Guidelines

Internet of Things (IoT) Cyber Security Guide

Annex C
Case study on Smart Buildings

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

BCA

In consultation with:

CSA SINGAPORE

IMDA IoT Cyber Security Guide Annex C
Version 2, Oct 2025

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Content

This Guide is a living document which is subject to review and revision periodically.

Guides are informative documents and voluntary in nature except when it is made mandatory by a regulatory authority. It can also be reference in contracts as mandatory requirements. Users are advised to assess the suitability of this guide for their intended use.

Compliance with this guide does not exempt users from any legal obligations.

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE LIABLE FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT THE PRACTICE OR IMPLEMENTATION OF THIS GUIDE MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY CONTRIBUTORS OF THIS DOCUMENT OR ANY THIRD PARTY.

AS OF THE DATE OF THE ISSUANCE OF THE PUBLIC CONSULTATION OF THIS GUIDE, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS GUIDE. HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELATED STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF PATENT RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN LEGAL AND/OR TECHNICAL ADVICE IN RELATION TO THE IMPLEMENTATION OF THE GUIDE IF REQUIRED.

Annex C: Case study on Smart Buildings (informative)

1. Overview

With the proliferation of the Internet, mobile technologies, and ubiquitous connectivity, devices deployed in a commercial building get increasingly connected, and isolation is rarely the case. Data from a traditionally isolated building's Operational Technology (OT) network is now available for use in data-driven decision-making, but it is also exposed to common IoT vulnerabilities, such as weak password, poor device management, insufficient data protection, etc.

The security of data that flows across and between smart Internet of Things (IoT) sensors and building systems in a commercial building is of paramount concern and cannot be overlooked. This case study will show how to implement and enforce cybersecurity and cyber resilience from both Information Technology (IT) and OT perspectives in the built environment for the commercial sector.

This case study provides a sample IoT application for Smart Building to illustrate the application of the recommendations defined in the main document ("IMDA IoT Cyber Security Guide"). The sample IoT application and guidance provided are not exhaustive. Users of this case study are required to customise the content according to their business needs and check with the relevant regulatory bodies on the latest regulatory and statutory requirements, where applicable.

1.1 Threat modelling

One cannot properly secure a commercial building without first performing a threat modelling, understanding the assets that matter and the threats that may surface. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of privilege) is a popular model used to help analyse and find threats to systems, in general. It should be noted that other methodologies exist and might be more appropriate for specific use cases. For example, the MITRE Attack framework provides tactics, techniques, and procedures (also known as TTPs) used by threat actors.

It is also worth mentioning that threat modelling should be performed on a frequent and regular basis. For example, it can be performed and reviewed yearly or anytime a new device or asset is added as part of a system or upon appearance of new threats that were not previously modelled.

Table C-1 depicts the threat modelling checklist, defined in the main document ("IMDA IoT Cyber Security Guide"), and its application to this case study.

ID	Threat modelling checklist	Y (yes) / N (no)	Supporting materials
1	Identify the potential target(s) to be protected: i) Define its boundaries and the external systems (including users) that it needs to interact with ii) Decompose the target(s) into its subcomponents iii) Identify data flows within the target(s), and inputs and outputs from external systems iv) Identify sensitive data and where they are handled (at rest, in transit, in use) v) Identify the security needs (based on potential impacts to Confidentiality, Integrity and Availability (CIA triad)) for subcomponents and data flows vi) Identify hardware, software and protocols in use	Y	Refer to section 2

ID	Threat modelling checklist	Y (yes) / N (no)	Supporting materials
2	Define the security problem: i) Identify system accessibility – Identify attack surfaces – Determine operating environments – Determine system / device lifecycles and supply chain ii) Identify system susceptibility / vulnerabilities (e.g. using STRIDE as a guide) – Determine known vulnerabilities – Enumerate threats to attack surfaces – Enumerate threats to operating environments – Enumerate threats to stages of system / device lifecycles and supply chain iii) State any assumptions	Y	Refer to section 3
3	Conduct risk assessment: i) Assess impact of threats and vulnerabilities to CIA triad and match against security needs of assets ii) Determine the system exploitability (resources required, techniques and tools available) to realise threats. iii) Assess the likelihood of the risk iv) Prioritise risks for mitigation, considering factors such as monetary impacts.	Y	Refer to section 4
4	Determine the security objectives. For example, OT system emphasises safety, where integrity takes precedent over confidentiality.	Y	Refer to section 5
5	Define the security requirements needed to address identified security objectives, without specifying their implementation details.	Y	Refer to section 6
6	Design and implement the security capabilities	N	Not cover in this document
7	Validate and verify that the capabilities address the security requirements adequately	N	Not cover in this document

Table C-1: Application of threat modelling checklist

1.2 Security frameworks

This case study was written with guidance provided by the main document ("IMDA IoT Cyber Security Guide"). Robust controls defined in frameworks such as NIST 800-53 and ISO 27001, as well as industrial security requirements such as IEC 62443 and NERC CIP can also be referenced to complement the various security controls and best practices mentioned inside this document. IEC 62443 should be referenced when formal evaluation and certification is required, for example industrial automation subsystems, such as lifts and escalators.

