Guidelines

Internet of Things (IoT) Cyber Security Guide

IMDA IoT Cyber Security Guide
Version 1, Jan 2019

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

Contents

1 Introduction ... 3
2 Scope ... 4
3 References ... 5
4 Terms and definitions ... 5
5 Abbreviations and acronyms ... 5
6 Baseline recommendations for the implementation phase ... 7
6.1 Introduction ... 7
6.2 Principle 1: Secure by default ... 7
6.2.1 Employ strong cryptography ... 7
6.2.2 Protect impactful system data ... 7
6.3 Principle 2: Rigour in defence ... 7
6.3.1 Conduct threat modelling ... 7
6.3.2 Establish hardware Root-of-Trust ... 8
6.3.3 Employ secure versions of transport protocols ... 8
6.4 Principle 3: Accountability ... 8
6.4.1 Enforce proper access controls ... 8
6.5 Principle 4: Resiliency ... 8
6.5.1 Prepare for and protect against attacks ... 8
7 Baseline recommendations for operational phase ... 9
7.1 Introduction ... 9
7.2 Principle 1: Secure by default ... 9
7.2.1 Use strong passwords ... 9
7.3 Principle 2: Rigour in defence ... 9
7.3.1 Segregate the IoT and enterprise networks ... 9
7.4 Principle 3: Accountability ... 9
7.4.1 Establish proper device management ... 9
7.5 Principle 4: Resilience ... 10
7.5.1 Recovery from attacks ... 10
7.5.2 Conduct periodic assessments ... 10
8 Threat modelling checklist ... 11
9 Vendor disclosure checklist ... 12
10 Bibliography ... 17

Annex A Foundational Concepts
Annex B Case Study on Home Control System

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

IMDA IoT Cyber Security Guide

1 Introduction

The Internet of Things (IoT) brings together the physical environment and a wide range of objects such that they can interact with one another seamlessly through the use of Information and Communication (ICT) systems. It encompasses many supporting technologies such as sensing and control technologies, networking technology, information technology and software technology. Together, all these technologies enable sensors, actuators, middleware, data and communication networks, and applications, to interconnect to form an IoT ecosystem.

The significance of the economic impact of IoT is well-documented and increasingly being felt, with the increasing adoption of IoT solutions among consumers, enterprises and governments. Examples include connected wearables, smart homes, smart buildings, connected vehicles, video surveillance and analytics.

As people and devices become more connected, issues relating to the safeguarding of data and management of cyber security threats become increasingly important. IoT devices can collect significant amounts of information about their users and their environment, including personally identifiable, commercially confidential and/or sensitive data. For example, wearables can track an individual's steps, heart rate and sleep patterns while commercial sensors and actuators may expose enterprise control systems to the risk of data exfiltration, or even worse attacks. Measures will need to be taken to protect this large and growing volume of sensors and sensitive data.

Unfortunately, early IoT devices have several vulnerabilities which may be easily exploited, making them easy targets for cyber security attacks. For instance, compromised devices can be controlled by a botnet and be made to participate in Distributed Denial-of-Service (DDoS) attacks on other organisations.

Security has been consistently ranked as the top concern inhibiting user adoption. On the other hand, industry has provided feedback that conforming to existing standards not designed with IoT in mind, is time-consuming, costly and impractical for the dynamic and evolving technologies and applications of IoT.

Protecting organisations and individuals from rising cyber threats is a national priority as well as an area of economic opportunity. It is integral to ensuring that Singapore remains cyber secure in a digital economy, with a set of trusted infrastructure to support our Smart Nation initiatives.

Similar to any system, an IoT system is as secure as its weakest link. It is thus important to ensure that proper security considerations and measures are put in place for both the implementation and operational stages of the deployment of any IoT system. This document aims to provide guidance to users and enterprises when procuring, deploying and operating IoT devices/systems, while enabling solution providers to verify the security posture of their solutions, by providing practical guidelines that include baseline recommendations, foundational concepts and checklists. A risk-based and system-oriented approach is taken to identify and mitigate threats to IoT solutions. Enterprise users and their vendors are guided to work together to secure their IoT systems over their lifecycles.

