IoT Security Compliance Framework

Release 2 December 2018

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org.

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

All product names are trademarks, registered trademarks, or service marks of their respective owners.

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this version of the document:

Abhay Soorya, Gemserv Ltd
Alex Margulis, Intel Corp
Arun Sambordaran, Gemserv Ltd
Chris Hills, Phaedrus Systems Ltd
Chris Shire, Infineon Technologies Ltd
Graham Markall, Embecosm Ltd
Ian Phillips, Roke Manor Research Ltd
Isaac Dangana, Red Alert Labs Ltd
Jan Krueger, Intel Corp
Jeremy Bennett, Embecosm Ltd
John Moor, IoT Security Foundation
Lokesh Johri, Tantive 4
Mark Beaumont, Roke Manor Research Ltd
Nick Hayes, Thinkstream Ltd
Pamela Gupta, Outsecure Inc
Peter Burgers, Display Link Ltd
Richard Marshall, Xitex Ltd
Richard Storer, MathEmbedded Ltd
Robert Dobson, Device Authority Ltd
Roger Shepherd, Chipless Ltd
Sean Gulliford, Gemserv Ltd
Trevor Hall, DisplayLink Ltd

Peer Reviewers
Brian Russell, Cloud Security Alliance
Colin Blanchard, BT Plc
Eric Vetillard, NXP Semiconductors NV
James Willison, Unified Security Ltd
Jeff Day, BT Plc
Marek Hubbell
Plus others – you know who you are!

Contents

1 Intent and Purpose

1.1 Introduction

The IoT Security Foundation (IoTSF) was established to address the challenges of IoT security in an increasingly connected world. It has a specific mission ***"to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this IoTSF will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems".***

In more concise terms for vendors, operators and end-users: **"Build Secure, Buy Secure, Be Secure***"*.

This IoT Security Compliance Framework ('Framework') leads its user through a structured process of questioning and evidence gathering. This ensures suitable security mechanisms and practices are implemented.

The Framework is intended to help all companies make high-quality, informed security choices by guiding them through a comprehensive requirement checklist and evidence gathering process. The evidence gathered during the process can used to declare conformance with best practice to customers and other stakeholders.

Providing good security capability requires decisions upfront in design and use – often referred to as ***secure by design***. In most cases, addressing the security of a product at the design stage is proven to be lower cost, and requiring less effort than trying to "put security" into or around a product after it has been created (which may not even be possible). Decisions need to be made to address use-case, business model, liability level and risk management in addition to technical concerns such as architecture, design features, implementation, testing, configuration and maintenance.

Throughout this document, and others published by the IoTSF, reference is made to "best practice" or "best practice security engineering". These best practices are derived from the combined expertise of the IoTSF members, used and tested within their own companies, and from the publications and guidance of other relevant organisations. Wherever possible, reference is made to existing standards and best practice materials to avoid unnecessary duplication. A list of external reference materials and related bodies is included at the end of this document.

1.2 Intended Audience

The Framework can be used internally in an organisation to self-assess or self-certify against, or by a third party auditor. It can also be used 'in part', as a procurement mechanism to help specify security requirements of a supplier contract. The Framework is aimed at the following stakeholders:

- For **Managers** in organisations that provide IoT products, technology and or services. It gives a comprehensive overview of the management process needed to adopt best practice. It will be useful for executive, programme and project managers, by enabling them to ask the right questions and assess the answers

- For **Developers and Engineers, Logistics and Manufacturing Staff**, it provides detailed requirements to use in their daily work and in project reviews to validate the use of best practice by different functions (e.g. hardware and software development, logistics etc.). In completing the Compliance Checklist [ref 19], documentary evidence will be compiled to demonstrate compliance both at development gates, and with third parties such as auditors or customers

- For **Supply Chain Managers**, the structure can be used to guide the auditing of security practices. It may therefore be applied within a producer organisation (as described above); and inspected by a customer of the producer

- For **Trusted Third Parties** as part of an audit or certification process

1.3 Scope

The scope of this document includes (but is not limited to):

- Business processes
- The “Things” in IoT i.e. Network connected products and/or devices
- Aggregation points such as gateways and hubs that form part of the connectivity
- Networking including wired, and radio connections, Cloud and server elements

1.3.1 Key Issues for IoT Security

The key compliance requirements can be summarised as follows:

Key Requirement	Action Required	Framework Reference
Management governance	There must be a named executive responsible for product security, and privacy of customer information.	2.4.3, 2.4.11
Engineered for security	The hardware and software must be designed with attention to security threats.	2.4.4, 2.4.5, 2.4.6, 2.4.7
Fit for purpose cryptography	These functions should be from the best practice industry standards.	2.4.8 , 2.4.9
Secure network framework and applications	Precautions have been taken to secure Apps, web interfaces and server software	2.4.12, 2.4.13
Secure production processes and supply chain	Making sure the security of the product is not compromised in the manufacturing process or in the end customer delivery and installation.	2.4.10, 2.4.12, 2.4.13
Safe and secure for the customer	The product is safe and secure "out of the box" and in its day to day use. The configuration and control should guide the person managing the device into maintaining security and provide for software updates, vulnerability disclosure policy, and life cycle management.	2.4.14

1.3.2 The Supply Chain of Trust

All end-use products are constructed using a set of component parts, typically sourced from a variety of suppliers. These parts may be electronic or mechanical components, software modules or packages, including open source. Many of these parts will be procured from third party suppliers. It is important that all parts, together with the supply chain logistics, are subject to a security review/audit.

The final IoT product can then be provided with its own evidence of security assessment, together with the component parts documents, as a complete package of auditable evidence. This will help users to assess how the product conforms to the overall ***"supply chain of trust"*** [ref 36].

1.4 About The Framework Supporting Resources From The IoTSF

The IoTSF provides a number of resources to foster security best practice:

- **This Framework** document [ref 19] is a structured list of security requirements and an evidence gathering process to guide an organisation through assurance and evidence gathering.
- The **Compliance Checklist** [ref 19] is a companion spread sheet to the Framework to aid collection and documentation of evidence.
- Additional **Best Practice Guidelines** are provided by the Foundation to help understanding of the most important topics [ref 44].
- Further resources including guides, documents, articles and blogs can be found on the IoTSF website**.**

All IoTSF publications are maintained and reviewed on a regular basis to keep them current – which is a crucial attribute, given the dynamic nature of cyber security.

This is the third public release and user feedback is welcome as part of its maintenance and evolution for addressing new security threats. You can send feedback and suggestions to improve the Framework by emailing contact@iotsecurityfoundation.org with a subject line of **"Compliance Framework Feedback"**.

Future releases may include extensions for specific application or product categories.

1.4.1 Changes from version V1.1 of Compliance Framework

Release 1.1 of the Framework was restricted to consumer class products. This Release 2.0 of the Framework includes products for a wider range of applications - from consumer to enterprise, including B2B markets.

New items for this release:

- Changed to risk based approach – to give a more flexible applicability
- Removal of application specific restrictions
- Addition of business and technical related keywords to allow filtering of relevant requirements for different stakeholder interests – see "keywords" section 0
- Combination of category and applicability level
- Additional explanatory text
- A companion spread sheet is available for this Framework to support evidence gathering.

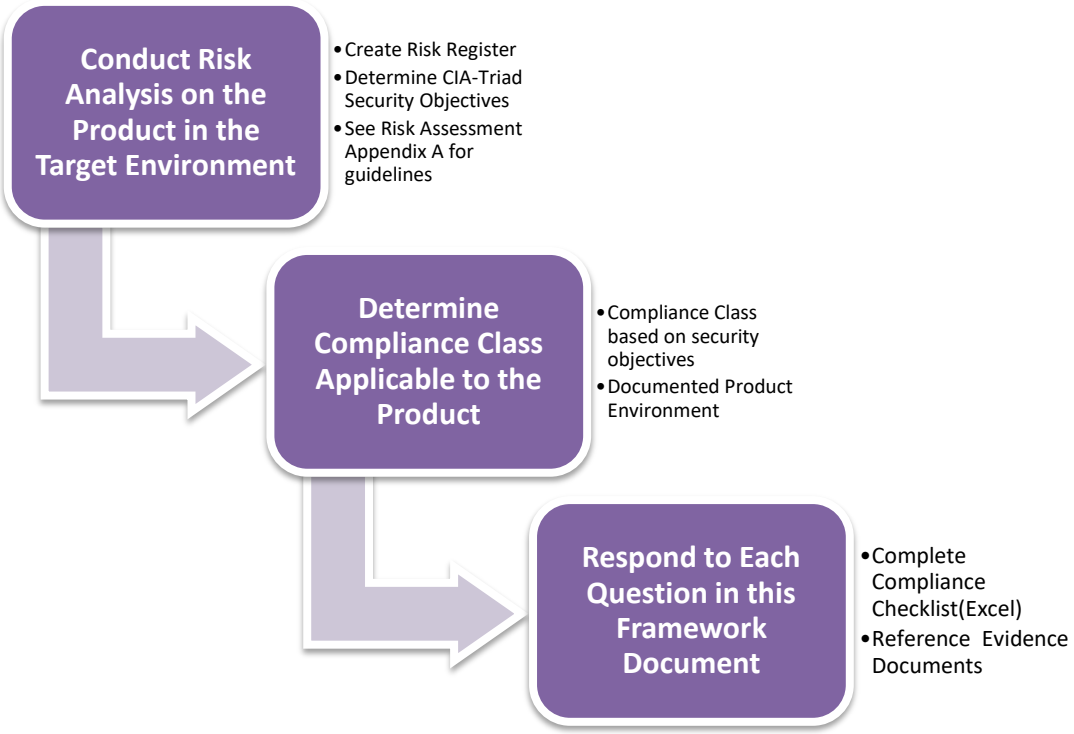
The requirements section detailed in section 2.4 and the numbering has been maintained where possible from prior releases of the Framework to maintain consistency.