It is recommended that the IoT device vendor reviews and adapts its security framework and policies regularly. This is crucial because it allows the company to adapt to ever-changing threats and ensure comprehensiveness and effectiveness. Additional guidance on IoT security controls could also be found in the document "IoT security reference architecture - an ANT-centric study"[1].

2. Identify the target of protection

This section illustrates the guidance provided in item-1 of Table C-1, which helps to identify the Target Of Protection (TOP) for this case study.

The TOP contains two system boundaries – the Proximity Network (PN) and the Commercial Building Network (CBN).

2.1 Proximity network

The PN consists of two critical components – the IoT Cloud and IoT Edge Gateway. The IoT Cloud, essentially is an operating system on the cloud, built on open standards to allow management, monitoring and control of IoT devices in a smart building and spans across the buildings, cities or countries. Such IoT clouds must ensure extensive connectivity while operating in a secure and open ecosystem to help organizations efficiently and agilely innovate and develop their ecosystems.

IoT Edge Gateway, as the data ingestion end of IoT Cloud, acts as a lightweight building management system (BMS) and adapts thousands of devices and systems within the CBN to connect to the cloud. This case study currently shows that ingestion can be achieved via message queuing telemetry transport (MQTT) over transport layer security (TLS) but this could potentially be extended to include other protocols, such as advanced message queuing protocol (AMQP) to support IoT device management, as required. The IoT Edge Gateway extends the intelligence of the IoT Cloud to the edge, by providing device management, device control, and edge computing through the integration and inheritance of traditional OT technologies, such as Modbus, BACnet, and IEC-104, and deep coordination with IoT Cloud Platform.

2.2 Commercial building network

The CBN contains the backend components deployed in a typical commercial building. End devices, such as power meters, water meters, air-conditioning, and solar, are connected to the IoT Edge Gateway, which now also acts as a lightweight BMS to work with direct digital controller (DDC) used to manage, monitor, and control equipment in a commercial building. Typically, the IoT Edge Gateway is interconnected to the end devices via OT protocols such as BACnet, OPC-UA, Modbus TCP or Modbus RTU. These protocols allow communication between the devices in a commercial building.

From a security perspective, these protocols tend to be unencrypted and without integrity checks, and it leaves them susceptible to cybersecurity attacks that include but are not limited to replay and manipulation attacks. A breach to a building network will simply open up to attackers to everything they can access.

[1] https://www.ntu.edu.sg/ntc/support-from-the-entrepreneurship-ecosystem/developing-the-technopreneurship-ecosystem/internet-of-things-(iot)-security-reference-architecture

2.3 Network separation

Figure C-1 shows the system architecture of an example case study, which will help to demonstrate the guidance provided by Table C-1. Note that in the case of a Smart Building scenario, it is not uncommon to find a BMS. In this case, it is appropriate to include the BMS in between the IoT Edge Gateway and the device layer. There can be more granularity in terms of zones definition but for the purpose of the illustration of the case study, we will define the zones as described in Figure C-1.

Although not modeled in this case study, the reader may include considerations, for smart buildings with decentralized IoT systems on separate networks. Doing so is often useful to curtail further compromises if a compromised device is detected early in a particular segment. Again, for the purpose of the illustration of the case study, we will define the zones as described in Figure C-1.

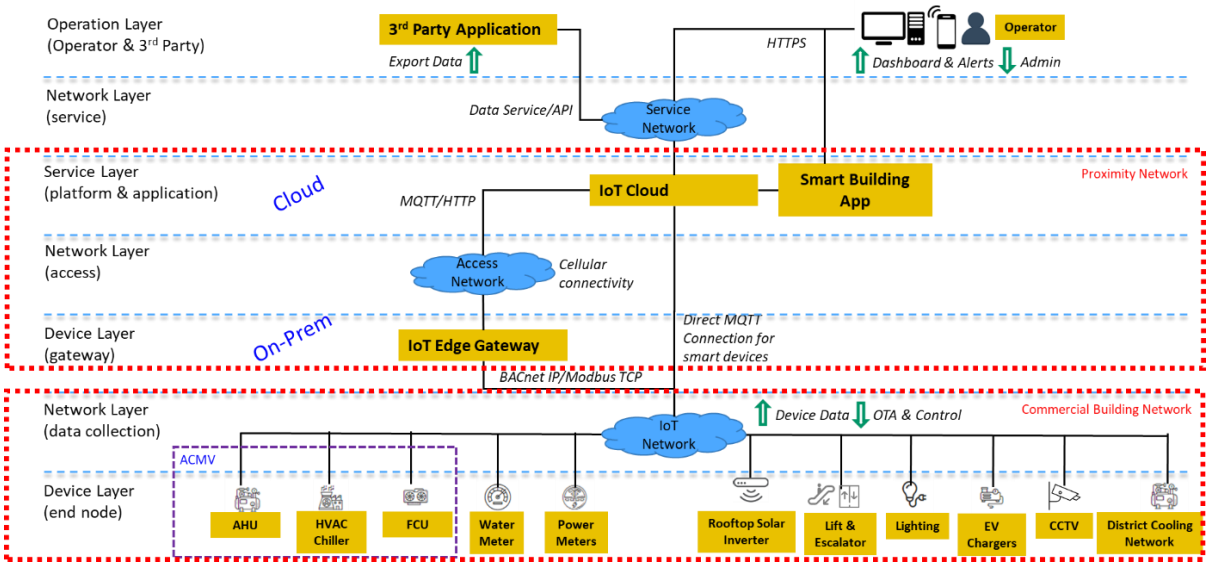

Figure C-1: General architecture of Smart Building

Through the threat model, assets under the TOP are being identified. Table C-2 determines the security needs of the assets with respect to the CIA triad. It helps to prioritise which assets and which aspects to secure.