2 Scope

This document serves as a practical guide for enterprise users intending to deploy IoT solutions as well as for their vendors, providing baseline recommendations, foundational concepts and checklists, focusing on the security aspects for the acquisition, development, operations and maintenance of IoT systems.

It builds on the concepts introduced in ITSC TR 64: “Guidelines for IoT security for smart nation” and provides further details on the implementation of IoT security through case studies.

This guide can be used by:

- **IoT developers** who want to design, develop and deploy secure IoT products and systems. Examples of developers include solution architects, programmers, manufacturers and system integrators.
- **IoT providers** who need to roll-out, configure, operate, maintain and de-commission IoT systems securely. Examples of providers include network operators, platform providers, data analysts and service delivery managers.
- **IoT users** who want to procure and interact with IoT systems. For system interactions, IoT users can by either human or software agents.

With respect to the lifecycles of IoT systems, IoT developers are mainly involved in the implementation phase, which covers the design, develop, deploy, integrate and test stages, while IoT providers are involved in the operational phase, which covers the operate, support, maintain, upgrade and retire stages. IoT users are involved in both the implementation and operational phases.

Figure 1 depicts the two areas of focus of this document with respect to ITU’s Information Security Management Framework as defined in ITU-T X.1052.

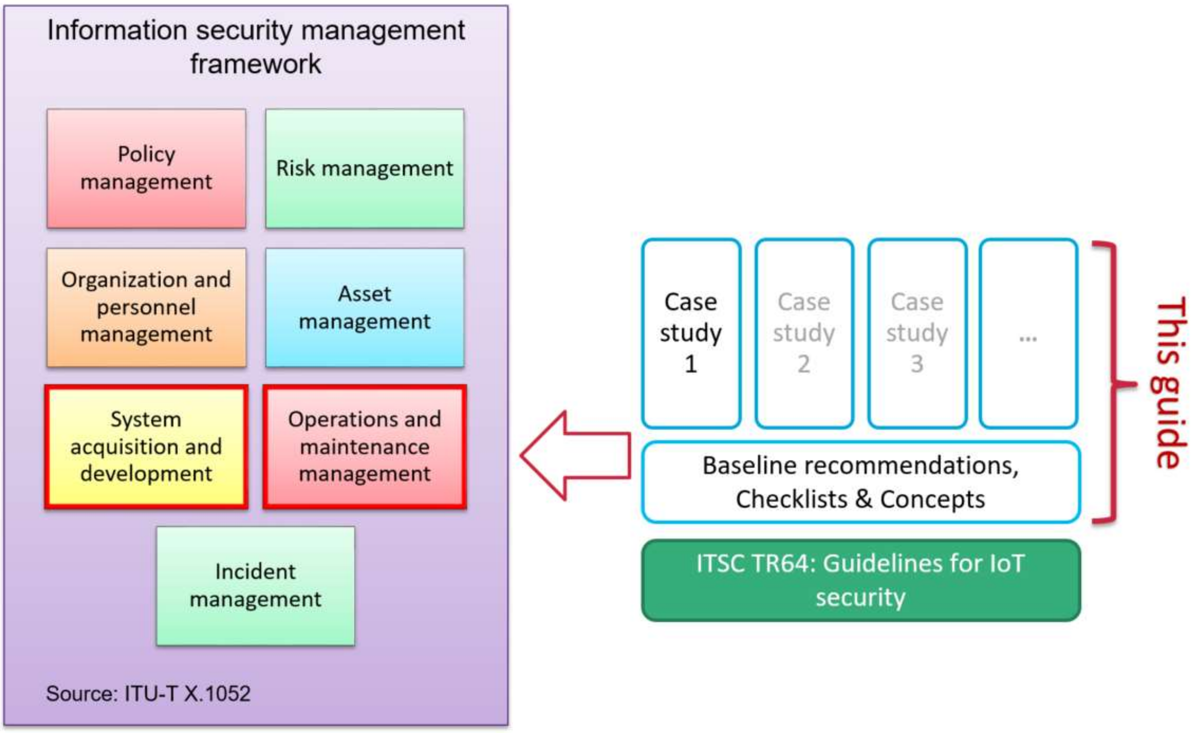

Figure 1: Overview of scope

3 References

In this document, reference has been made to the following standards. Where versions are not indicated, reference shall be based on current and valid versions of these standards published by the respective Standards Development Organisations.