2 The IoT Security Compliance Framework

2.1 The Process

The Framework sets out a comprehensive set of security requirements for aspects of the organisation and product. A response to each requirement needs to be entered into a Compliance Checklist [ref 19], with supporting statements or evidence. For requirements deemed "not applicable", an explanation must be provided as to why. Any alternative countermeasures to reduce any security risk should also be listed.

The compliance process breaks down into a number of steps:



2.1.1 Risk Assessment

In security terms, ***context is everything*** - each application differs in use-case and operating environment. It is the responsibility of the Framework user to determine their risk appetite within their stated usage environment and therefore the specific compliance class (section 2.2) of the security measures applied.

To achieve this, **a comprehensive risk assessment is a pre-requisite to using the Framework**. The risk assessment process will help determine the compliance class for the product/service. Section 2.2 has more details on compliance classes and how they relate to the Confidentiality, Integrity and Availability otherwise known as the CIA Triad [ref 1] model commonly used by security professionals. As a general rule, the highest possible compliance class should be adopted, considering not just the immediate context of the product, but also the potential hazards to the system(s) the product/service may eventually be used within.

A basic outline of the risk assessment process can be found in Appendix A. Risk management techniques can also be found in publications from organisations such as NCSC, ENISA and NIST [ref 39, 40 and 41].

2.2 Compliance Class

Determining the security objectives across the full diversity of IoT-class applications is a subjective endeavour. Even within vertical sectors such as consumer and enterprise, the security measures and strength of controls will vary depending on the actual use case. In making the Framework more practical across a range of applications, this version has adopted a risk-based approach derived from the commonly used CIA Triad [ref 1]. Whilst it is not a perfect model, its simplicity is its strength, and good security practice can be derived from the core principles.

Depending on the market and application into which the product is intended to be used, a risk assessment may require a higher compliance class in order to mitigate the determined level of risk. Consider the following example: a fictional case of a Wi-Fi relay box used in a remote monitoring station, where the threat to the enterprise operation is considered low, could be assessed under Compliance Class 1 requirements. However when deployed into a hospital, with higher threat dependencies, it could be assessed to be under Compliance Class 4 requirements. A further example is provided in section 2.2.1.

In order to apply an appropriate level of security compliance to a product, the requirements in the checklist are classified using the following compliance classes:

- *Class 0: where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organisation*
- *Class 1: where compromise to the data generated or loss of control is likely to result in no more than limited impact on an individual or organisation*
- *Class 2: in addition to class 1, the device is designed to resist attacks on availability that would have significant* impact *on an individual or organisation, or impact many individuals. For example by limiting operations of an infrastructure to which it is connected*
- *Class 3: in addition to class 2, the device is designed to protect sensitive data including sensitive personal data*
- *Class 4: in addition to class 3, where compromise to the data generated or loss of control have the potential to affect critical infrastructure or cause personal injury*

For each compliance class, the levels of integrity, availability and confidentiality are shown in **Table 1** below.

Compliance Class	Security Objective		
	Confidentiality	**Integrity**	**Availability**
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

Table 1: Compliance Class Security Objectives

The definitions of the levels of confidentiality, integrity, and availability are as follows:

- Confidentiality
    - Basic – devices or services processing public information
    - Medium – devices or services processing sensitive information, including Personally Identifiable Information, whose compromise would have limited impact on an individual or organisation
    - High – devices or services processing very sensitive information, including sensitive personal data whose compromise would have significant impact on an individual or organisation
- Integrity
    - Basic – devices or services whose compromise could have a minor or negligible impact on an individual or organisation
    - Medium – devices or services whose compromise could have limited impact on an individual or organisation
    - High – devices or services whose compromise could have a significant or catastrophic impact on an individual or organisation
- Availability
    - Basic – devices or services whose lack of availability would cause minor disruption
    - Medium – devices or services whose lack of availability would have limited impact on an individual or organisation
    - High – devices or services whose lack of availability would have significant impact to an individual or organisation, or impacts many individuals

[ref 11, 12, 13 & 14 were used as the basis of the above definitions]

Please Note: the Framework Compliance Class is provided for guidance only. A supplier may know of application specific concerns that would change the class values. Requirements deemed "not applicable" must be supported by credible evidence to explain the case.

2.2.1 Determining Security Goals – An Example

To illustrate via a practical example, consider the security features required by a connected thermostat used in a commercial greenhouse. The Compliance Class selection for the device might be determined in the following way:

- Confidentiality is Basic: the underlying assumption is that the thermostat does not store sensitive, confidential or personally identifiable information
- Integrity is Medium: for a thermostat in a commercial greenhouse, poor data integrity could have a business/financial impact
- Availability is Medium: the thermostat in a commercial greenhouse setting is likely to be part of an environmental control system. As such an individual sensor failure will have little impact, yet a denial of service attack across multiple sensors carries a greater commercial risk

In this case, the thermostat may be classified in the following way:

Compliance Class	Security Objective		
	Confidentiality	Integrity	Availability
Class 1	Basic	Medium	Medium

Table 2: Example of Compliance Class Security Objectives

2.3 Completion of a Compliance Checklist

It is anticipated that compliance with the Framework will become an integral part of an organisation's security process and will provide the supporting evidence for business assurance. An accompanying spreadsheet, the Compliance Checklist [ref 19], may be used at various stages in the product lifecycle. First by identifying the need for security at the concept stage, and then listing evidence gathered to finally signing off security requirements for production release.

The evidence gathering process can only commence after establishing the Compliance Class described in section 2.2. This is done through the use of a risk assessment (see Appendix A).

Once the Compliance Class is determined, the applicable requirements are automatically derived by the accompanying spreadsheet as either mandatory (M) or advisory (A). The spreadsheet could also be used to optimise the product design and establish if a change would allow a lower Compliance Class to be selected. For example, by not collecting or processing sensitive personal data or perhaps providing automatic failover to alternative services for customers to maintain service availability.

2.3.1 Keywords

To improve the usability of this document the requirements in sections 2.4.3 to 2.4.16 have been categorised using the keywords defined in the Table below.

Primary Keyword	Description	Secondary keyword	Description
System	The requirement is applicable to the technical elements of the Device/product or service	***Software***	The requirement is directly applicable to the software of the device or service
		Hardware	The requirement is directly applicable to the electronics of the device/service hardware (PCB, processor, components etc.)
		Physical	The requirement is directly applicable to mechanical aspects of the device such as the casing, form factor etc.
Business	A business requirement not directly related to the operational function of the device/ product or service	***Process***	A flow of activities that indirectly contributes to the security characteristics of a device or service
		Policy	The instructions and guidelines that indirectly contribute to the security characteristics of a device or service
		Responsibility	A role or responsibility that indirectly contributes to the security characteristics of a device or service

Table 3: Keyword Categories

Please Note: the terms Device and Product are considered to be interchangeable in this document

2.3.2 Compliance Requirements Completion Responsibilities

The Compliance requirements completion will be addressed by a variety of roles in an organisation. These roles cannot be prescribed exactly as every organisation is different, but each section of requirements may require the attention of Managers and other staff as suggested in the table 4 below. Responsibility for any individual requirement may be determined by use of the associated Keywords, which can be selected by filter, when using the Compliance Checklist spreadsheet.