Note that several end devices may be interconnected to the IoT Edge Gateway. This may include, but not limited to, electrical monitoring and control devices, autonomous robots, access management system (e.g. physical gantry and card access), smart pump systems, mechanical ventilation systems and centralized/district level cooling systems.

For illustration, we will simply pick a few end devices to support the case study.

Legend: H = High, M = Moderate, L = Low

Assets	Confidentiality	Integrity	Availability	Rationale
IoT Cloud	H	H	H	Confidentiality is high because of customers' information on the cloud and access to the backend. Integrity is high to safeguard commands invocation, and availability needs to be high to maintain the ability to access and control the backend.
IoT Edge Gateway	H	H	H	Confidentiality is high because of customers' information on the Edge

				Gateway and access to the cloud. Integrity is high to safeguard commands invocation, and availability needs to be high to maintainability access and control the backend at all times.
Device – Water Meter	L	H	H	Confidentiality is not an issue, but rather readings must be true, and availability must be present.
Device – Power Meter	L	H	H	Confidentiality is not an issue, but rather readings must be true, and availability must be present.
Device - Rooftop Solar Inverter	L	H	H	Confidentiality is not an issue, but controls must not be modified, and availability must be present.
Device – Lift and Escalator	L	H	M	Confidentiality is not an issue, but controls and readings must not be modified. Availability may/may not be an issue because downtime can be afforded.

Table C-2: Security needs of assets

Table C-3 determines the security needs of the data flows between assets with respect to the CIA triad. It provides information on which data flows required attention and the type of security required.

Legend: H = High, M = Moderate, L = Low

Data flow	Confidentiality	Integrity	Availability	Rationale
Devices -> IoT Edge Gateway	M	H	H	Raw sensor data collection requires high integrity and availability. Confidentiality is not as important for raw data. Integrity and availability are high to ensure the information communicated is correct and available.
IoT Edge Gateway -> IoT Cloud	H	H	H	Confidentiality is high as communication maybe over the Internet. Integrity and availability are high to ensure the information communicated is correct and available.
IoT Cloud -> 3rd party application	H	H	M	Analysis of data by 3rd party applications requires high data integrity. Confidentiality is high to protect the data collected. Availability may/may not be an issue because downtime can be afforded.
IoT Cloud -> Operator	H	H	H	Data analysis reporting requires high confidentiality, integrity, and availability for operators/users.
Operator -> IoT Cloud -> IoT Edge Gateway -> Devices	H	H	M	Management of devices by users requires high confidentiality and integrity. Some downtime can be afforded.
3rd party Application -> IoT Cloud -> IoT Edge Gateway -> Devices	H	H	M	Management of devices by 3rd party applications requires high confidentiality and integrity. Some downtime can be afforded.

Table C-3: Security needs of data flows

2.4 Extending assets' CIA assessment to OT's safety, resilience and reliability

Equally important to the security well-being of a Smart Building eco-system are the 3 attributes of OT, i.e. Safety, Resilience and Reliability. This is especially important if the device layer includes physical systems such as lift and escalator in the case study illustrated in Figure C-1. For more information, please refer to Annex A ("Foundational Concepts").

Safety refers to the ability of the asset to operate in a safe manner that will not be detrimental to the safety of users at all times. A very classic example is that of a smart escalator. It should fail gracefully in a case of a fault and not be able to cause any harm to the vulnerable.

Resilience refers to the asset's ability to maintain functioning state while reliability refers to the ability of the asset to perform a specific function as it is expected to. In the same manner, Table C-3 can be extended to identify the security needs to ensure safety, resilience as well as reliability of the assets.

To focus and illustrate how the security requirements can be defined for Smart Building, we will focus on the CIA triad.

3. Define the security problem

This section illustrates the guidance provided by item-2 of Table C-1, which helps define the security problem for this case study.

Table C-4 identifies the concerns that contribute to system accessibility and system susceptibility for assets under TOP. It provides the information (threats, vulnerabilities, operating environments, assumptions, etc.) required to define the security problem.

Assets	System accessibility	System susceptibility
IoT Cloud	The following attack surfaces are relevant for the IoT Cloud: API calls, HTTPS traffic, storage SW, memory, VM, OS, firmware, middleware, server software The IoT Cloud is hosted in the cloud and may be accessible from the Internet. All stages of the system lifecycle need to be considered.	OWASP Top 10 Application Security Risks Scan for relevant known vulnerabilities from prominent vulnerability repositories such as https://www.cve.org/
IoT Edge Gateway	The following attack surfaces are relevant for IoT Edge Gateway: MQTT/HTTP traffic, storage SW and HW, memory, OS, firmware, communication ports, WIFI, 4G IoT Edge Gateway is hosted in the commercial building network and may be accessible via the Internet. All stages of the device lifecycle need to be considered.	OWASP IoT Attack Surface Areas and OWASP IoT Vulnerabilities Scan for relevant known vulnerabilities from prominent vulnerability repositories such as https://www.cve.org/
Device – Water Meter	The following attack surfaces are relevant for Water Meter: Modbus traffic, firmware Water Meter is hosted in the commercial building network and is accessible from the IoT Edge Gateway (or BMS connected in between) only. All stages of the device lifecycle need to be considered.	OWASP IoT Attack Surface Areas and OWASP IoT Vulnerabilities Scan for relevant known vulnerabilities from prominent vulnerability repositories such as https://www.cve.org/
Device – Power Meter	Similar concerns as Water Meter	Similar concerns as Water Meter
Device – Rooftop Solar Inverter	Similar concerns as Water Meter	Similar concerns as Water Meter
Device – Lift and Escalator	Similar concerns as Water Meter	Similar concerns as Water Meter

