overflows
Race conditions
Validation
Input
SQL injections
Cross site scripting (XSS)
Authentication
Cross site request forgery
Brute force
Disasters
Natural disasters
Earthquakes
Floods
Tsunamis
Landslides
Lightning strike
Heavy rains
Heavy snowfalls
Heavy winds
Wildfire
Electromagnetic storm
Environmental disasters
Fires
Dangerours radiation leaks
Pollutions
Dusts
Corrosions
Unfavourable climatic conditions
Major events in the environment
Explosions
Failures/Malfunctions
Failures of parts of devices
Linecards
Connectors
Failures of devices or systems
Network devices
Servers
Data centers
Failures or disruptions of communication links (communication networks)
Cable breaks
Cable cuts
Failures or disruptions of main supply
Power
Cooling
Water
Failures of disruptions of service providers (supply chain)
Failures or disruptions of the power supply
Malfunctions of parts of devices
Linecards
Connectors
Malfunctions of devices or systems
Network devices
Servers
Data centers
Software bugs
Configuration errors
Misconfigurations
Unintentional damages (accidental)
Information leakage/sharing
Erroneous use or administration of devices and systems
Using information from unreliable sources
Unintentional changes of data in an information systems
Inadequate designs and planning or lack of adaptions
Inadequate specifications
Inadequate usability
Insecure interfaces (APIs)
Policy/procedure flaws
Design errors
Damage/Loss (IT assets)
Damage caused by a third party
Internal cases
External cases
Ship collides with cable
Damages resulting from penetration testing
Loss of information
Loss of (integrity of) sensitive information
Loss of reputation
Sybil attacks
Unfair ratings
Playbooks
Discriminations
Collusions
Proliferation
Reputation lag exploitations
Re-entries
Value imbalance exploitations
Loss
Devices
Storage media
Cables
Documents
Destruction of records, devices or storage media
Power surges
Wildlife
Rats
Sharks
Mice
Eavesdropping/Interception/Hijacking
Interception compromising emissions
Interception of information
Espionage
Nation state espionage
Corporate espionage
Rogue hardware
Software interceptions
Interfering radiations
Replay of messages
Man in the middle/session hijacking
Route leaks
BGP sessions
Network injection
Repudiation of actions
Legal
Violation of laws or regulations/breach of legislation
Judiciary decisions/court orders
No-IP Microsoft domains seizure
Failure to meet contractual requirements