Section	Topic	Topic Audience & Typical Responsibilities
2.4.3	Business Security Processes, Policies and Responsibilities	Management responsible for governance of a business developing and deploying IoT Devices.
2.4.4	Device Hardware & Physical Security	Design and Production staff responsible for hardware and mechanical quality.
2.4.5	Device Software	Device application quality management by Software Architects, Product Owners, and Release Managers.
2.4.6	Device Operating System	Management and Design staff responsible for selection of a third party Operating System or assessing the quality of 'in-house' developed software.
2.4.7	Device Wired and Wireless Interfaces	Design and Production staff responsible for Device communications security.
2.4.8	Authentication and Authorisation	Design and Production staff responsible for security of the IoT systems interfaces and foundations of authentication.
2.4.9	Encryption and Key Management for	Design and Production staff responsible for security of

	Hardware	the IoT systems hardware key management and encryption.
2.4.10	Web User Interface	Design and Production staff responsible for security of the IoT Product or Services' Web Systems.
2.4.11	Mobile Application	Design and Production staff responsible for security of the IoT Product or Services' Mobile Application.
2.4.12	Privacy	Management and staff responsible for Data Protection and Privacy regulatory compliance.
2.4.13	Cloud and Network Elements	Design and Production staff responsible for security of the IoT Product or Services' Cloud or Network Systems.
2.4.14	Secure Supply Chain and Production	Management, Design and Production staff responsible for security of the IoT Product or Services' Supply Chain.
2.4.15	Configuration	Design and Production staff responsible for security of the device and IoT Services configurations.
2.4.16	Device Ownership Transfer	Management, Design and Production staff responsible for a products and services' Supply Chain.

Table 4: Compliance Responsibilities

Relevant requirements should be shown as "addressed" and a reference made to the applicable evidence for the product design.

The accompanying Compliance Checklist allows for entries, against each relevant requirement, of either the evidence gathered to prove compliance or a link to that evidence. The evidence may be compiled from a number of sources and people. Evidence should be verified by the person responsible for completion of the Framework and such verification should also be recorded.

An example of completed Compliance Checklist fragment on Business Processes for a high risk Class 3 device is shown Figure 1 below.

Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword	Required Compliance Method
There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	M for Class 3	Business	Responsibility	Class 3 Audit: CSO appointed: (insert URL)
There is a person or role, who takes ownership for adherence to this compliance checklist process.	M for Class 3	Business	Responsibility	Class 3 Audit: IT Security Mgr. "name"
There are documented business processes in place for security.	M for Class 3	Business	Process	Class 3 Audit Business process documents – Intranet link

The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework, ISO27000 etc.).	A for all Classes	Business	Policy	Class 3 Audit Certificate available (insert URL)

Figure 1: Compliance Checklist Partially Completed Example

2.3.3 Evidence

The Framework is a summary checklist, and should be complemented with the product design documentation including the Risk Register. Evidence of the mitigations made to address each risk line item must also be recorded.

Such records should be kept safe and secure, we recommend having back-up copies. They could be useful in the case of real world threats to the product, but also as evidence for any business compliance regimes used in the organisation. The record keeper should enable access, for auditing, to any referenced evidence and supporting documents. URLs especially should be checked to ensure they will remain accessible at least for the life of the product plus any warranty period. Attention should also be paid to maintaining any tools or applications needed to view the evidence material.

An organisation procuring products, systems and services from a supplier which declares it has used the Framework may request an audit of the evidence assembled, using either internal resources or a Trusted Third Party ("T3P"). A T3P might be used in situations where the documented evidence would expose sensitive information such as intellectual property or commercial aspects.

2.4 Compliance Terminology and Applicability

2.4.1 Terminology

The following terms "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may" and "optional" are used in accordance with the definitions in RFC2119 [ref 25].

2.4.2 Level of Compliance

The applicability levels are defined as follows.

Mandatory	**This requirement shall be met as it is vital to meet the security objectives of the product.**
Advisory	This requirement should be met unless there are sound product reasons (e.g. economic viability, hardware complexity). The reasons for deviating from the requirement and alternative countermeasures to reduce any security risk should be documented.

For example in the following tables, where it shows "M of 2 and above" compliance class, this means that the requirement is mandatory for all other levels i.e. 2, 3 & 4.

2.4.3 Compliance Applicability – Business Security Processes, Policies and Responsibilities

This section's intended audience is those personnel who are responsible for governance of a business developing and deploying IoT Devices. There must be named executive(s) responsible for product security, and privacy of customer information.

There are several classes of requirements that have been identified by a keyword. Each class should be allocated to a specified person or persons for the product being assessed. Further guidance is available from the IoTSF Best Practice Guidelines [ref 44].

The applicability of each requirement is defined as **A**dvisory or **M**andatory for the assessed risk level of any device, the default is Advisory.

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.3.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	M for All classes	Business	Responsibility
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance checklist process.	M for All Classes	Business	Responsibility
2.4.3.3				
2.4.3.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework, ISO27000 etc.).	M for Class 2 and above	Business	Policy
2.4.3.5	A policy has been established for interacting with both internal and third party security researcher(s) on the products or services.	M for All Classes	Business	Policy
2.4.3.6	A policy has been established for addressing risks that could impact security and affect or involve technology or components incorporated into the product or service provided.	M for Class 2 and above	Business	Policy
2.4.3.7	Processes and plans are in place based upon the IoTSF Vulnerability Disclosure Guidelines [ref 19], or a similar recognised process, to deal with the identification of a security vulnerability or compromise when they occur.	M for All classes	Business	Process
2.4.3.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those executives who may deal with the media or make public announcements. In particular, that any public statements made in the event of a security breach should give as full and accurate an account of the facts as possible.	M for All Classes	Business	Process
2.4.3.9	There is a secure notification process based upon the IoTSF Vulnerability Disclosure Guidelines [ref 19] or a similar recognised	M for All Classes	Business	Process

	process, for notifying partners/users of any security updates.			
2.4.3.10	A security threat and risk assessment shall have been carried out using a standard methodology such as OWASP, Octave or NIST RMF Risk Management Framework [ref 35] to determine the risks and evolving threats before a design is started.	M for All Classes	Business	Process
2.4.3.11	As part of the Security Policy, develop specific contact web pages for Vulnerability Disclosure reporting.	M for All classes	Business	Policy
2.4.3.12	As part of the Security Policy, provide a dedicated security email address and/or secure online page for Vulnerability Disclosure communications.	M for All Classes	Business	Policy
2.4.3.13	As part of the Security Policy, develop a conflict resolution process for Vulnerability Disclosures.	M for Class 3 and above	Business	Process
2.4.3.14	As part of the Security Policy, publish the organisation's conflict resolution process for Vulnerability Disclosures.	A for All Classes	Business	Process
2.4.3.15	As part of the Security Policy, develop response steps and performance targets for Vulnerability Disclosures.	M for All Classes	Business	Process
2.4.3.16	As part of the Security Policy, develop security advisory notification steps. For examples see US Cert programme [ref 46].	M for All Classes	Business	Process
2.4.3.17	The Security Policy shall be compliant with ISO 30111 or similar standard.	A for All classes	Business	Policy
2.4.3.18	Where real-time or up-time expectations are present, a procedure must be defined for notifying connected components of impending downtime for updates.	M for Class 2 and above	Business	Process
2.4.3.19	Responsibility is allocated for each stage of the update process.	M for Class 2 and above	Business	Responsibility
2.4.3.20	Responsibility is allocated for control, logging and auditing of the update process.	M for Class 2 and above	Business	Process Role
2.4.3.21	There is a point of contact for third party suppliers with security issues.	M for Class 1 and above	Business	Process Role
2.4.3.22	Where remote update is supported, there is an established process/plan for validating "updates" and updating devices on an on-going or remedial basis e.g. guidance on software updates is available from the IoTSF Best Practice Guidelines Part L [ref 44].	M for Class 2 and above	Business	Process
2.4.3.23	The security update policy for devices with a constrained power source shall be assessed to balance the needs of maintaining the integrity and availability of the device.	M for Class 2 and above	Business	Policy
2.4.3.24	There is a named owner responsible for assessing third party supplied components (hardware and software) used in the product e.g.	M for Class 2 and above	Business	Role

	The OS suppliers provided a completed IoTSF Framework Compliance Checklist [ref 19], document or equivalent.			
2.4.3.25	Where a remote software upgrade can be supported by the device, there should be a transparent and auditable policy with schedule of actions to fix any vulnerabilities found.	M for Class 2 and above	Business	Policy

2.4.4 Compliance Applicability – Device Hardware & Physical Security

This section's intended audience is those personnel who are responsible for hardware and mechanical quality. Guidance is available from the IoTSF [Ref 44] regarding Physical Security (part B) Secure Boot (part C) and Secure Operating Systems (part D).