Table C-4: System accessibility and susceptibility

4. Conduct risk assessment

This section illustrates the guidance provided by item-3 of Table C-1, which guides how risk assessment is conducted for this case study.

Table C-5 demonstrates a risk assessment of system accessibility and system susceptibility for each asset. This is for illustration purposes only as risks are context-sensitive to the real world. In the table, risks are classified as high, moderate, and low, according to the given rationale.

Legend: H = High, M = Moderate, L = Low

Assets	System accessibility (attack surfaces, operating environments, lifecycles)	System susceptibility (known vulnerabilities, STRIDE)	Rationales
IoT Cloud	H	H	System accessibility is high because it is hosted in the public cloud. System susceptibility is high because it may contain some vulnerabilities. Refer to OWASP Top 10 Application Security Risks
IoT Edge Gateway	M	H	System accessibility is medium because it "sits" within the CBN. System susceptibility is high because it may contain some vulnerabilities and can be connected to the IoT Cloud. Refer to OWASP IoT Attack Surface areas.
Device – Water Meter	M	M	System accessibility and susceptibility of water meters are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.
Device – Power Meter	M	M	System accessibility and susceptibility of the power meter are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.
Device – Rooftop Solar Inverter	M	M	System accessibility and susceptibility of the rooftop solar inverter are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.
Device – Lift and Escalator	M	M	System accessibility and susceptibility of lift and escalator are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.

Table C-5: Assessment of system accessibility and susceptibility

It is worth mentioning that some devices may contain multiple units, which may or may not reduce its susceptibility and impact to the system. For example, in Table C-5, the system susceptibility of the rooftop solar inverter is estimated to be moderate, which may be reduced to low, if another inverter is connected in another separated isolated zone, which is not illustrated in this case study.

Table C-6 demonstrates a risk assessment of attacker capability for each asset, for illustrative purposes only. It determines a list of attacker types (script kiddies, criminals, hacktivists, terrorists, state-sponsored, etc.) that have an interest in the assets. The risks are defined by the capability of the most sophisticated attacker in the list, which can compromise the assets. Similarly, risks are classified as high, moderate, and low, according to the given rationale.

Legend: H = High, M = Moderate, L = Low

Assets	Attacker capability	Rationale
IoT Cloud	H	The asset is valuable to a range of attackers (script kiddies, criminals, hacktivists, terrorists, state-sponsored), including some with high capabilities and resources.
IoT Edge Gateway	H	The asset is valuable to a range of attackers (script kiddies, criminals, hacktivists, terrorists, state-sponsored), including some with high capabilities and resources.
Device – Water Meter	L	The asset is valuable to script kiddies only.
Device – Power Meter	L	The asset is valuable to script kiddies only.
Device – Rooftop Solar Inverter	M	The asset is valuable to script kiddies, criminals, and hacktivists with moderate capabilities and resources.
Device – Lift and Escalator	M	The asset is valuable to script kiddies, criminals, and hacktivists with moderate capabilities and resources.

Table C-6: Assessment of attacker capability

Table C-7 determines the priority for mitigation of the threats for each asset, with holistic considerations for risks of system accessibility, system susceptibility, and attacker capability, for illustration purposes only. Our case study will only elaborate on the high priority items for mitigation in subsequent sections for illustrative purposes.

Legend: H = High, M = Moderate, L = Low

Assets	System accessibility (attack surfaces, operating environments, lifecycles)	System susceptibility (known vulnerabilities, STRIDE)	Attacker capability	Priority
IoT Cloud	H	H	H	H
IoT Edge Gateway	M	H	H	H
Device – Water Meter	M	M	L	
Device – Power Meter	M	M	L	
Device – Rooftop Solar Inverter	M	M	M	
Device – Lift and Escalator	M	M	M	

Table C-7: Assessment of priority

5. Determine the security objectives

This section illustrates the guidance provided by item-4 of Table C-1, which guides how security objectives are determined for this case study.

Table C-8 demonstrates the definition of security objectives for the threat modelling process. For illustrative purposes, we limit the assets to those identified as high priority in Table C-7. The needs of the CIA triad for the assets are identified in Table C-2 and defined in this table as principal objectives to safeguard. This table also identified a list of possible security objectives.