[1] ITSC TR 64 : 2018 Guidelines for IoT security for smart nation

4 Terms and definitions

Access Control	Functions which include identification, authentication, authorisation and accountability.
Authentication	Act of confirming the identity of an entity.
Authorisation	Act of specifying the access permissions to a resource.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes. [ITSC TR 64]
Denial of service (DoS)	Prevention of authorised access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorised users. [ITSC TR 64]
Identification	Act of stating the identity of an entity.
Internet of Things (IoT)	System of physical and virtual entities that are connected with one another, allowing interaction anytime, anywhere. [ITSC TR 64]

5 Abbreviations and acronyms

AAA	Authentication, Authorisation, Accounting
ABAC	Attribute-Based Access Control
APN	Access Point Name
CIA	Confidentiality, Integrity, Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	De-Militarised Zone
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
HTTP	HyperText Transfer Protocol
IoT	Internet of Things
IT	Information Technology
ITSC	Information Technology Standards Committee (Singapore Standards)
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JTAG	Joint Test Action Group
MFA	Multi-Factor Authentication
MQTT	Message Queueing Telemetry Transport
OT	Operational Technology
OTA	Over-The-Air
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOP	Target Of Protection
TPM	Trusted Platform Module
TR	Technical Reference
UDP	User Datagram Protocol
UTF	Unicode Transformation Format

VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

6 Baseline recommendations for the implementation phase

6.1 Introduction

Section 6 provides a set of baseline security recommendations for IoT users and IoT developers during the implementation phase. The recommendations cover four fundamental IoT security design principles (refer to Annex A for more details):

1. Secure by default
2. Rigour in defence
3. Accountability
4. Resiliency

Individual products are used to implement a system and the system operates in the context of an organisation's processes, policies and people. The increasing levels of integration, from product to system and finally organisation require additional considerations, as the overall security posture is only as strong as its weakest links. Together, the recommendations are fundamental to safeguarding the IoT system systematically and over its lifecycle.

6.2 Principle 1: Secure by default

6.2.1 Employ strong cryptography

Strong cryptographic capabilities are the fundamental building blocks used to ensure the security of data transactions. Examples of the usage of cryptographic capabilities include digital signatures and encryption.

Recommendation: Products/solutions shall employ current and industry accepted cryptographic techniques and best practices applicable for the purposes. Examples of best practices include:

- use of approved algorithms
- sufficient key length
- use of approved random number generator(s)
- recommended crypto-period

6.2.2 Protect impactful system data

Impactful data can refer to keys, credentials, codes/firmware, personal data, inputs/commands and sensing data, etc. Access to impactful data should require assurance and/or verification that it originates from authentic sources, and be protected from tampering, modification and/or disclosure to unauthorised parties.

Recommendation: Impactful data shall be checked for authenticity, and protected from disclosure and modifications by unauthorised parties. All sensitive communications to/from IoT devices shall be encrypted.

6.3 Principle 2: Rigour in defence

6.3.1 Conduct threat modelling

Threat modelling provides a systematic approach, which helps to identify the system assets, the security needs of the system assets and the possible threats to these system assets so that the limited available resources can be focused on what needs to be protected. Threat modelling helps to minimise the exposed attack surfaces and mitigates the remaining vulnerabilities.

Recommendation: Threat modelling should be conducted as part of the design stage, based on the intended usage of IoT devices in their operating environment as proposed in the solution design.

Note: A threat modelling checklist is provided in section 8 of this document as a reference.

6.3.2 Establish hardware Root-of-Trust

Hardware Root-of-Trust is a tamper protected hardware module that stores and protects the keys of the devices so as to provide a firm foundation for other security mechanisms to build upon, hence achieving higher assurance of security.