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.4.1	The product's processor system has an irrevocable hardware Secure Boot process.	M for Class 1 and above	System	Hardware
2.4.4.2	The product's processor system has an irrevocable "Trusted Root Hardware Secure Boot".	M for Class 2 and above	System	Hardware
2.4.4.3	The product's processor system has a measured irrevocable hardware Secure Boot process.	M for Class 3 and above	System	Hardware
2.4.4.4	The Secure Boot process is enabled by default.	M for Class 1 and above	System	Hardware
2.4.4.5	Any debug interface (for example, I/O ports such as JTAG) only communicates with authorised and authenticated entities on the production devices.	M for Class 1 and above	System	Hardware Software
2.4.4.6	The hardware incorporates protection against tampering and this has been enabled. The level of tamper protection must be determined by the risk assessment.	M for Class 1 and above	System	Hardware
2.4.4.7	The hardware incorporates physical protection against tampering to reduce the attack surface. The level of protection must be determined by the risk assessment.	M for Class 3 and above	System	Hardware Physical
2.4.4.8	The hardware incorporates physical protection against reverse engineering. The level of protection must be determined by the risk assessment.	M for Class 2 and above	System	Hardware
2.4.4.9	All communications port(s), such as USB, RS232 etc., which are not used as part of the product's normal operation are not physically accessible or only communicate with authorised and authenticated entities.	M for all Classes	System	Hardware Physical Software

2.4.4.10	All the product's development test points are securely disabled or removed wherever possible in production devices.	M for Class 2 and above	System	Hardware Physical
2.4.4.11	Tamper Evident measures have been used to identify any interference to the assembly to the end user.	M for Class 2 and above	System	Hardware
2.4.4.12				
2.4.4.13	In production devices the microcontroller/ microprocessor(s) shall not allow the firmware to be read out of the products non-volatile [FLASH] memory. Where a separate non-volatile memory device is used the contents shall be encrypted.	M for Class 1 and above	System	Hardware
2.4.4.14	Where the products' credential/key storage is external to its processor, the storage and processor shall be cryptographically paired to prevent the credential/key storage being used by unauthorised software.	M for All Classes	System	Hardware
2.4.4.15	Where production devices have a CPU watchdog, it is enabled and will reset the device in the event of any unauthorised attempts to pause or suspend the CPU's execution.	M for All Classes	System	Hardware
2.4.4.16	Where the product has a hardware source for generating true random numbers, it is used for all relevant cryptographic operations including nonce, initialisation vector and key generation algorithms. For guidance see: NIST SP 800-90A [ref 3].	M for All Classes	System	Hardware Software
2.4.4.17	The product shall have a hardware source for generating true random numbers.	M for Class 2 and above	System	Hardware

2.4.5 Compliance Applicability – Device Software

This section's intended audience is for those personnel who are responsible for device application quality e.g. **Software Architects, Product Owners, and Release Managers.** Guidance is available from the IoTSF [ref 44] regarding Secure Operating Systems (part D), Credential Management (Part F), and Software Updates (part J).

Req. No	Requirement	Compliance Class and Applicability	Primary Keywords	Secondary Keywords
2.4.5.1	The product has measures to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or in a sandbox.	M for All Classes	System	Software
2.4.5.2	Where remote software updates can be supported by the device, the software images are digitally signed by an approved signing authority.	M for All Classes	System	Software
2.4.5.3	Where updates are supported the software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.	M for All Classes	System	Software
2.4.5.4	If remote software upgrade is supported by a device, software images shall be encrypted whilst being transferred to it.	M for Class 2 and above	System	Software
2.4.5.5	If the product has any virtual port(s) that are not required for normal operation, they are only allowed to communicate with authorised and authenticated entities or securely disabled when shipped. Where a port is used for field diagnostics, the port input commands are deactivated and the output provides no information which could compromise the device, such as credentials, memory address or function names.	M for Class 2 and above	System	Software
2.4.5.6	To prevent the stalling or disruption of the device's software operation, watchdog timer are present, and cannot be disabled.	M for All Classes	System	Hardware Software
2.4.5.7	The product's software signing root of trust is stored in tamper-resistant memory.	M for All Classes	System	Hardware
2.4.5.8	The product has protection against unauthorised reversion of the software to an earlier and potentially less secure version.	M for All classes	System	Software
2.4.5.9	There are measures to prevent the installation of non-production software onto production devices.	M for All Classes	Business	Process
2.4.5.10	Production software images shall be compiled in such a way that all unnecessary debug and symbolic information is removed, to prevent accidental release of superfluous data.	M for All Classes	Business	Process
2.4.5.11	Development software versions have any debug functionality switched off if the software is	M for Class 2 and above	Business	Process

	operated on the product outside of the product vendor's trusted environment.			Policy
2.4.5.12	Steps have been taken to protect the products' software from sensitive information leakage and side-channel attacks.	M for Class 3 and above	System	Software Hardware
2.4.5.13	The product's software source code follows the basic good practice of a Language subset (e.g. MISRA-C) coding standard.	M for Class 2 and above	Business	Policy
2.4.5.14	The product's software source code follows the basic good practice of static vulnerability analysis [ref 37] by the developer.	M for Class 2 and above	Business	Process
2.4.5.15	The software must be architected to identify and ring fence sensitive software components, including cryptographic processes, to aid inspection, review and test. The access from other software components must be controlled and restricted to known and acceptable operations. For example, security related processes should be executed at higher privilege levels in the application processor hardware.	M for Class 1 and above	Business System	Process Software
2.4.5.16	Software source code is developed, tested and maintained following defined repeatable processes.	M for All classes	Business	Process
2.4.5.17	The build environment and toolchain used to compile the application is run on a build system with controlled and auditable access.	M for Class 2 and above	Business	Policy Process
2.4.5.18	The build environment and toolchain used to create the software is under configuration management and version control, and its integrity is validated regularly.	M for Class 2 and above	Business	Process
2.4.5.19	Where present, production software signing keys are under access control.	M for all classes	Business	Policy
2.4.5.20	The production software signing keys are stored and secured in a storage device compliant to FIPS-140-2 level 2 [ref 5], or equivalent or higher standard.	M for Class 2 and above	Business	Policy
2.4.5.21	Where the device software communicates with a product related webserver or application over TCP/IP or UDP/IP, the device software uses certificate pinning or public/private key equivalent, where appropriate.	M for Class 2 and above	System	Software
2.4.5.22	For devices with no possibility of a software update, the conditions for and period of replacement support should be clear.	M for all classes	Business	Policy
2.4.5.23	All inputs and outputs are checked for validity e.g. use "Fuzzing" tests to check for acceptable responses or output for both expected (valid) and unexpected (invalid) input stimuli.	M for Class 2 and above	Business	Process
2.4.5.24	The software has been designed to meet the safety requirements identified in the risk assessment; for example in the case of unexpected invalid inputs, or erroneous software operation, the product does not become dangerous, or compromise security of other	M for Class 2 and above	System	Software

	connected systems.			
2.4.5.25	Support for partially installing updates is provided for devices whose on-time is insufficient for the complete installation of a whole update.	A for All classes	System	Software
2.4.5.26	Support for partially downloading updates is provided for devices whose network access is limited or sporadic.	A for All classes	System	Software
2.4.5.27	Where real-time expectations of performance are present, update mechanisms must not interfere with meeting these expectations (e.g. by running update processes at low priority).	A for All classes	System	Software
2.4.5.28	Where a device doesn't support secure boot, upon a firmware update the user data and credentials should be re-initialised.	M for All classes	System	Hardware Software
2.4.5.29	Where a device cannot verify authenticity of updates itself (e.g. due to no cryptographic capabilities), only a local update by a physically present user is permitted and is their responsibility.	M for All classes	System	Software
2.4.5.30	When a device cannot verify authenticity of updates itself, it shall be possible revert to the last known good configuration which was stored on the device before the update was attempted.	M for All classes	System	Software
2.4.5.31	Cryptographic keys for update integrity protection and confidentiality are securely managed in accordance with industry standards such as FIPS 140-2 [ref 5].	M for All classes	Business	Process Policy
2.4.5.32	There is secure provisioning of cryptographic keys for updates during manufacture in accordance with industry standards such as FIPS 140-2 [ref 5].	M for All classes	Business	Process Policy
2.4.5.33	Memory locations used to store sensitive material (e.g. cryptographic keys, passwords/passphrases, etc.) are sanitised as soon as possible after they are no longer needed. These can include but are not limited to locations on the heap, the stack, and statically-allocated storage [ref 47].	M for Class 2 and above	System	Software
2.4.5.34	Any caches which potentially store sensitive material are cleared / flushed after memory locations containing sensitive material have been sanitised.	M for Class 3 and above	System	Hardware Software
2.4.5.35	An end-of-life policy shall be published which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to users and an update should be easy to implement.	M for All classes	Business	Policy
2.4.5.36	Where possible, software updates should be pushed for a period appropriate to the device. This period shall be made clear to a user when supplying the device. The supply chain partners should inform the user that an update is required.	M for All classes	Business	Policy

2.4.6 Compliance Applicability – Device Operating System

This section's intended audience are the personnel responsible for the selection of a third party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers quality. The term Operating System (OS) is below used for sake of brevity to imply all such options. Guidance is available from the IoTSF [Ref44] regarding Secure Operating Systems (part D).