Legend: H = High, M = Moderate, L = Low

Assets	Confidentiality	Integrity	Availability	Security objectives
IoT Cloud	H	H	H	1. Ensure confidentiality of sensitive data 2. Provide proper access control 3. Ensure integrity of the system 4. Prevent multitenancy from compromising security 5. Ensure confidentiality and integrity of data and commands 6. Resilience against DOS
IoT Edge Gateway	H	H	H	1. Ensure confidentiality of sensitive data 2. Provide proper access control 3. Ensure integrity of the system 4. Fail safely 5. Ensure confidentiality and integrity of data and commands 7. Resilience against DOS

Table C-8: Security objectives

From the availability perspective, there may be dependencies between system components in the building but is not illustrated in this case study. In addition, Table C-3 guides the identification of security requirements under network protection and data protection categories.

6. Define the security requirements

This section illustrates the guidance provided by item-5 of Table C-1, which helps define the security requirements for this case study. It should be noted that the checklist is only a template of common security considerations. Users must determine the appropriateness and applicability of the checklist items to add on, remove, and/or adjust according to the uses and business needs. This checklist alone is not a substitute for formal evaluation and certification.

Table C-9 suggests the application of the vendor disclosure checklist for assets highlighted in Table C-8. In practice, the technology solution provider would have to further elaborate on how they address the security requirements listed.

Vendor disclosure checklist	**Y (yes) / N (no) / NA (not applicable)**	**Supporting materials**
1. Cryptographic support		
CHECK-CS-01: Do your devices and system employ industry-accepted cryptography and best practices? Examples include the use of: a) Accepted algorithms and their correct implementation and application. b) Accepted entropy sources and approved random number generator(s). c) Sufficient key length. d) Sufficient crypto-period. e) Use of updatable cryptography.	Y	The strength of cryptography is fundamental to safeguard the objectives of confidentiality and integrity. In particular, cryptography must be approved for the lifetime of the devices. Recommended for IoT Cloud and IoT Edge Gateway to maintain confidentiality and integrity of the information.
CHECK-CS-02: Do you define and implement proper key management practices (generation, exchange, storage, use, destruction and replacement) accordingly to industry-accepted best practices and recommendations?	Y	Proper key management is required to prevent the disclosure of keys through the system/device lifecycles. Recommended for IoT Cloud and IoT Edge Gateway to ensure that keys used to establish confidentiality and integrity are supported with proper key management.
2. Security function protection		
CHECK-FP-01: Do you employ and properly implement a trusted computing base (TCB) according to industry-accepted recommendations and best practices? The TCB should include: a) policies; b) hardware; c) firmware; d) operating systems; e) virtualisation; f) software;	Y	Recommended for: IoT Cloud and IoT Edge Gateway

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
g) basic input/output system; h) system services; i) device drivers; j) protocols; k) RoT; and l) trust anchor.		
CHECK-FP-02: Do you establish RoT for your devices and system, according to industry-accepted best practices and recommendations?	Y	To safeguard the confidentiality and integrity of sensitive data (e.g., keys) at rest and in use. Recommended for IoT Cloud and IoT Edge Gateway
CHECK-FP-03: Do you employ secure boot mechanisms to protect and verify software according to industry-accepted best practices and recommendations? If an unauthorised change to the software is detected, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.	Y	To safeguard the integrity of the boot process. Recommended for IoT Edge Gateway since it is an on-prem physical device with the necessary resources to support Secure Boot.
CHECK-FP-04: Do you protect security data elements, such as credentials, keys, and tokens, from unauthorised disclosure and modification according to industry-accepted best practices and recommendations?	Y	Recommended for: IoT Cloud and IoT Edge Gateway
3. Identification and authentication		
CHECK-IA-01: Do you establish unique, non-modifiable, and verifiable identities for IoT entities (i.e., users, platforms, gateways, devices)?	Y	To safeguard the integrity of identification to mitigate threats of spoofing. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-IA-02: Do you securely provision and manage the credentials of IoT entities (i.e., users, platforms, gateways, devices)? For example, by being salted, hashed, or encrypted.	Y	
CHECK-IA-03: Do you employ secure authentication mechanisms according to industry-accepted best practices and recommendations?	Y	
CHECK-IA-04: Do you establish mutual authentication before any interactions between clients (users, devices, gateways, applications) and servers?	Y	To safeguard the integrity of connections to prevent unauthorized remote access. Recommended for IoT Cloud and IoT Edge Gateway
4. Network protection		
CHECK-NP-01: Do you employ proven transport protocols and recommended network services with properly activated security controls?	Y	To safeguard the confidentiality and integrity of the payloads. Recommended for IoT Cloud and IoT Edge Gateway