Recommendation: Hardware Root-of-Trust should be established for key system components, which include IoT gateways and IoT platforms, as they may host sensitive data and execute impactful operations. For example, hardware Root-of-Trust can be based on a Trusted Platform Module (TPM) chip embedded in the device.

6.3.3 Employ secure versions of transport protocols

Transport protocols are used to transfer data within and between systems. It is thus important to ensure that secure versions of transport protocols are properly configured, so as to effectively protect the data in transit.

Recommendation: Proven transport protocols shall be employed with security controls properly activated. Examples of security controls of proven transport protocols include:

- use of TLS for TCP payloads
- use of DTLS for UDP payloads

6.4 Principle 3: Accountability

6.4.1 Enforce proper access controls

Access to system resources shall be controlled and managed throughout its lifecycles, minimising opportunities for malicious actors. Default passwords and weak passwords are the most commonly exploited vulnerabilities. The use of Multi-Factor Authentication (MFA) provides a higher assurance of the identity of initiators, enhances accountability and mitigates against mistakes.

Recommendation: Proper access controls, both cyber and physical, for devices, networks and data shall be enforced. Fundamental access controls include:

- Replacement of all default passwords
- Implementation of strong passwords as specified in section 7.2.1
- Enforcement of multi-factor authentication (MFA) for impactful operations
- Securing physical access to devices and their service ports

6.5 Principle 4: Resiliency

6.5.1 Prepare for and protect against attacks

Despite the implementation of the recommended measures specified in sections 6.2 to 6.4, there is still a need for mechanisms to safeguard against attempts to compromise the IoT system.

Recommendation: Firewalls and anti-malware software should be employed to prevent, detect, identify, stop and remove malicious software, especially known ones. The system should have audit log capability that records all attempts at accessing or altering system resources.

7 Baseline recommendations for operational phase

7.1 Introduction

Section 7 provides a set of baseline security recommendations for IoT users and IoT providers during the operational phase. The recommendations are organised according to the same four fundamental IoT security design principles used in section 6.

7.2 Principle 1: Secure by default

7.2.1 Use strong passwords

Weak passwords have consistently been highlighted as a top vulnerability, subjected to brute-force attacks.

Recommendation: Default passwords should be changed and strong passwords should be used. Strong passwords should preferably consist of 8 or more characters comprising a combination of letters and numbers. It is also encouraged that symbols and upper-case characters be used to enhance password strength. Multi-factor authentication should always be enabled, where possible, for access to critical information.

7.3 Principle 2: Rigour in defence

7.3.1 Segregate IoT and enterprise networks

A single compromised device can be the attack vector into your enterprise systems.

Recommendation: Network segmentation should be employed so that IoT devices belonging to different networks can be properly segregated from one another and also from other corporate enterprise systems and networks. Firewalls and malware mitigation solutions should be implemented to protect each network whenever possible.

7.4 Principle 3: Accountability

7.4.1 Establish proper device management

All connected devices are potentially exposed to malicious actors, and may be exploited, allowing cyberattacks to compromise the whole IoT system. Stolen devices can be tampered with, reverse-engineered and used against the IoT system. Outdated and unpatched firmware/software can contain known vulnerabilities that malicious actors can exploit. Hence, proper management of connected devices is critical to ensure the security of the whole system.

Recommendation: Proper management of devices, including firmware/software updates and patches, shall be established. An inventory of connected devices, software and firmware versions should be kept and up-to-date patches should be applied throughout the “Operational” lifecycle stage. Access controls, including for physical access to IoT devices, should be strictly enforced. IoT users and IoT providers should subscribe to notifications and advisories issued by IMDA’s ISG-CERT and CSA’s SINGCERT, as appropriate, to be apprised of newly discovered vulnerabilities and threats to IoT and ICT systems.

Note: IoT users and IoT providers may be dependent on IoT developers to provide patches for new vulnerabilities in a timely manner.

