Smart Home Systems
OCTAVE Allegro

1 - Establish Risk Management Criteria

Key Impact Areas:

Life: Impact on overall well-being and quality of life, encompassing physical, mental, and emotional aspects.
Health: Impact on physical and mental health, including risks posed by medical devices related to health information.
Safety: Impact on the physical safety and security of individuals, property, and assets.
Compliance: Adherence to regulations and standards related to data protection and smart devices.
Reputation: Effect on the company's reputation if a security breach occurs.
Privacy: Impact on the confidentiality of personal user data.
Financial: Financial loss due to compromised devices or data breaches.
Functionality: Impact on the operational functionality of smart home devices.

Stakeholders:

Non-commercial Stakeholders: End users of the smart home system.
Commercial Stakeholders: Software and hardware manufacturers, private and public companies involved in the installation and deployment of home automation systems.

Impact Values:

High Impact: Severe consequences that significantly affect the organization’s mission and objectives, such as substantial financial loss, major privacy breaches, severe safety risks, or significant reputational damage.
Medium Impact: Moderate consequences that impact the organization’s mission and objectives but are manageable, such as moderate financial losses, privacy issues, or reputational concerns.
Low Impact: Minor consequences with minimal effect on the organization’s mission and objectives, such as minor financial losses, isolated privacy issues, or negligible reputational effects.

Criteria for Evaluation:

Life (Priority 5):
High Impact: Loss of human life.
Medium Impact: Users' lives are in danger, but they recover after medical care.
Low Impact: No loss or significant threat to the lives of end users.

Health (Priority 5):
High Impact: Significant health violation, recovery period more than one month, potential chronic diseases.

Medium Impact: Temporary deterioration of users' health.
Low Impact: Minimal deterioration, treated with recovery within a few days.

Safety (Priority 5):
High Impact: End-user safety is compromised, presence of a criminal offense.
Medium Impact: Minimal impact on end-user safety, presence of an administrative offense.
Low Impact: Safety of the end consumer is in question.

Compliance (Priority 4):
High Impact: Significant legal penalties or loss of compliance certifications due to regulatory violations.
Medium Impact: Notices or fines from regulatory bodies, requiring corrective actions.
Low Impact: Minor compliance issues easily rectified with minimal consequences.

Reputation (Priority 4):
High Impact: Major public relations crisis due to a high-profile security breach, severely damaging customer trust.
Medium Impact: Negative media coverage causing some reputational harm, but manageable through effective communication.
Low Impact: Isolated incidents with little to no effect on public perception.

Privacy (Priority 3):
High Impact: Unauthorized access to personal data affecting multiple users, leading to identity theft or significant privacy violations.
Medium Impact: Breach of personal data affecting a small number of users, resulting in limited privacy concerns.
Low Impact: Minimal exposure of non-sensitive personal data, causing negligible privacy concerns.

Financial (Priority 2):
High Impact: Significant financial loss due to large-scale device compromise or data breach.
Medium Impact: Moderate financial implications, such as costs related to device repair or limited data breach.
Low Impact: Minor financial losses with minimal impact on the organization.

Functionality (Priority 1):
High Impact: Extended downtime or malfunction of key smart home systems affecting daily living conditions.
Medium Impact: Temporary disruption of device functionality with moderate impact on user experience.
Low Impact: Minor glitches with minimal effect on overall functionality.

2 - Develop Information Asset Profile

Critical Information Assets:

User Data: Personal information, usage patterns, preferences, and habits.
Security Data: Access codes, encryption keys, and security protocols.
Information Resources: Documents, user files, and other digital resources stored within the smart home system.
Data from Video Surveillance Cameras: Visual data captured by video surveillance cameras.
Smart Home Configuration Settings: Settings and preferences configured to customize the operation of smart home devices and systems.
Event Log Information: Records detailing past events and activities logged by the smart home system.
User Devices: Devices owned and operated by users that interact with the smart home system.
Location Information: Data indicating the physical location of users, devices, or smart home components.