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
Examples of best practices for transport protocols include using the following: a) TLS for TCP payloads. b) DTLS for UDP payloads. c) TLS for MQTT. d) HTTPS.		
CHECK-NP-02: Do you establish secure connectivity according to industry-accepted best practices and recommendations? Examples include: a) Use of VPN. b) Use of private mobile access point names (APN) from telecommunication operators when using a public mobile carrier network. c) Use of secure DNS to prevent DNS spoofing. d) Use of traffic filtering based on type, port, and destination. e) Use of mutual TLS (mTLS). f) Use whitelisting to establish or deny connections from non-trusted sources. Additionally, IETF Request for Comments (RFC) 8520 Manufacturer Usage Description (MUD) can be a mechanism for devices to provide this information to the network.	Y	Applicable to safeguard the data flows highlighted in Table C.3 Recommended for IoT Cloud and IoT Edge Gateway For cellular communications (i.e. 4G, NB-IoT), certain security enhancement considerations include providing a private APN provisioned together with dedicated VPN channel between telecommunication's network infrastructure to cloud platform infrastructure. Inter-device connectivity should be disabled at the telecommunications level to prevent malicious attack at one location to gain access to other location through cellular network. Static IPs can also be assigned for each device over cellular communications to identify each device. It is also worth mentioning the controls are also applicable to wireless protocols that are increasingly been used in building management system (BMS).
CHECK-NP-03: Do you employ segregation of communication channels for endpoints with varying trust-levels according to industry-accepted best practices and recommendations? Examples include using VLAN, firewalls for DMZ, unidirectional security gateway, network segmentation or micro-segmentation, and physical isolation.	Y	Applicable to safeguard the data flows highlighted in Table C.3 Recommended for IoT Cloud and IoT Edge Gateway Commercial Building Network is physically isolated from the enterprise network. DMZ is designed to restrict external access without exposing the internal network and system. The network traffic is safeguarded by web proxy and firewall with strict rules. Consideration can also be made to segregate management network, physical security network, building control and instrumentation network and voice and data network, if it exists and wherever applies.

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
CHECK-NP-04: Do you implement network monitoring and access control according to organisational information flow control policy? Examples of access control include: a) Use of secure authorisation mechanisms for each connection to join a network. b) Use of secure de-authorisation mechanisms for each connection to disconnect and forget a network.	Y	Proper access control is required to limit access to the system networks. Recommended for IoT Cloud and IoT Edge Gateway Network access controls should also be in place to prevent unauthorised devices from connecting.
5. Data protection		
CHECK-DP-01: Do you protect data in transit, in use, and at rest, from unauthorised disclosure and modification according to industry-accepted best practices and recommendations? Examples of data include, but are not limited to, security data, personal data, sensing data, metadata, event logs, software, and their configurations.	Y	To safeguard the confidentiality and integrity of sensitive data. Sensitive data includes cryptographic keys and user credentials. IoT Edge communicates with IoT Cloud communicates TLS protected data tunnel. Full disk encryption enabled for both IoT Cloud and IoT Edge Gateway. Recommended for IoT Cloud and IoT Edge Gateway This is optional for devices such as Lift and Escalator and Rooftop Solar Inverter and where the protocols can support.
CHECK-DP-02: Do you provide evidence and means to attest the authenticity and integrity of data-in-transit, data-in-use, and data-at-rest according to industry-accepted best practices and recommendations? Examples include using hashing and digital signatures. These data include sensing data, software, and its configurations.	Y	To safeguard the software and firmware in IoT Cloud, IoT Edge Gateway, including updates. Features such as platform code integrity (where available can be enabled for IoT Cloud while secure boot features can be enabled for IoT Edge Gateway. Recommended for IoT Cloud and IoT Edge Gateway
CHECK-DP-03: Do you implement input validation to safeguard input data, which includes commands and sensing data? Examples of input validation include: a) Validating incoming content types. b) Validating response types. c) Validating the HTTP methods against authorisation credentials. d) Whitelisting allowable HTTP methods. e) Defining the acceptable character set, e.g., Unicode Transformation Format-8 (UTF-8). f) Validating that input characters are acceptable. g) Encoding/escaping input and output.	Y	To safeguard the data in IoT Cloud, IoT Edge Gateway, and devices, including inputs and commands. API endpoints should be TLS protected and authentication enforced. Data inputs should be properly validated along. Recommended for IoT Cloud and IoT Edge Gateway This may apply to Lift and Escalator, and Rooftop Solar Inverter devices and where the protocols can support.

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
h) Checking for anomalies.		
CHECK-DP-04: Do you enforce access control to detect and prevent unauthorised data access and data exfiltration? Additionally, do you verify and filter independently data output, including commands and processed sensing data?	Y	To safeguard aggregated data in IoT Cloud and IoT Edge Gateway from unauthorized access. Both web interface and API endpoints should be TLS protected and authentication enforced. Data inputs should be properly validated along. Recommended for IoT Cloud and IoT Edge Gateway
6. Access protection		
CHECK-AP-01: Do you employ session management to secure interactions for different clients according to industry-accepted best practices and recommendations? Examples include: a) Verify and protect the integrity of sessions. b) Restrict access by client types. c) Restrict data transfer and file transfer by clients.	Y	
CHECK-AP-02: Do you implement lock-out mechanism to protect against repeated unauthorised attempts by any user (human, software or device)? Examples of mechanisms include delay in between login attempts, lock-out for repeated unauthorised attempts, and forced reauthorisation.	Y	To safeguard IoT Cloud and IoT Edge Gateway from unauthorized access, both locally and remotely, including physical access. Recommended for IoT Cloud and IoT Edge Gateway
CHECK-AP-03: Do you employ multi-factor authentication (for user access) and timely notifications?	Y	To safeguard impactful operations by requiring a higher level of authentication. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-AP-04: Do you enforce physical and remote access restriction to safeguard against unauthorised access to assets, equipment, user devices, removable media, and interfaces?	Y	To safeguard against physical access to system/device interfaces. Recommended for IoT Cloud and IoT Edge Gateway
CHECK-AP-05: Do you employ anti-tampering mechanisms to detect, prevent, make evident and/or respond to physical attacks?	Y	To prevent and detect physical tampering. Recommended for: IoT Edge Gateway To support and enhance physical security, the use of physical lock and tamper resistant enclosure can be considered.
7. Security audit		
CHECK-AU-01: Do you synchronise your clocks to authoritative time sources to provide timestamps for audit records?	Y	Recommended for: IoT Cloud and IoT Edge Gateway