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keywords
2.4.6.1	The OS is implemented with relevant security updates prior to release.	A for all Classes	Business	Process
2.4.6.2				
2.4.6.3	All unnecessary accounts or logins have been disabled or eliminated from the software at the end of the software development process. E.g. Development or debug accounts.	A for all Classes	System	Software
2.4.6.4	Files, directories and persistent data are set to minimum access privileges required to correctly function.	A for all Classes	System	Software
2.4.6.5	If passwords absolutely must be stored in a local file, then passwords file(s) are owned by and are only accessible to and writable by the by the Devices' OS's most privileged account.	M for Class 1 and above	System	Software
2.4.6.6	All OS non-essential services have been removed from the product's software, image or file systems.	A for all Classes	System	Software
2.4.6.7	All OS command line access to the most privileged accounts has been removed from the OS.	A for all Classes	System	Software
2.4.6.8	The product's OS kernel and its functions are prevented from being called by external product level interfaces and unauthorised applications.	M for Class 1 and above	System	Software
2.4.6.9	Applications are operated at the lowest privilege level possible and only have access to the resources they need as controlled through appropriate access control mechanisms. For example, Products with one or more network interfaces, the uncontrolled, and any unintended packet forwarding functions should be blocked.	M for All Classes	System	Software
2.4.6.10	All the applicable security features supported by the OS are enabled.	M for Class 1 and above	System	Software
2.4.6.11	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	A for all Classes	System	Software
2.4.6.12	The OS implements a separation architecture to separate trusted from untrusted applications	M for Class 2 and above	System	Software
2.4.6.13	The product's OS kernel is designed such that each component runs with the minimal security capabilities required (e.g. a microkernel architecture).	M for Class 2 and above	System	Software

2.4.7 Compliance Applicability – Device Wired and Wireless Interfaces

This section's intended audience is for those personnel who are responsible for device security. Guidance is available from the IoTSF Best Practice Guidelines [ref 44] regarding Credential Management (Part F), and Network Connections (Part H).

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.7.1	The product prevents unauthorised connections to it or other devices the product is connected to. For example, there is a firewall on each interface and internet layer protocol.	M for Class 1 and above	System	Software
2.4.7.2	The network component and firewall (if applicable) configuration has been reviewed and documented for the required/defined secure behaviour.	M for Class 1 and above	Business	Process
2.4.7.3	In products with network interfaces, to stop bridging of security domains, the uncontrolled, and any unintended packet forwarding functions should be blocked to stop undesirable communication paths.	M for Class 1 and above	System	Software
2.4.7.4	Devices support only the versions of application layer protocols with no publically known vulnerabilities.	M for Class 1 and above	Business	Process
2.4.7.5	If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.	M for all Classes	System	Software
2.4.7.6	All the products unused ports are closed and only the required ports are active.	M for Class 1 and above	Business	Process
2.4.7.7	If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device. Examples are Wi-Fi access passwords and Bluetooth PINS.	M for Class 1 and above	Business	Process
2.4.7.8	Where using initial pairing process, a Strong Authentication shall be used; requiring physical interaction with the device or possession of a shared secret. For example, Bluetooth Numeric Comparison [ref 38].	M for Class 1 and above	System	Software
2.4.7.9	Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued, or reset password prior to providing normal service.	M for Class 1 and above	Business	Policy
2.4.7.10	For any Wi-Fi connection WPA2 [ref 51], or later versions with AES, or a similar strength encryption has been used and insecure protocols such as WPA and TKIP are disabled	M for Class 1 and above	System	Software

2.4.7.11	Where WPA2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	M for Class 1 and above	System	Software
2.4.7.12	All network communications keys are stored securely, in accordance with industry standards such as FIPS 140-2 [ref 5] or similar.	M for Class 1 and above	System	Software
2.4.7.13	Where a TCP protocol, such as MQTT, is used, it is protected by a TLS connection with no known vulnerabilities.	M for Class 1 and above	System	Software
2.4.7.14	Where a UDP protocol is used, such as CoAP, it is protected by a DTLS connection with no known vulnerabilities.	M for Class 1 and above	System	Software
2.4.7.15	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A [ref 2] or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	M for Class 1 and above	Business	Process
2.4.7.16	All use of cryptography by the product, such as TLS cipher suites, shall be listed and validated against the import/export requirements for the territories where the product is to be sold and/or shipped.	M for Class 1 and above	Business	Process
2.4.7.17	Where there is a loss of communications or availability it shall not compromise the local integrity of the device.	M for all Classes	System	Software
2.4.7.18	The product only enables the communications interfaces, network protocols, application protocols and network services necessary for the product's operation.	M for Class 1 and above	System	Software
2.4.7.19	Communications protocols should be latest versions with no publically known vulnerabilities and/or appropriate for the product.	M for Class 1 and above	Business	Policy
2.4.7.20	Post product launch communications protocols should be maintained throughout the product life cycle to the most secure versions available with no publically known vulnerabilities.	M for Class 1 and above	Business	Policy
2.4.7.21	If a factory reset is made, the device should warn that secure operation may be compromised unless updated.	M for Class 1 and above	System	Software
2.4.7.22	Where RF communications are enabled (e.g., ZigBee, etc.) antenna power is configured to limit ability of mapping assets to limit attacks such as WAR-Driving (see https://techterms.com/definition/wardriving).	A for all classes	System	Software
2.4.7.23	Protocol anonymity features are enabled in protocols (e.g., Bluetooth) to limit location tracking capabilities.	A for all classes	System	Software
2.4.7.24	As far as reasonably possible, devices should remain operating and locally functional in the case of a loss of network connection and	M for all Classes	System	Software

	should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.			

2.4.8 Compliance Applicability – Authentication and Authorisation

This section's intended audience is for those personnel who are responsible for the security of the IoT systems interfaces and foundations of authentication. Guidance is available from the IoTSF [ref 44] regarding Credential Management (Part F).

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.8.1	The product contains a unique and tamper-resistant device identifier (e.g. the chip serial number or other unique silicon identifier) for example binding code and data to a specific device hardware. This is to mitigate threats from cloning.	M for Class 1 and above	System	Hardware
2.4.8.2	Where the product has a secure source of time there is a method of validating its integrity, such as Secure NTP https://www.ntpsec.org.	M for all Classes	System	Software
2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is unique to each device in the product family. If a password-less authentication is used the same principles of uniqueness apply.	M for Class 1 and above	System	Software
2.4.8.4	The product does not accept the use of null or blank passwords.	M for Class 1 and above	System	Software
2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	M for Class 1 and above	System	Software
2.4.8.6	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy [ref 17], NIST SP800-63b [ref 26] or NCSC [ref 48] on password length, characters from the groupings and special characters.	M for Class 1 and above	System	Software
2.4.8.7	The product has defence against brute force repeated login attempts, such as exponentially increasing retry attempt delays.	M for Class 1 and above	System	Software
2.4.8.8	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard such as NIST SP800-63b [ref 26] or similar.	M for Class 1 and above	System	Software
2.4.8.9	The product supports access control measures to the root/highest privilege account to restrict access to sensitive information or system processes.	M for Class 1 and above	System	Software
2.4.8.10	The access control privileges are defined, justified and documented.	M for Class 1 and above	Business	Process

2.4.8.11	The product only allows controlled user account access; access using anonymous or guest user accounts is not supported without justification.	M for Class 1 and above	System	Software
2.4.8.12	The product allows the factory issued or OEM login accounts to be disabled or erased or renamed when installed or commissioned.	A for all Classes	System	Software
2.4.8.13	The product supports having any or all of the factory default user login passwords altered when installed or commissioned.	M for all Classes	Business	Process
2.4.8.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorised party.	M for Class 1 and above	Business	Process
2.4.8.15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.	M for Class 1 and above	System	Software
2.4.8.16	The product allows an authorised and complete factory reset and all of the device's authorisation information.	A for all Classes	System	Software
2.4.8.17	Where the product has the ability to remotely recover from attack, it should return to a known good state, to enable safe recovery and updating of the device.	M for all Classes	System	Software

2.4.9 Compliance Applicability – Encryption and Key Management for Hardware

This section's intended audience is for those personnel who are responsible for the security of the IoT systems hardware key management and encryption. Guidance is available from the IoTSF [ref 44] regarding Encryption (Part G).