Each Information Asset Profile:

User Data

Justification of the Choice: User data is essential for the smart home system as it provides insights into personal preferences, habits, and usage patterns of the occupants. Understanding user behavior helps optimize the functionality and efficiency of the smart home system.
Description: User data encompasses personal information, usage patterns, preferences, and habits of the occupants. It enables personalized interactions and customization within the smart home environment, enhancing user experience and satisfaction.
Owner(s): The smart home system itself acts as the owner of user data, with responsibility for its management and protection falling under the system's jurisdiction.
Custodians: Custodians responsible for managing and safeguarding user data may include system administrators, data privacy officers, and designated personnel authorized to handle sensitive information.
Security Requirements:

- Confidentiality: User data must be kept confidential and accessible only to authorized users. Any access or sharing of user data should comply with relevant privacy regulations and user consent.
- Integrity: User data should remain accurate and reliable, without unauthorized alterations or tampering. Measures should be in place to prevent data corruption or manipulation.
- Availability: Authorized users should have timely and reliable access to their own user data as needed. Adequate security measures should be implemented to ensure data availability while protecting against unauthorized access or breaches.

Security Data

Justification of the Choice: Security data plays a critical role in safeguarding the integrity and confidentiality of the smart home system. Access codes, encryption keys, and security protocols are essential components for securing sensitive information and protecting against unauthorized access and malicious activities.

Description: Security data encompasses access codes, encryption keys, and security protocols used to authenticate users, encrypt communication, and enforce security measures within the smart home system. These elements are vital for ensuring data confidentiality, integrity, and availability.

Owner(s): The smart home system holds ownership of security data, with responsibility for its management, implementation, and enforcement.

Custodians: Custodians responsible for managing security data include system administrators, cybersecurity experts, and designated personnel with expertise in information security management.

Security Requirements:

- Confidentiality: Security data must be kept confidential and protected from unauthorized disclosure. Access to sensitive security information should be restricted to authorized individuals only.
- Integrity: Security data should remain intact and trustworthy, free from unauthorized modifications or alterations. Measures should be in place to detect and prevent any attempts to tamper with security settings or protocols.
- Availability: Security data should be readily accessible to authorized users and systems as needed. Adequate redundancy and backup mechanisms should be implemented to ensure the continuous availability of security resources and prevent disruptions in system operations.

Information Resources:

Justification of the Choice: Information resources encompass documents, user files, and digital assets stored within the smart home system, serving as vital components for user interaction, system operation, and data management. Access to these resources is essential for facilitating communication, information sharing, and system functionality within the smart home environment.

Description: Information resources include a variety of digital assets such as documents, user files, media content, and other digital resources stored within the smart home system. These resources serve diverse purposes, including user communication, system configuration, data management, and entertainment.

Owner(s): The smart home system holds ownership of information resources, responsible for their storage, organization, and accessibility to authorized users.

Custodians: Custodians responsible for managing information resources include system administrators, data managers, and designated individuals tasked with content management and data governance within the smart home environment.

Security Requirements:

- Confidentiality: Information resources must be protected from unauthorized access or disclosure to maintain the privacy and confidentiality of sensitive data. Access controls and encryption measures should be implemented to restrict access to authorized users only.
- Integrity: Information resources should remain accurate, reliable, and free from unauthorized modifications or tampering. Data integrity checks and version control mechanisms should be in place to ensure the consistency and reliability of stored information.
- Availability: Information resources should be available for timely access and retrieval by authorized users as needed. Adequate backup solutions and redundancy measures should be implemented to prevent data loss or downtime and ensure continuous availability of critical resources.