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
CHECK-AU-02: Do you record security events to facilitate monitoring, analysis, and timely alerts raised (e.g., who does what and when) regarding activities performed? Examples of security events include the following: a) User logins, logouts, and unsuccessful authentication attempts. b) Connection, disconnection attempts and unsuccessful connection attempts. c) Unsuccessful authorisation attempts. d) Access to sensitive data. e) Import and export of data from removable media. f) Any change in access privileges. g) Creation, modification, and deletion of data by user. h) Remote operations. i) Security update failures. j) Physical access attempts where possible. k) Emergency access where possible. l) Configuration changes.	Y	To safeguard the system by having the ability to detect and analyze when attacks are realised. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-AU-03: Do you protect audit records from unauthorised operations (create, read, update and delete)? Do you allocate sufficient record storage, and raise timely alerts before records are overwritten?	Y	To safeguard the confidentiality and integrity of audit logs. Recommended for: IoT Cloud and IoT Edge Gateway
8. Security management		
CHECK-SM-01: Do you employ strong credential management according to industry-accepted best practices and recommendations? Examples include: a) Enforcing a strong password policy. b) Enforcing no default passwords. c) Specifying password expiration periods. d) Ensuring that password recovery and reset mechanisms are secure. e) Randomising pre-loaded login credentials. f) Use of FIDO2 security tokens.	Y	To safeguard access to IoT Platform Recommended for: IoT Cloud and IoT Edge Gateway It is worth mentioning in certain cases/project deployment, disabling password login and using certificate-based authentication is implemented.
CHECK-SM-02: Do you employ access control policies and mechanisms to manage system, networks, and devices according to industry-accepted best practices and recommendations. Examples include: a) Use of attribute-based access control (ABAC) or role-based access control (RBAC).	Y	To safeguard the administration functions of IoT Platform. Recommended for IoT Cloud and IoT Edge Gateway

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
b) Enforce a least privilege policy. c) Restrict and manage privilege access rights.		
CHECK-SM-03: Do you employ protection mechanisms to detect and mitigate the effects of unauthorised and malicious software and hardware? Examples include the following: a) Ensuring file integrity using cryptographic hash. b) Baselining normal behaviour. c) Detecting unauthorised software. d) Monitoring devices and traffic flows. e) Scanning software and backup images. f) Prohibiting insecure bootloaders.	Y	To safeguard the integrity of the software. It will be useful to add if you have/deployed any threat detection/monitoring services, for example, endpoint detection and response? Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-SM-04: Do you employ protection mechanisms to secure the remote management of devices and gateways? Examples include: a) Supporting secure OTA updates of device applications and configurations. b) Supporting software and/or firmware updates using secure processes and cryptographically secure methods. c) Supporting platform integrity checking such as the measured boot mechanism or verifying the firmware integrity. d) Restricting remote management to secure networks.	Y	To safeguard the remote management function of Edge and devices, including remote updates. Recommended for: IoT Edge Gateway
9. Resiliency support		
CHECK-RS-01: Do you employ mechanisms to support integrity self-test, error detection, correction for critical functions, and return to a safe state? For example, leaving the device in a state that minimises potential for harm during an unexpected interruption of an update, taking into account the risks of the IoT device not functioning as expected.	Y	To safeguard the integrity and availability of the system, devices are monitored and attested periodically. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-RS-02: Do you implement measures to protect against failures from outages, resource exhaustion, and/or malicious DoS attacks? Examples include the following: a) Monitoring to ensure that cloud resources are sufficient to sustain services. b) Detecting resource exhaustion for early preventive or corrective actions. c) Controlling the execution of resource-intensive software. d) Enforcing power thresholds. e) Limiting the number of concurrent sessions.	Y	To safeguard the availability of the system by detecting and preventing resource exhaustion. Recommended for: IoT Cloud

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
f) Having the capacity to operate during resource outages (e.g., power, network) or the ability to operate in a degraded mode.		
CHECK-RS-03: Do you employ mechanisms to periodically back up system data, including their settings? Do you conduct disaster recovery exercises to verify the backup and recovery mechanisms?	Y	To safeguard the availability of the system, ensuring the ability to recover from a compromised state. Recommended for: IoT Cloud
CHECK-RS-04: Do you maintain or degrade the IoT system and devices to a safe and expected state on encountering errors/failures? Do you provide timely alerts, with sufficient information, to relevant authorised users to support effective remediation?	Y	
10. Lifecycle support		
CHECK-LP-01: Do you conduct threat modelling to identify, analyse, assess, and document threats to the IoT system?	Y	To understand and focus limited resources on what needs protection. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-LP-02: Do you design and develop your IoT solution according to industry-accepted secure systems engineering approaches, best practices, and recommendations?	Y	To employ the baseline recommendations for implementation and operational phases, as defined by this guide. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-LP-03: Do you construct and maintain your IoT solution using components with no known unmitigated vulnerabilities?	Y	To safeguard the supply chain of system components. In this case, maintain a list of suppliers for the components. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-LP-04: Do you identify and manage supply chain risks with defined processes and procedures, including risks from the use of opensource software?	Y	
CHECK-LP-05: Do you harden your IoT solution before putting it into operation? Examples of system hardening include the following: a) Removing all backdoors; b) Removing all debug codes from the released version; c) Enabling secure configuration and settings; d) Removing unnecessary software and services; e) Removing or tamper-covered JTAG;	Y	Employ the “security by defaults” principle and ensure the system is configured securely before operation. Recommended for: IoT Cloud and IoT Edge Gateway To minimize potential attack surfaces, if the product has unused features such as DHCP or Wi-Fi, it is also suggested to disable them.