Req. No	Requirement	Compliance Class	Primary Keyword	Secondary Keyword
2.4.9.1				
2.4.9.2	If present, a true random number generator source has been validated for true randomness using an NIST SP800-22 [ref 4], FIPS 140-2 [ref 5] or a similar compliance process.	A for all Classes	System	Hardware
2.4.9.3	There is a process for secure provisioning of keys that includes generation, distribution, update, revocation and destruction. For example in compliance with FIPS140-2 [ref 5] or a similar process.	M for Class 2 and above	Business	Process
2.4.9.4	There is a secure method of key insertion that protects keys against copying.	M for Class 1 and above	System	Software
2.4.9.5	All the product related cryptographic functions have no publicly known unmitigated weaknesses, for example MD5 and SHA-1 are not used, e.g. those stipulated in NIST SP800-131A [ref 2].	M for Class 1 and above	Business	Process
2.4.9.6	All the product related cryptographic	M for Class	Business	Process

	functions are sufficiently secure for the lifecycle of the product, e.g. those stipulated in NIST SP800-131A [ref 2].	1 and above		
2.4.9.7	The product stores all sensitive unencrypted parameters, e.g. keys, in a secure, tamper-resistant location.	M for Class 1 and above	System	Hardware
2.4.9.8	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images or support requirement.	A for all Classes	System	Software
2.4.9.9	In device manufacture, all asymmetric encryption private keys that are unique to each device are secured as outlined in FIPS 140-2[ref 5].They must be truly randomly internally generated or securely programmed into each device.	M for Class 2 and above	Business	Process
2.4.9.10	All key lengths are sufficient for the level of assurance required such as detailed in NIST SP800-57 Part 1.	M for Class 2 and above	Business	Policy

2.4.10 Compliance Applicability – Web User Interface

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Web Systems. Guidance is available from the IoTSF [ref 44] regarding Application Security (part E), and Credential Management (Part F).

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.10.1	Where the product or service provides a web based user interface, Strong Authentication is used.	M for Class 1 and above	System	Software
2.4.10.2	Where the product or service provides a web based interface, public and restricted areas shall be separated for authentication.	M for all Classes	System	Software
2.4.10.3	Where the product or service provides a web based management interface, Strong Authentication is used to the web server.	M for Class 1 and above	System	Software
2.4.10.4	Where a web user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	M for Class 1 and above	System	Software
2.4.10.5	The web user interface is protected by an automatic session idle logout timeout function.	M for Class 1 and above	System	Software
2.4.10.6	User passwords are not stored in plain text Strong passwords are required, and a random salt value is incorporated with the password. For further info see the 3GPP TS33.117 Password policy [ref 17], NIST SP800-63b [ref 26] and NCSC [ref 48].	M for Class 1 and above	System	Software
2.4.10.7	Where passwords are entered on a user	M for Class 1	System	Software

	interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	and above		
2.4.10.8	The web user interface shall follow good practice guidelines, such as those listed in the OWASP [Ref 30].	M for Class 1 and above	Business	Policy
2.4.10.9	A vulnerability assessment has been performed before deployment and on an ongoing basis afterwards.	M for Class 1 and above	Business	Process
2.4.10.10	All data being transferred over interfaces should be validated where appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency.	M for all Classes	System	Software
2.4.10.11	Sanitize input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script.	M for all classes	System	Software
2.4.10.12	All inputs and outputs are validated using for example a whitelist containing authorised origins of data and valid attributes of such data.	M for all classes	System	Software
2.4.10.13	Administration Interfaces are accessible only by authorized operators. Mutual Authentication is used over administration interfaces, for example, by using certificates.	M for Class 1 and above	System	Software
2.4.10.14	Reduce the lifetime of sessions to mitigate the risk of session hijacking and replay attacks. For example to reduce the time an attacker has to capture a session cookie and use it to access an application.	M for Class 1 and above	System	Software
2.4.10.15	All inputs and outputs are checked for validity e.g. use “Fuzzing” tests to check for acceptable responses or output for both expected (valid) and unexpected (invalid) input stimuli.	M for Class 1 and above	Business	Process

2.4.11 Compliance Applicability – Mobile Application

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Mobile Application. Guidance is available from the IoTSF [ref 44] regarding Application Security (Part E) and Credential Management (Part F).

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keywords
2.4.11.1	Where an application's user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	M for Class 1 and above	System	Software
2.4.11.2	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy [ref 17] or NIST SP800-63b [ref 26].	M for Class 1 and above	System	Software
2.4.11.3	The mobile application ensures that any related databases or files are either tamper resistant or restricted in their access. Upon detection of tampering of the databases or files they are re-initialised.	M for Class 1 and above	System	Software
2.4.11.4	Where the application communicates with a product related remote server(s), or device, it does so over a secure connection such as a TLS connection using certificate pinning.	M for Class 1 and above	System	Software
2.4.11.5	The product securely stores any passwords using an industry standard cryptographic algorithm, for example see FIPS 140-2 [ref 5].	M for Class 1 and above	System	Software
2.4.11.6	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	M for Class 1 and above	System	Software
2.4.11.7	All data being transferred over interfaces should be validated where appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency.	M for all classes	System	Software
2.4.11.8	Secure administration interfaces: it is important that configuration management functionality is accessible only by authorised operators and administrators. Enforce strong authentication over administration interfaces, for example, by using certificates.	M for Class 1 and above	System	Software

2.4.11.9	All application inputs and outputs are validated using for example a whitelist containing authorised origins of data and valid attributes of such data, see NIST SP 800-167 [ref 34].	M for all classes	System	Software

2.4.12 Compliance Applicability – Privacy

This section's intended audience is for those personnel who are responsible for Data Protection and Privacy regulatory compliance.

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keywords
2.4.12.1	The product/service stores the minimum amount of Personal Information from users required for the operation of the service.	M for All Classes	System Business	Software Policy
2.4.12.2	The product/service ensures that all Personal Information is encrypted (both when stored and if communicated out of the device, see IoTSF guidance [ref 44] Part H on Network Connections	M for Class 1 and above	System Business	Software Policy
2.4.12.3	The product/service ensures that only authorised personnel have access to personal data of users.	M for All Classes	System Business	Software Policy
2.4.12.4	The product/service ensures that Personal Information is anonymised whenever possible and in particular in any reporting.	M for All Classes	System Business	Software Policy
2.4.12.5	The Product Manufacturer or Service Provider shall ensure that a data retention policy is in place and documented for users.	M for Class 1 and above	Business	Policy
2.4.12.6	There is a method or methods for the product owner to be informed about what Personal Information is collected, why, where it will be stored.	M for Class 1 and above	Business	Process
2.4.12.7	There is a method or methods for the product owner to check/verify what Personal Information is collected and deleted.	M for All Classes	System	Software
2.4.12.8	The product / service can be made compliant with the local and/or regional Personal Information protection legislation where the product is to be sold for example GDPR [ref 14].	M for All Classes	System Business	Software Process
2.4.12.9	The supplier or manufacturer of any device shall provide information about how the device(s) functions within the end user's network may affect their privacy.	A for All Classes	Business	Process

2.4.12.10	The supplier or manufacturer of any devices or devices shall provide clear information about how the device(s) shall be setup to maintain the end user's privacy and security.	M for All Classes	Business	Process
2.4.12.11	The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal shall be carried out to maintain the end user's privacy and security.	M for Class 1 and above	Business	Process
2.4.12.12	The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.	M for Class 1 and above	Business	Process
2.4.12.13	Security of devices and services should be designed with usability in mind. Reducing user decision points that may have a detrimental impact on security and privacy.	M for All Classes	System	Software
2.4.12.14	The product or service only records audio/visual data in accordance with the authorization of the user (e.g., no passive recording without explicit authorisation).	M for all classes	System	Software
2.4.12.15	The supplier or manufacturer performs a privacy impact assessment (PIA) to identify Personally Identifiable Information (PII) and design approaches for safeguarding user privacy [ref 49].	A for all classes	Business	Process

2.4.13 Compliance Applicability – Cloud and Network Elements

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Cloud or Network Systems.