7.5 Principle 4: Resilience

7.5.1 Recovery from attacks

IoT systems will be targeted for attacks, especially if the asset is valuable enough. A determined attacker will find a way to compromise the system as more sophisticated attacking tools are developed. There is therefore a need to be prepared to fail safely and recover from it, especially when the compromise of an IoT system can affect the safety of humans or facilities.

Recommendation: Regular backups of system data (include settings) as well as regular disaster recovery exercises for systems shall be conducted.

7.5.2 Conduct periodic assessments

An IoT system can be a dynamic and complex system. As threats are always evolving, periodic penetration testing and/or vulnerability assessment is required to mitigate security risks.

Recommendation: Penetration testing and/or vulnerability assessments should be conducted periodically.

8 Threat modelling checklist

This section provides a suggested checklist for threat modelling. The checklist can be used to guide the threat modelling process and ensure that it is conducted properly and systematically.

Please refer to the case study in annex B for an illustration of the application of the threat modelling checklist.

ID	Threat modelling checklist	Y / N	Please elaborate
1	Identify the potential target(s) to be protected a. Define its boundaries and the external systems (including users) that it needs to interact with b. Decompose the target(s) into its subcomponents c. Identify data flows within the target(s), and inputs and outputs from external systems d. Identify sensitive data and where they are handled (at rest, in transit, in use) e. Identify the security needs (based on potential impacts to Confidentiality, Integrity and Availability (**CIA triad**)) for subcomponents and data flows f. Identify hardware, software and protocols in use		
2	Define the security problem a. Identify system accessibility • Identify attack surfaces • Determine operating environments • Determine system / device lifecycles and supply chain b. Identify system susceptibility (aka vulnerabilities) • Determine known vulnerabilities • Enumerate threats to attack surfaces (using Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (**STRIDE**) as a guide) • Enumerate threats to operating environments (using STRIDE as a guide) • Enumerate threats to stages of system / device lifecycles and supply chain (using STRIDE as a guide) c. State any assumptions		
3	Conduct risk assessment • Assess impact of threats and vulnerabilities to CIA triad and match against security needs of assets • Assess attacker capabilities required to realise the threats • Assess the likelihood of the risk • Prioritise the risks for mitigation, including other considerations (e.g. monetary impact)		
4	Determine the security objectives • State the security objectives. For example, OT systems emphasize safety, where system integrity takes precedence over data confidentiality		
5	Define the security requirements • State the necessary requirements to address the identified security objectives without going into their specific implementation		
6	Design and implement the capabilities		
7	Validate and verify that the capabilities address the security requirements adequately		

9 Vendor disclosure checklist

This section provides a checklist of baseline security requirements that enterprise solution vendors can use for self-disclosure. It guides buyers on how to evaluate and compare the security implementations of IoT solutions across different vendors. It also guides vendors on what security capabilities/services are important and encourages vendors to differentiate their products through security. Thus, this checklist facilitates communication, enables fair comparisons of security across IoT solutions and promotes the implementation of better security.

Please refer to the case study in annex B for an illustration of the application of the vendor disclosure checklist.

Legend: Y – Yes, N – No, NA – Not applicable

ID	Vendor disclosure checklist	Y / N / NA	Please elaborate
1. Cryptographic support			
CK-CS-01	Do your devices and system employ current and industry accepted cryptographic techniques and best practices? Examples of best practices include: · use of approved algorithms · sufficient key length · use of approved random number generator(s) · recommended crypto-period		
CK-CS-02	Do you employ proper key management (generation, exchange, storage, use, destruction, replacement, etc.) techniques?		
2. Security function protection			
CK-FP-01	Do you establish hardware Root-of-Trust?		
CK-FP-02	Do you employ secure boot?		
3. Identification and authentication			
CK-IA-01	Do you employ unique, non-modifiable and verifiable identities for clients (user, device, gateway, application) and servers?		
CK-IA-02	Do you employ mutual authentication? For example, before establishing connections and after pre-defined intervals		
4. Network protection			
CK-NP-01	Do you enforce network access control? For example, ensure explicit authorisation to join a new network and/or allow remote access.		
CK-NP-02	Do you employ proven transport protocols with security controls properly activated? Examples include: · Use of TLS for TCP payloads. · Use of DTLS for UDP payloads.		
CK-NP-03	Do you employ industry best practices for secure connectivity? Examples of industry best practices: · Use of VPN or leased lines. · Use of private mobile APNs from telecommunication operators when using a public mobile carrier network. · Use of DNS pinning to prevent DNS spoofing. · Use of traffic filtering based on type, port and destination. · Use of certificate pinning. · Employ TLS when using MQTT. · Scan for open network ports.		