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
f) Removing unnecessary serial ports and other ports before deployment; g) Appropriate hardening of VM host, including disabling memory sharing between VMs; h) Removing default and hardcoded passwords; and i) Removing unused networks and interfaces.		
CHECK-LP-06: Do you provide, communicate, and update security information in a timely manner? Examples of security information include the following: a) Terms of service. b) Support policies. c) Security guidelines, instructions, and educational materials. d) Security notifications and updates. e) Instructions for device/media sanitisation. f) Phase out plan and end-of-life notifications.	Y	Ensure that there is an ownership and commitment to providing security information promptly so that known vulnerabilities can be mitigated. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-LP-07: Do you maintain an information inventory of system components and assets throughout the IoT system operation? Examples include the following: a) Supplier information. b) Hardware models and versions, including physical locations. c) Software and firmware versions, including applied patches and updates. d) Configurations and settings, including IP addresses, ports, protocols, and services. e) Maintenance status.	Y	Employ the "accountability" principle to keep track that only authorized and patched devices are in use. Evidence of device OS update and patching be included in the audit. In support of this activity, it is also useful to keep an inventory of the software bill of materials (SBOM), including the operating system so as to keep track and identify the vulnerabilities associated with them. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-LP-08: Do you conduct penetration testing and vulnerability scanning as part of the security assessment, before commissioning, periodically, and before each major release? Do you enable and test all optional, non-default features of the IoT devices for security?	Y	Conduct periodic testing on the integrated system to detect vulnerabilities due to improper integration. For example, by going through Cyber Security Agency (CSA) Cybersecurity Labelling Scheme (CLS). Please send any enquiries on the Cybersecurity Labelling Scheme to certification@csa.gov.sg. Managing and maintenance of device and system security as part of building management audit Verification of the device could cover Printed circuit board (PCB) level.

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
		Recommended for: IoT Cloud and IoT Edge Gateway and devices.
CHECK-LP-09: Do you establish vulnerability management and disclosure according to industry-accepted best practices and recommendations? Examples include the following: a) Ensuring the supply chain's capability to provide upgrades and patches. b) Providing vulnerability disclosure and processes to track and respond promptly. c) Providing firmware and software patches/updates for discovered vulnerabilities in a timely manner. d) Employing proper change management processes to manage security patches or updates. e) Notifying and/or allowing users to approve/reject updates, patches, and changes to user settings, where appropriate. f) Disclosing minimum support period.	Y	Build resilience by establishing ownership and standard operating procedures (SOPs) to disclosure, manage and resolve the vulnerability. Recommended for: IoT Cloud and IoT Edge Gateway Further to vulnerability disclosure, it is also recommended the vendor implement/establish both a threat & vulnerability management system as well as cybersecurity incident and response plan with playbooks and workflow process. This will help the organization to respond to cybersecurity incidents in a more organized and responsive manner.
CHECK-LP-10: Do you manage identities, certificates, and secrets securely throughout their lifecycles, including creation, provisioning, renewal, and revocation?	Y	By the “accountability” principle, the identities and secrets should be safeguarded throughout their lifecycles. Recommended for: IoT Cloud and IoT Edge Gateway
CHECK-LP-11: Do you employ mechanisms for the proper disposal of devices and systems, and for resetting or sanitising sensitive data by authorised users when feasible, according to industrial best practices? Examples include the option to factory reset, erase and zeroise both security data and user data.	Y	The “accountability” principle should safeguard sensitive data throughout the system/device’s lifecycles. Recommended for: IoT Cloud and IoT Edge Gateway

Table C-9: Usage of vendor disclosure checklist

7. Additional resources

Readers, who are also interested in the implementations of specific vendors, can refer to the following non-exhaustive list of online resources:

- “Case Study on Smart Facilities Security through Envision EnOS” whitepaper by Envision: https://developer.envisioniot.com/contactus/

- “Building resilience, through visibility.” whitepaper by Honeywell: https://buildings.honeywell.com/content/dam/hbtbt/en/documents/downloads/Cybersecurity%20-%20Building%20Resilience,%20Through%20Visibility.pdf

- “A Practical Framework for Cyber Secure, Cloud Connected Smart Building Control Systems“ whitepaper by Schneider Electric: https://download.schneider-electric.com/files?p_enDocType=Brochure&p_File_Name=998-20437895+A+Practical+Framework+for+Cyber+Secure+Cloud+Connected+Smart+Building+Control+Systems+-+White+Paper.pdf