Data from Video Surveillance Cameras:

Justification of the Choice: Data from video surveillance cameras is essential for monitoring and ensuring the security and safety of the smart home environment. It provides visual insights into activities within and around the premises, enabling proactive responses to potential security threats or incidents.
Description: Data from video surveillance cameras consists of visual recordings captured by surveillance cameras installed within the smart home premises. These recordings document activities, events, and interactions, serving as valuable evidence for security monitoring and incident investigation.
Owner(s): The smart home system assumes ownership of data from video surveillance cameras, responsible for its storage, management, and utilization in accordance with privacy regulations and security policies.
Custodians: Custodians responsible for managing video surveillance data include system administrators, security personnel, and designated individuals tasked with monitoring and reviewing surveillance footage.
Security Requirements:

- Confidentiality: Video surveillance data must be kept confidential and protected from unauthorized access or disclosure. Access to recorded footage should be restricted to authorized personnel for security monitoring purposes only.
- Integrity: Video surveillance data should remain intact and unaltered to maintain its accuracy and reliability as evidence. Measures should be implemented to prevent tampering or unauthorized modifications to recorded footage.
- Availability: Video surveillance data should be available for timely retrieval and review by authorized personnel as needed. Adequate storage capacity and backup solutions should be in place to ensure continuous access to recorded footage and prevent data loss or corruption.

Smart Home Configuration Settings:
Justification of the Choice: Smart home configuration settings are essential for customizing the operation of smart home devices and systems according to user preferences and requirements. These settings enable users to personalize their smart home environment, optimize device functionality, and enhance user experience.
Description: Smart home configuration settings encompass a range of preferences, options, and parameters configured to customize the behavior and operation of smart home devices and systems. These settings include preferences for device control, automation rules, scheduling, notifications, and other customization options.
Owner(s): The smart home system holds ownership of configuration settings, responsible for their management, storage, and enforcement across the smart home environment.
Custodians: Custodians responsible for managing smart home configuration settings include system administrators, device manufacturers, and designated personnel involved in system configuration and maintenance.
Security Requirements:

- Confidentiality: Smart home configuration settings should be protected from unauthorized access or disclosure to prevent tampering or misuse. Access controls and encryption measures should be implemented to restrict access to authorized users only.
- Integrity: Configuration settings should remain accurate, reliable, and consistent to ensure the proper functioning of smart home devices and systems. Measures should be in place to prevent unauthorized modifications or alterations to configuration settings.
- Availability: Configuration settings should be readily accessible for modification and customization by authorized users as needed. Adequate backup solutions and redundancy measures should be implemented to prevent data loss or corruption and ensure continuous availability of configuration options.

Event Log Information:

Justification of the Choice: Event log information is crucial for tracking past events and activities within the smart home system. It provides a historical record of system interactions, device operations, and user activities, enabling troubleshooting, analysis, and auditing.
Description: Event log information consists of records documenting past events, activities, and system interactions logged by the smart home system. These logs capture details such as device activations, sensor readings, user interactions, system alerts, and other relevant information.
Owner(s): The smart home system holds ownership of event log information, responsible for its generation, storage, and management to facilitate system monitoring and analysis.
Custodians: Custodians responsible for managing event log information include system administrators, cybersecurity personnel, and designated individuals tasked with log monitoring, analysis, and maintenance.
Security Requirements:

- Confidentiality: Event log information should be protected from unauthorized access or disclosure to prevent the exposure of sensitive system data or user activities. Access controls and encryption measures should be implemented to restrict access to authorized personnel only.
- Integrity: Event logs should remain accurate, reliable, and tamper-proof to ensure the trustworthiness and reliability of recorded information. Measures should be in place to detect and prevent unauthorized modifications or alterations to log records.
- Availability: Event log information should be readily accessible for monitoring, analysis, and auditing purposes by authorized users as needed. Adequate storage capacity and backup solutions should be in place to ensure the continuous availability and integrity of log records, even in the event of system failures or disruptions.

User Devices:
Justification of the Choice: User devices play a vital role in interacting with the smart home system, enabling users to control and monitor their smart home environment remotely. Understanding these devices is essential for ensuring seamless integration and compatibility within the smart home ecosystem.
Description: User devices refer to electronic devices owned and operated by users that interact with the smart home system. These devices include smartphones, tablets, computers, smartwatches, and other personal gadgets used for accessing smart home applications, controlling devices, and receiving notifications.
Owner(s): Users hold ownership of their respective devices and are responsible for their usage, maintenance, and security. The smart home system interacts with user devices but does not assume ownership of them.
Custodians: Custodians responsible for managing user devices include individual users themselves, along with device manufacturers, app developers, and service providers involved in device support and maintenance.
Security Requirements:

- Confidentiality: User devices should be protected from unauthorized access or data breaches to safeguard sensitive information and user privacy. Secure authentication mechanisms and encryption protocols should be employed to prevent unauthorized access to device data.
- Integrity: User devices should remain free from tampering or unauthorized modifications to ensure the integrity and reliability of device functionality and data. Users should be cautious about installing only trusted applications and keeping their devices up to date with security patches.
- Availability: User devices should be readily available and operational for users to access and interact with the smart home system as needed. Adequate support and troubleshooting resources should be provided to ensure the continuous availability and functionality of user devices within the smart home ecosystem.

Location Information:
Justification of the Choice: Location information is critical for various smart home functionalities, including personalized automation, security monitoring, and energy management. Understanding and managing location data is essential for optimizing smart home services and ensuring user privacy.
Description: Location information refers to data indicating the physical whereabouts of users, devices, or smart home components within the smart home environment. This data may include GPS coordinates, Wi-Fi network information, or proximity sensor readings, providing insights into the spatial relationships and movements of entities within the smart home ecosystem.
Owner(s): Ownership of location information may vary depending on the context of its collection. Users typically own their personal location data, while the smart home system may own location information related to devices and components within its infrastructure.
Custodians: Custodians responsible for managing location information include individual users, the smart home system administrators, and third-party service providers involved in location-based services or analytics. These custodians must ensure compliance with privacy regulations and ethical data handling practices.
Security Requirements:

- Confidentiality: Location information should be protected from unauthorized access or disclosure to prevent privacy breaches and location tracking abuses. Access controls, encryption, and anonymization techniques should be implemented to safeguard sensitive location data.
- Integrity: Location data should remain accurate and reliable to support trustworthy smart home functionalities and location-based services. Measures should be in place to detect and prevent data tampering or manipulation, ensuring the integrity of location information.
- Availability: Location information should be available for legitimate smart home applications and services while respecting user preferences and privacy concerns. Adequate safeguards should be implemented to prevent service disruptions or data loss, ensuring the continuous availability and reliability of location-based functionalities within the smart home ecosystem.

3 - Identify Information Asset Container

User Data:

Container Type	Description	Owner
Technical Containers		
Internal	Servers, user devices	Smart home owner / residents
External	Cloud storage, third-party services	Cloud service providers
Physical Containers		
Internal	None (Data primarily stored digitally)	Smart home owner / residents
External	Not applicable	
Human Containers		
Internal	Family members, residents	Smart home owner / residents

External	Third-party service providers, support personnel	Third-party service providers, vendors

Security Data:

Container Type	**Description**	**Owner**
Technical Containers		
Internal	Authentication servers, encryption modules	Smart home owner / administrators
External	Not applicable	
Physical Containers		
Internal	Secure storage devices	Smart home owner / administrators
External	Not applicable	
Human Containers		
Internal	Authorized personnel	Smart home owner / administrators
External	Third-party security consultants, support personnel	Third-party security consultants, vendors

Information Resources:

Container Type	Description	Owner
Technical Containers		
Internal	File servers, cloud storage	Smart home owner / administrators
External	Not applicable	
Physical Containers		
Internal	None (Data primarily stored digitally)	Smart home owner / administrators
External	Not applicable	
Human Containers		
Internal	Authorized users, administrators	Smart home owner / administrators
External	Third-party service providers, support personnel	Third-party service providers, vendors

Data from Video Surveillance Cameras:

Container Type	Description	Owner
Technical Containers		
Internal	Video surveillance system, DVR/NVR	Smart home owner / administrators
External	Cloud storage, third-party services	Cloud service providers
Physical		

Containers		
Internal	None (Data primarily stored digitally)	Smart home owner / administrators
External	Not applicable	
Human Containers		
Internal	Authorized users, security personnel	Smart home owner / administrators
External	Third-party security consultants, support personnel	Third-party service providers, vendors

Smart Home Configuration Settings:

Container Type	Description	Owner
Technical Containers		
Internal	Configuration servers, device firmware	Smart home owner / administrators
External	Not applicable	
Physical Containers		
Internal	None (Settings primarily stored digitally)	Smart home owner / administrators
External	Not applicable	
Human Containers		
Internal	Authorized users, administrators	Smart home owner / administrators
External	Third-party service providers, support personnel	Third-party service providers, vendors

Event Log Information:

Container Type	Description	Owner
Technical Containers		
Internal	Logging servers, event management systems	Smart home owner / administrators
External	Not applicable	
Physical Containers		
Internal	None (Data primarily stored digitally)	Smart home owner / administrators
External	Not applicable	
Human Containers		

Internal	Authorized users, administrators	Smart home owner / administrators
External	Third-party service providers, support personnel	Third-party service providers, vendors

User Devices:

Container Type	Description	Owner
Technical Containers		
Internal	Device management systems, user device firmware	Smart home owner / administrators
External	Not applicable	
Physical Containers		
Internal	None (Information primarily stored digitally)	Smart home owner / administrators
External	Not applicable	
Human Containers		
Internal	Authorized users, administrators	Smart home owner / administrators
External	Third-party service providers, support personnel	Third-party service providers, vendors

Location Information:

Container Type	Description	Owner
Technical Containers		
Internal	Location tracking systems, GPS modules	Smart home owner / administrators
External	Not applicable	
Physical Containers		
Internal	None (Data primarily stored digitally)	Smart home owner / administrators
External	Not applicable	
Human Containers		
Internal	Authorized users, administrators	Smart home owner / administrators
External	Third-party service providers, support personnel	Third-party service providers, vendors

4 - Identify Areas Of Concern

Area of Concern	**Problem**	**Impact**	**Condition**
Changing the Gas Sensor	Tampering with gas sensor	Incorrect readings, potential failure to detect gas leaks, endangering residents' lives	Unauthorized physical access to the sensor
Obtaining Data from Motion Sensor	Unauthorized access to motion sensor data	Increased risk of burglary, privacy invasion	Weaknesses in network security allowing unauthorized access
Reading Status of Door Locks and Alarm Systems	Unauthorized reading of lock and alarm status	Increased risk of break-in, compromise of security system	Inadequate encryption of transmitted data
Denial of Service (DoS) Attacks	DoS attacks on the smart home system	System unable to monitor critical events like fire or flooding, compromising safety	Network vulnerabilities that allow DoS attacks
Unauthorized Access to sensitvie data	Unauthorized access to personal information	Privacy invasion, potential identity theft	Weak authentication methods, weak access controls
Data Breaches	Breaches leading to leakage of personal data	Compromise of personal information, identity theft	Insufficient data encryption, inadequate security measures
Data Misuse	Misuse of personal information	Potential exploitation, targeted advertising, privacy violations	Lack of data governance, inadequate privacy policies
Data Integrity	Unauthorized modification of user data	Loss of trust, potential misinformation	Weak data validation processes, lack of data integrity controls
Data Retention Policies	Lack of clear data retention policies	Over-retention of personal data, potential privacy violations, regulatory non-compliance	Absence of clear guidelines or policies on data retention and deletion

Key Management	Insecure storage or management of encryption keys	Potential compromise of encrypted data, unauthorized decryption	Weak encryption protocols, lack of key rotation policies
Security Protocol Weaknesses	Weaknesses in security protocols	Vulnerabilities exploited by attackers, compromise of security measures	Lack of regular security audits, outdated security protocols
Insider Threats	Misuse or leakage of security data by insiders	Compromise of security, unauthorized access or control over the smart home system	Inadequate employee training, lack of insider threat detection mechanisms
Unauthorized access to the main smart home system	Unauthorized execution of operations	Loss of control over the smart home system, adversary can take photos, record conversations, and track locations	Weak authentication methods, lack of access controls
Unauthorized Access to Main System	Attacker finds a way to access the main system	Attacker changes system configuration and adds back doors, financial losses	Weak system access controls, inadequate security measures
Unauthorized Access During Absence	Breaking into the smart home if it is vacant	Financial losses, user privacy violation	Weak physical security measures, lack of remote monitoring