Req. No	Requirement	Compliance Class	Primary Keyword	Secondary Keyword
2.4.13.1	All the product related cloud and network elements have the latest operating system(s) security updates implemented and processes are in place to keep them updated.	M for Class 2 and above	Business System	Process Software
2.4.13.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	M for Class 1 and above	System	Software
2.4.13.3	All product related web servers have their webserver HTTP trace and trace methods disabled.	M for Class 1 and above	System	Software
2.4.13.4	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	M for Class 1 and above	System	Software
2.4.13.5	The Product Manufacturer or Service Provider has a process to monitor the relevant security advisories to ensure all the product related web servers use protocols with no publicly known weaknesses.	M for Class 1 and above	Business	Process
2.4.13.6	The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers. For example see guidance at ENISA [ref 27], SSL Labs [ref 29], IETF RFC7525 [ref 28] and NCSC [ref 50].	A for all Classes	System	Software
2.4.13.7	The product related web servers have repeated renegotiation of TLS connections disabled.	M for Class 1 and above	System	Software
2.4.13.8	The related servers have unused IP ports disabled.	M for Class 1 and above	System	Software
2.4.13.9	Where a product related to a webserver encrypts communications using TLS and requests a client certificate, the server(s) only establishes a connection if the client certificate and its chain of trust are valid.	M for Class 1 and above	System	Software
2.4.13.10	Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented. For example, using OWASP [ref 31] or	A for all Classes	System	Software

	similar organisations' certificate and public key pinning guidance.			
2.4.13.11	All the related servers and network elements prevent the use of null or blank passwords.	M for Class 1 and above	System	Software
2.4.13.12				
2.4.13.13				
2.4.13.14	All the related servers and network elements enforce passwords that follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy [ref 17], NIST SP800-63b [ref 26] and NCSC guidance [ref 48].	M for Class 1 and above	System	Software
2.4.13.15	The maximum permissible number of consecutive failed user account login attempts follows the recommendations of 3GPP TS33.117 password policy [ref 17].	M for Class 1 and above	System	Software
2.4.13.16	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms, for example see FIPS 140-2 [ref 5].	M for Class 1 and above	System	Software
2.4.13.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	M for Class 1 and above	System	Software
2.4.13.18	All the related servers and network elements prevent anonymous/guest access except for read only access to public information.	M for Class 1 and above	System	Software
2.4.13.19	If run as a cloud service, the service meets industry standard cloud security principles such as the Cloud Security Alliance [ref 18], NIST Cyber Security Framework [ref 21] or UK Government Cloud Security Principles [ref 24].	A for all Classes	System	Software
2.4.13.20	Where a Product or Services includes any safety critical or life-impacting functionality, the services infrastructure shall incorporate protection against DDOS attacks, such as dropping of traffic or sink-holing. See NIST SP 800-53 SC-5 [ref 32].	M for Class 2 and above	System	Software
2.4.13.21	Where a Product or Service includes any safety critical or life-impacting functionality, the services infrastructure shall incorporate redundancy to ensure service continuity and availability.	M for Class 1 and above	System	Software
2.4.13.22	Input data validation should be	M for Class 1	System	Software

	maintained in accordance with industry practiced methods as per NIST 800-53 SI-10 [Ref 33].	and above		
2.4.13.23	If run as a cloud service, the cloud service TCP based communications (such as MQTT connections) are encrypted and authenticated using the latest TLS standard.	M for Class 1 and above	System	Software
2.4.13.24	If run as a cloud service, UDP-based communications are encrypted using the latest Datagram Transport Layer Security (DTLS).	M for Class 1 and above	System	Software
2.4.13.25	Where device identity and/or configuration registries (e.g. thing shadows) are implemented within a cloud service, the registries are configured to restrict access to only authorised administrators.	M for all Classes	System	Software
2.4.13.26	Product-related cloud services bind API keys to specific IoT applications and are not installed on non-authorised devices.	M for Class 2 and above	System	Software
2.4.13.27	Product-related cloud services API keys are not hard-coded into devices or applications.	M for all Classes	System	Software
2.4.13.28	If run as a cloud service, privileged roles are defined and implemented for any gateway/service that can configure devices.	M for Class 2 and Above	System	Software
2.4.13.29	Product-related cloud service databases are encrypted during storage.	M for all Classes	System	Software
2.4.13.30	Product-related cloud service databases restrict read/write access to only authorized individuals, devices and services.	M for all Classes	System	Software
2.4.13.31	Product-related cloud services are designed using a defence-in-depth architecture consisting of Virtual Private Clouds (VPCs), firewalled access, and cloud-based monitoring.	M for all Classes	System	Software
2.4.13.32	When implemented as a cloud service, all remote access to cloud services is via secure means (e.g., SSH).	M for all Classes	System	Software
2.4.13.33	Product-related cloud services monitor for compliance with connection policies and report out-of-compliance connection attempts.	M for Class 2 and above	System	Software
2.4.13.34	IoT devices should connect to cloud services using edge-to-cloud secure hardware (e.g., zero-touch provisioning).	A for all Classes	System	Hardware

2.4.14 Compliance Applicability – Secure Supply Chain and Production

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Supply Chain.

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.14.1	The product has the entire production test and calibration software used during manufacture erased or removed or secured before the product is dispatched from the factory. This is to prevent alteration of the product post manufacture when using authorised production software, for example hacking of the RF characteristics for greater RF ERP. Where such functionality is required in a service centre, it shall be erased or removed upon completion of any servicing activities.	A for all Classes	System	Software
2.4.14.2	Any hardware design files, software source code and final production software images with full descriptive annotations are stored encrypted in off-site locations or by a 3rd party Escrow service.	A for all Classes	Business	Process
2.4.14.3	In manufacture, all the devices are logged by the product vendor, utilising unique tamper resistant identifiers such as serial number so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.	M for Class 1 and above	Business	Process
2.4.14.4	The production system for a device has a process to ensure that any devices with duplicate serial numbers are not shipped and are either reprogrammed or destroyed.	M for Class 1 and above	Business	Process
2.4.14.5	Where a product includes a trusted Secure Boot process, the entire production test and any related calibration is executed with the processor system operating in its secured boot, authenticated software mode.	A for all Classes	System	Software
2.4.14.6	A securely controlled area and process shall be used for device provisioning where the production facility is untrusted. For example, implements the controls required in Common Criteria EAL5+/6 certification [refs 6, 7, 8 and 9].	A for all Classes	Business	Process
2.4.14.7	A cryptographic protected ownership proof shall be transferred along the supply chain and extended if a new owner is added in the chain. This process shall be based on open standards like Enhanced Privacy ID, Certificates per definition in ISO 20008/20009 [ref 42].	M for Class 1 and above	Business	Process
2.4.14..8	An auditable manifest of all libraries used within the product (open source, etc.) to support informed vulnerability management during deployment is maintained.	A for all classes	Business	Process

2.4.15 Compliance Applicability – Configuration

This section's intended audience is for those personnel who are responsible for the security of the device and IoT Services configurations.

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.15.1	The configuration of the device and any related web services is tamper resistant i.e. sensitive configuration parameters should only be changeable by authorised people (evidence should list the parameters and who is authorised to change).	M for Class 1 and above	Business	Policy
2.4.15.2	The configuration shall be provisioned to the device just in time by authorised services, to replace any existing pre-configuration for secure operation.	M for Class 1 and above	Business	Process

2.4.16 Compliance Applicability – Device Ownership Transfer

This section's intended audience is for those personnel who are responsible for Data Protection and Device Ownership management.

Req. No	Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.16.1	Where a device or devices are capable of having their ownership transferred to a different owner, all the previous owner's Personal Information shall be removed from the device(s) and registered services. This option must be available when a transfer of ownership occurs or when an end user wishes to delete their Personal Information from the service or device.	M for Class 1 and above	Business	Process
2.4.16.2	Where a device or devices user wishes to end the service, all Personal Information shall be removed from the device and related services.	M for Class 1 and above	Business	Process
2.4.16.3	The Service Provider should not have the ability to do a reverse lookup of device ownership from the device identity.	M for Class 2 and above	Business	Process
2.4.16.4	In case of ownership change, the device has an irrevocable method of decommissioning and recommissioning.	M for Class 1and above	System	Software
2.4.16.5	The device registration [ref 16] with the Service Provider shall be secure (method and reasoning needed in evidence).	M for Class 1 and above	Business	Process
2.4.16.6	The device manufacturer ensures that the identity of the device is independent of the end user, to ensure anonymity and comply with relevant local data privacy laws e.g. GDPR [ref 14] in the EU.	M for Class 1 and above	Business	Policy

3 References and Abbreviations

3.1 References & Standards

The following organisations, publications and/or standards have been used for the source of references in this document:

- 3GPP (3rd Generation Partnership Project)
- CSA (Cloud Security Alliance)
- DoD (US Department of Defense)
- ENISA (European Union Agency for Network and Information Security)
- ETSI (European Telecommunications Standards Institute)
- EU (European Union)
- FIPS (US Federal Information Processing Standard)
- GSMA (GSM Association)
- IETF (Internet Engineering Task Force)
- IoTSF (Internet of Things Security Foundation
- ISO (International Standard Organisation)
- JTAG (Joint Test Action Group)
- NCSC (UK National Cyber Security Centre)
- NIST (US National Institute of Standards and Technology)
- OWASP (Open Web Application Security Project)

The following references are used in this document.