ID	Vendor disclosure checklist	Y / N / NA	Please elaborate
	· Use whitelisting to establish or deny connections from non-trusted sources.		
CK-NP-04	Do you segregate communication channels for trusted end points from non-trusted ones? Examples include: · Use of VLAN. · Use of firewalls for DMZ. · Use of unidirectional security gateway. · Physical isolation.		
5. Data protection			
CK-DP-01	Do you protect the confidentiality and integrity of your sensitive data? · in transit · in use · at rest		
CK-DP-02	Do you protect the authenticity and integrity of your codes and firmware? · in transit · in use · at rest		
CK-DP-03	Do you ensure the authenticity and integrity of your data (e.g. inputs, commands and sensing data)? · in transit · in use · at rest Examples include: · Validate incoming content-types. · Validate response types. · Validate the HTTP methods against authorisation credentials. · Whitelist allowable HTTP methods. · Define the acceptable character set (e.g. UTF-8). · Validate that input characters are acceptable. · Encode/escape input and output.		
CK-DP-04	Do you enforce access control to detect and prevent unauthorised data access and exfiltration, and filter your outputs?		
6. Access protection			
CK-AP-01	Do you employ mechanisms to manage and secure local and/or remote access? Example of mechanisms include: · auto logoff. · screen lock. · lock-out for repeated unauthorised attempts. · forced re-authorisation.		
CK-AP-02	Do you send out-of-band notifications on impactful operations and/or alerts (eg. credential reset, security update failures)?		
CK-AP-03	Do you enforce access control to prevent unauthorised access to system interfaces, system files and removable media?		

ID	Vendor disclosure checklist	Y / N / NA	Please elaborate
CK-AP-04	Do you employ anti-tamper mechanisms for resistance, evidence, detection and/or response?		
CK-AP-05	Do you support multi-factor authentication for impactful operations (e.g. credential reset)?		
7. Security management			
CK-MT-01	Do you employ proper user and password management? Examples include: · Enforce strong password policy. · Enforce no default passwords. · Ensure that password recovery and reset mechanism are secure.		
CK-MT-02	Do you enforce proper access control to management functions? Examples include: · Enforce least privilege policy. · Use of attribute-based access control (ABAC) or role-based access control (RBAC). · Implement dual control for key management protection to prevent a single bad actor's compromise to the key materials. · Implement separation of duties to key management system to prevent a single bad actor/administrator from compromising the system.		
CK-MT-03	Do you employ malware mitigation mechanisms? Examples include: · Ensure file integrity using cryptographic hash. · Baseline "normal" behaviour. · Detect unauthorised software. · Prohibit insecure bootloaders.		
CK-MT-04	Do you secure remote management of devices, including sensor gateways? Examples include: · Support secure Over-The-Air (OTA) updates of device applications and configurations. · Support software and/or firmware updates using cryptographically secure methods. · Support platform integrity checking, such as the measured boot mechanism or verifying the firmware integrity. · Restrict remote management to secure networks.		
8. Resiliency support			
CK-RS-01	Does your device support integrity self-test, error detection and correction for critical functions and return to a safe state?		
CK-RS-02	Do you safeguard against a compromised device from compromising the system? Examples include: · Use of Perfect Forward Secrecy (PFS) for secure communication. · Use of distinct secret keys for individual device.		
CK-RS-03	Do you employ mechanisms against failures from resource exhaustion and/or malicious attacks such as DDoS? Examples include:		