5 - Identify Threat Scenarios

Area of Concern	Threat Actor	Means	Motive	Undesirable Outcome
Changing the Gas Sensor	Intruder (hacker or unscrupulous supplier)	Hacking tools or vulnerabilities in hardware	Financial gain or personal satisfaction	Incorrect gas readings leading to potential harm or property damage
Obtaining Data from Motion Sensor	Malicious software or unauthorized user	Exploiting network vulnerabilities	Espionage or data theft	Unauthorized access to sensitive data, compromising residents' privacy and security
Reading Status of Door Locks and Alarm Systems	Intruder or malicious software	Exploiting encryption weaknesses	Planning burglaries or disrupting security	Compromised security system status, increasing the risk of break-ins or system manipulation
Denial of Service (DoS) Attacks	Hackers or malicious entities	Launching DoS attacks targeting vulnerabilities	Disruption of service, causing chaos or financial harm	Disabling critical monitoring functions, potentially leading to missed security events or emergencies
Unauthorized Access to Sensitive Data	Malicious insider or external hacker	Exploiting weak access controls or social engineering	Espionage, blackmail, or data theft	Exposure of sensitive data, leading to privacy breaches and potential identity theft
Data Breaches	Cybercriminals or malicious insiders	Hacking, phishing, or exploiting software vulnerabilities	Financial gain, espionage, or sabotage	Loss of data integrity and confidentiality, legal ramifications, and financial losses
Data Misuse	Unauthorized personnel or malicious insiders	Misusing legitimate access to data	Personal gain or malicious intent	Unauthorized distribution or use of data, leading to loss of trust and potential legal issues
Data Integrity	Malicious software or insider threats	Tampering with data during transmission or storage	Disruption, fraud, or sabotage	Corrupted data leading to incorrect decision-making and operational failures

Data Retention Policies	Negligence or malicious insiders	Failure to follow data retention policies	Negligence or intent to misuse data	Unauthorized retention or deletion of data, resulting in legal and compliance issues
Key Management	Hackers or insiders	Compromising encryption keys through weak key management practices	Gaining unauthorized access to encrypted data	Decryption of sensitive data, leading to breaches and loss of data confidentiality
Security Protocol Weaknesses	Hackers or malicious software	Exploiting flaws in security protocols	Unauthorized access, data theft, or disruption	Compromised communication channels and data breaches
Insider Threats	Disgruntled employees or contractors	Using legitimate access for malicious purposes	Revenge, financial gain, or espionage	Unauthorized data access, manipulation, or sabotage
Unauthorized Access to the Main Smart Home System	Hackers or unauthorized users	Exploiting system vulnerabilities or weak authentication mechanisms	Full control over the smart home system for various malicious purposes	Complete system takeover, leading to privacy breaches and physical security risks
Unauthorized Access During Absence	Burglars or malicious insiders	Exploiting physical or digital security gaps during homeowner’s absence	Burglary or sabotage	Theft of property, unauthorized access, and potential physical harm

6 - Identify Risks

Threat Scenario	Consequences
An intruder exploits vulnerabilities in the gas sensor, altering its readings for financial gain.	Incorrect gas readings lead to potential harm or property damage due to inaccurate detection of gas leaks.
Malicious software gains unauthorized access to motion sensor data, compromising residents' privacy.	Intruders monitor residents' movements, enabling targeted burglaries or invasion of privacy.
A hacker compromises encryption on door locks and alarm systems, gaining unauthorized access to their status.	Burglars exploit unlocked doors or disabled alarms, increasing the risk of break-ins and property theft.
Hackers launch DoS attacks on the smart home system, disrupting critical monitoring functions.	Critical security events or emergencies are missed due to disabled monitoring functions, risking residents' safety.
Cybercriminals breach the smart home system, stealing sensitive data for financial gain.	Legal ramifications, financial losses, and compromised privacy result from the exposure of sensitive data.
Unauthorized personnel misuse legitimate access to data for personal gain, leading to loss of trust.	Misused data leads to compromised privacy, loss of trust, and potential legal consequences for the smart home system.
Malicious software tampers with data during transmission, leading to incorrect decision-making.	Operational failures occur due to corrupted data, jeopardizing the effectiveness of the smart home system.
Negligence or malicious insiders fail to follow data retention policies, resulting in unauthorized data retention or deletion.	Legal and compliance issues arise from unauthorized handling of data, leading to regulatory fines and penalties.
Hackers compromise encryption keys through weak management practices, decrypting sensitive data.	Sensitive data is exposed, leading to breaches, loss of confidentiality, and compromised privacy for residents.
Exploiting flaws in security protocols, hackers gain unauthorized access to the smart home system.	Data breaches occur, compromising privacy, and exposing residents to financial losses and identity theft.
Disgruntled employees misuse their access to the smart home system, sabotaging its functionality.	Unauthorized data access, manipulation, or sabotage disrupts system operations and compromises residents' security.
Hackers exploit vulnerabilities to gain unauthorized access, enabling complete system takeover.	Complete control over the smart home system allows for privacy breaches, physical security risks, and potential harm to residents.
Burglars exploit security gaps during the homeowner's absence, gaining unauthorized access to the property.	Theft of property, unauthorized access, and potential physical harm occur due to compromised security during absence.

7 - Analyze Risks

Threat Scenario 1: An intruder exploits vulnerabilities in the gas sensor, altering its readings for financial gain.

Impact Area	Ranking	Impact Value	Score
Life	5	High (3)	15
Health	5	Medium (2)	10
Safety	5	High (3)	15
Compliance	4	Medium (2)	8
Reputation	4	Medium (2)	8
Privacy	3	Low (1)	3
Financial	2	Medium (2)	4
Functionality	1	Low (1)	1
Total Score			64

Threat Scenario 2: Malicious software gains unauthorized access to motion sensor data, compromising residents' privacy.

Impact Area	Ranking	Impact Value	Score
Life	5	Medium (2)	10
Health	5	Medium (2)	10
Safety	5	High (3)	15
Compliance	4	Medium (2)	8
Reputation	4	Medium (2)	8
Privacy	3	High (3)	9
Financial	2	Medium (2)	4
Functionality	1	Low (1)	1
Total Score			65

Threat Scenario 3:A hacker compromises encryption on door locks and alarm systems, gaining unauthorized access to their status.

Impact Area	Ranking	Impact Value	Score
Life	5	Medium (2)	10
Health	5	Medium (2)	10
Safety	5	High (3)	15
Compliance	4	Medium (2)	8
Reputation	4	Medium (2)	8
Privacy	3	Medium (2)	6
Financial	2	High (3)	6
Functionality	1	Low (1)	1
Total Score			64

Threat Scenario 4: Hackers launch DoS attacks on the smart home system, disrupting critical monitoring functions.

Impact Area	Ranking	Impact Value	Score
Life	5	Medium (2)	10
Health	5	Medium (2)	10
Safety	5	High (3)	15
Compliance	4	Medium (2)	8
Reputation	4	Medium (2)	8
Privacy	3	Low (1)	3
Financial	2	Medium (2)	4
Functionality	1	High (3)	3
Total Score			61

Threat Scenario 5: Cybercriminals breach the smart home system, stealing sensitive data for financial gain.

Impact Area	Ranking	Impact Value	Score
Life	5	Low (1)	5
Health	5	Low (1)	5
Safety	5	Low (1)	5
Compliance	4	High (3)	12
Reputation	4	High (3)	12
Privacy	3	High (3)	9
Financial	2	High (3)	6
Functionality	1	Low (1)	1
Total Score			55

Threat Scenario 6: Unauthorized personnel misuse legitimate access to data for personal gain, leading to loss of trust.

Impact Area	Ranking	Impact Value	Score
Life	5	Low (1)	5
Health	5	Low (1)	5
Safety	5	Low (1)	5
Compliance	4	Medium (2)	8
Reputation	4	High (3)	12
Privacy	3	High (3)	9
Financial	2	Medium (2)	4
Functionality	1	Low (1)	1
Total Score			49

Threat Scenario 7: Malicious software tampers with data during transmission, leading to incorrect decision-making.