ID	Vendor disclosure checklist	Y / N / NA	Please elaborate
	· Monitor to ensure that cloud resources are sufficient to sustain services. · Detect resource exhaustion, for early preventive or corrective actions · Control the execution of resource-intensive software. · Enforce power thresholds. · Limit the number of concurrent sessions. · Operate with excess capacity.		
CK-RS-04	Do you conduct regular backups of system data (including settings)?		
9. Security audit			
CK-AU-01	Do your devices and system record enough information (e.g. who does what and when) in audit logs and flag significant events? Example of events include: · User logins, logouts and unsuccessful authentication attempts. · Connection, disconnection attempts and unsuccessful connection attempts. · Unsuccessful authorisation attempts. · Access to sensitive data. · Import and export of data from removable media. · Any change in access privileges. · Creation, modification and deletion of data by user. · Impactful operations. · Remote operations. · Security update failures. · Physical access attempts where possible. · Emergency access where possible.		
CK-AU-02	Are your audit logs protected from modification, deletion, physical tampering and sensitive data disclosure?		
10. Lifecycle protection			
CK-LP-01	Have you conducted threat modelling to identify, analyse and mitigate threats to the system?		
CK-LP-02	Did you design and develop the system using a secure systems engineering approach?		
CK-LP-03	Do you implement and maintain the system with components from a secure supply chain, with no known vulnerabilities?		
CK-LP-04	Do you communicate, provide and update security information (terms of service, features, guidelines, instructions and notifications, etc.), in simple language and timely manner? Examples of security information include: · Security policies. · Security updates. · Instructions for device/media sanitisation. · End-of-life notifications.		
CK-LP-05	Do you ensure that the system is hardened before the "Operational" lifecycle phase? Examples of system hardening include: · Remove all backdoors. · Remove all debug codes from the released version.		

ID	Vendor disclosure checklist	Y / N / NA	Please elaborate
	· Change default configuration and disable unnecessary services. · Remove or tamper-covered JTAG, unneeded serial and ports before deployment. · Harden VM host properly, including disabling memory sharing between VM. · Remove default and hardcoded passwords.		
CK-LP-06	Do you maintain an inventory of connected devices, software and firmware versions, applied patches and updates throughout the "Operational" lifecycle stage?		
CK-LP-07	Do you conduct penetration testing and/or vulnerability assessment periodically, and before each major release?		
CK-LP-08	Do you establish proper vulnerability disclosure and management? Examples include: · Ensure the supply chain's capability to provide upgrades and patches. · Provide vulnerability disclosure and processes to track and response promptly. · Provide firmware and software patches/updates for vulnerabilities discovered, in a timely manner. · Employ proper change management processes to manage security patches or updates. · Notify and/or allow user to approve/reject updates, patches and changes to user settings, where appropriate. · Disclose minimum support period.		
CK-LP-09	Do you ensure that identities, certificates and secrets are secured throughout the lifecycle (e.g. creation, provisioning, renewal and revocation)?		
CK-LP-10	Do you sanitise devices and systems of security data and sensitive user data, before the "Reuse or Dispose" lifecycle stages?		

10 Bibliography

[1] GSMA IoT security guidelines for endpoint ecosystems

[2] https://cve.mitre.org/

[3] https://www.owasp.org/index.php/Application_Threat_Modeling

[4] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[5] Identity and access management for the Internet of Things – Cloud Security Alliance

[6] Industrial Internet of Things: volume G4 – Security framework

[7] IoT trust framework – Online Trust Alliance

[8] IEC 62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

[9] ISO/IEC 27000 Information security management systems – Information security risk management

[10] ISO/IEC 27002 Information security management systems – Code of practice for information security controls

[11] Strategic principles for securing the Internet of Things (IoT) – U.S. Department of Homeland Security

[12] ITSC TR 38 : 2014 Technical Reference for sensor network for Smart Nation (public areas)

[13] ITSC TR 40 : 2015 Technical Reference for sensor networks for Smart Nation (homes)

[14] ITSC TR 47 : 2016 Technical Reference for IoT reference architecture for Smart Nation

[15] ITSC TR 50 : 2016 Technical Reference for IoT information and services interoperability for Smart Nation

[16] TS-0003 OneM2M technical specification – Security solutions