Impact Area	Ranking	Impact Value	Score
Life	5	Low (1)	5
Health	5	Low (1)	5
Safety	5	High (3)	15
Compliance	4	Medium (2)	8
Reputation	4	Medium (2)	8
Privacy	3	Low (1)	3
Financial	2	Low (1)	2
Functionality	1	High (3)	3
Total Score			49

Threat Scenario 8: Negligence or malicious insiders fail to follow data retention policies, resulting in unauthorized data retention or deletion.

Impact Area	Ranking	Impact Value	Score
Life	5	Low (1)	5
Health	5	Low (1)	5
Safety	5	Low (1)	5
Compliance	4	High (3)	12
Reputation	4	High (3)	12
Privacy	3	High (3)	9
Financial	2	Medium (2)	4
Functionality	1	Low (1)	1
Total Score			43

8 - Select Mitigation Approach

One straightforward method is to begin by sorting the risks in order from highest to lowest

Then separate the risks into four pools with equal number of risks

Pool	**Mitigation Approach**
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

Malicious software gains unauthorized access to motion sensor data, compromising residents' privacy.-pool 1

Mitigation: Strengthen access controls and authentication mechanisms to prevent unauthorized access to motion sensor data. Implement intrusion detection systems to monitor and detect suspicious activities related to motion sensor data access.

An intruder exploits vulnerabilities in the gas sensor, altering its readings for financial gain.-pool 1

Mitigation: Implement regular security updates and patches for the gas sensor firmware to address known vulnerabilities. Additionally, encrypt communication between the gas sensor and the central control system to prevent tampering with sensor readings.

A hacker compromises encryption on door locks and alarm systems, gaining unauthorized access to their status.-pool 2

Mitigation: Enhance encryption protocols used for door locks and alarm systems to resist cryptographic attacks. Implement multi-factor authentication for accessing door locks and alarm system status to mitigate the risk of unauthorized access.

Hackers launch DoS attacks on the smart home system, disrupting critical monitoring functions.-pool 2

Mitigation: Deploy DoS mitigation solutions such as rate limiting, traffic filtering, and network segmentation to mitigate the impact of DoS attacks on critical monitoring functions. Implement redundancy and failover mechanisms to ensure continuous monitoring capability.

Cybercriminals breach the smart home system, stealing sensitive data for financial gain.- pool 3

Mitigation: Implement end-to-end encryption for sensitive data transmitted within the smart home system to protect against data breaches. Enhance network security measures such as firewalls, intrusion detection/prevention systems, and network segmentation to prevent unauthorized access to sensitive data.

Unauthorized personnel misuse legitimate access to data for personal gain, leading to loss of trust.- pool 3

Mitigation: Implement role-based access control (RBAC) and least privilege principles to limit access to sensitive data to authorized personnel only. Conduct regular access reviews and audits to detect and prevent unauthorized access and misuse of data.

Malicious software tampers with data during transmission, leading to incorrect decision-making.-pool 4

Mitigation: Implement data integrity mechanisms such as digital signatures and checksums to detect and prevent data tampering during transmission. Use secure communication protocols (e.g., HTTPS) to encrypt data in transit and protect against interception and tampering.

Negligence or malicious insiders fail to follow data retention policies, resulting in unauthorized data retention or deletion.-pool 4

Mitigation: Enforce strict access controls and auditing mechanisms to monitor compliance with data retention policies. Provide regular training and awareness programs to educate personnel about the importance of data retention policies and the consequences of non-compliance. Implement data loss prevention (DLP) solutions to prevent unauthorized data retention or deletion.

RESOURCES:

Relative Risk Matrix			
Probability	Risk Score		
	60<x	x>=50=<x	x>40
High	Pool 1	Pool 2	Pool 2
Medium	Pool 2	Pool 2	Pool 3
Low	Pool 3	Pool 3	Pool 4

- https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf
- https://elar.khmnu.edu.ua/server/api/core/bitstreams/9e3829a5-2b43-4d40-a0d8-271b7737278b/content
- https://www.mdpi.com/1424-8220/18/3/817