1. NIST Special Publication SP800-57 Part 3 Revision 1" NIST Special Publication 800 – 57 Part 3 Revision 1 Recommendation for Key Management Part 3: Application – Specific Key Management Guidance" January 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdfhttp://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
2. NIST Special Publication 800-131A Revision 1 "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" November 2015
3. NIST Special Publication 800-90A Revision 1 "Recommendation for Random Number Generation Using Deterministic Random Bit Generators" June 2015
4. Special Publication 800-22 Revision 1a "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" April 2010
5. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
6. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012 Version 3.1 CCMB-2012-09-001 CCMB-2012-09-003
7. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4 CCMB-2012-09-002
8. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012 Version 3.1 Revision 4
9. Draft Framework for Cyber-Physical Systems; NIST; October 2016

10. UK Government advice on Password Guidance, Simplifying your approach, CESG and CPNI Sept 2015: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf
11. DoDI-8500.2 IA Controls: http://www.dote.osd.mil/tempguide/index.html
12. NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, NIST, April 2010: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
13. Key definitions of the Data Protection Act, ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions
14. Overview of the General Data Protection Regulations (GDPR), ICO: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr
15. Annex J (normative): List of Privacy Attributes and Clause 11 Privacy Protection Architecture using Privacy Policy Manager（PPM)

    http://www.onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf
16. Example of IoT application id registry and possible privacy profile registry

    https://appid.iconectiv.com/appid/#
17. 3GPP TS33.117. Catalogue of general security assurance requirements produced by ESTI https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928
18. Cloud Security Alliance, Cloud Security Alliance is a not-for-profit organization promoting best practices for security assurance within Cloud Computing https://cloudsecurityalliance.org
19. IoTSF Compliance Framework, Compliance Checklist and Vulnerability Disclosure Guidelines can be found https://iotsecurityfoundation.org/best-practice-guidelines
20. NIST National Institute of Standards and Technology www.nist.gov
21. NIST Cyber Security Framework https://www.nist.gov/cyberframework
22. Octave, programming language https://www.gnu.org/software/octave/
23. UK Cyber Essentials: UK government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks https://www.cyberaware.gov.uk/cyberessentials
24. UK Government Cloud Security Principles is for consumers and providers using cloud services https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles
25. IETF – RFC2119 “Key words for use in RFCs to Indicate Requirement Levels” https://www.ietf.org/rfc/rfc2119.txt
26. NIST SP800-63b Revision 1” NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management” June 2017 https://pages.nist.gov/800-63-3/sp800-63b.html
27. ENISA “Algorithms, Key Sizes and Parameters Report – 2013” https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report
28. IETF RFC7525 “Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)” https://tools.ietf.org/html/rfc7525
29. SSL Labs “SSL-and-TLS-Deployment-Best-Practices” 31 March 2017 https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
30. OWASP “Transport Layer Protection Cheat Sheet” https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
31. OWASP Certificate and Public Key Pinning https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

32. NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" – SC-5 Denial of Service Protection

    https://nvd.nist.gov/800-53/Rev4/control/SC-5

33. NIST 800-53, Revision 4, "Security Controls and Assessment Procedures for Federal Information Systems and Organizations" - SI10 Information Input Validation

    https://nvd.nist.gov/800-53/Rev4/control/SI-10

34. NIST Special Publication 800–167 "Guide to Application Whitelisting"

    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

35. NIST SP 800-37 Rev. 1 "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach Risk Management Framework"
    https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final or Otave from ENISA
    https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

36. Supply Chain of Trust by Hayden Povey of Secure Thingz and the IoTSF
    http://www.newelectronics.co.uk/article-images/152099/P18-19.pdf

37. Static Code Analysis Tools https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html

38. Bluetooth Numeric Comparison
    https://csrc.nist.gov/publications/detail/sp/800-121/rev-1/archive/2012-06-11 page 14

39. UK Government Cyber security risk assessment guidance https://www.ncsc.gov.uk/guidance/risk-management-collection

40. NIST Special Publication 800-30 guidance for conducting risk assessments
    https://www.nist.gov/publications/guide-conducting-risk-assessments

41. EU ENISA guidance of Cyber Security Risk Management https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

42. Security Policy ISO/IEC Standards for Vulnerability Disclosures ISO/IEC 29147 and ISO/IEC 30111
    http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip and
    https://www.iso.org/standard/53231.html

43. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008
    https://www.iso.org/standard/57018.html

44. IoTSF Best Practice Guidelines for Connected Consumer Products V1.1
    https://www.iotsecurityfoundation.org/best-practice-guidelines/#ConnectedConsumerProducts includes at time of publication individual guidelines for the following topics:

    A. Classification of data
    B. Physical security
    C. Device secure boot
    D. Secure operating system
    E. Application security
    F. Credential management
    G. Encryption
    H. Network connections
    J. Securing software updates
    L. Logging

L. Software update policy

45. CIA Triad has no original source , but for more info visit: https://www.techrepublic.com/blog/it-security/the-cia-triad
46. Examples of security vulnerability advisory programs: https://www.us-cert.gov/report and https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy
47. Example of memory sensitization:

    SEI CERT C Coding Standard Recommendation MEM03-C: "Clear sensitive information stored in reusable resources" https://wiki.sei.cmu.edu/confluence/display/c/MEM03-C.+Clear+sensitive+information+stored+in+reusable+resources

    ISO/IEC TR 24772:2013 "Information technology -- Programming languages -- Guidance to avoiding vulnerabilities in programming languages through language selection and use"

    "Sensitive Information Uncleared Before Use" https://www.iso.org/standard/61457.html

    Other references:

    MITRE CWE-226 "Sensitive Information Uncleared Before Release" https://cwe.mitre.org/data/definitions/226.html

    CWE-244 "Improper Clearing of Heap Memory Before Release ('Heap Inspection')" https://cwe.mitre.org/data/definitions/244.html
48. NCSC password guidance https://www.ncsc.gov.uk/guidance/password-collection
49. Privacy Impact Assessment advice can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ and https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf
50. NCSC guidance on TLS management https://www.ncsc.gov.uk/guidance/tls-external-facing-services
51. WPA - Wi-Fi Protected Access is the name given to wireless security standard IEEE 802.11i-2004 https://standards.ieee.org/standard/802_11i-2004.html

3.2 Definitions and Abbreviations

For the purposes of the present document, the following abbreviations apply.

3.2.1 Definitions

Anonymity	**In case of market requirements, an anonymous identity is required during ownership transfer. EU data privacy or Germany Privacy Regulations apply.**
Application	Applications (also called end-user programs) are software programs designed to perform a group of coordinated functions or tasks that may vary by installation or model. Examples of IoT applications include a web browser, sensor management, or actuator controller. This contrasts with system software, which executes the operating software of the main processor in the device.
Authentication	Authentication is the process of recognizing an identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are checked with those in the device or within an authentication service.

Boot	The initial process used by the device when turned on that prepares the system for operation (Normally contains low level Secure Boot steps).
Consumer	An end user, and not necessarily a purchaser, in the distribution chain of a good or service who make personal use an IoT device and/or service.
Deployment	The placing of the product into customer trial or service.
Encrypted	Data secured using a recognised algorithm and protected keys so as to be meaningful only if decoded, and decodable only by those with access to the relevant algorithm and keys.
Enterprise	An organisation in business for commercial or not-for-profit purposes that share information technology resources.
Firmware	Computer programs and data stored in hardware – typically in read only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs.
IoT Product Class	Class of network products that all implement a common set of IoTSF defined functions for that particular IOT product.
Interactive Account	Interactive accounts include non-personal accounts such as root, admin, service, batch, superuser or privilege accounts that permit infrastructural changes.
Mutual Authentication	Mutual authentication refers to a security process or technology in which two entities in a communications link verify the origin and integrity of each other before any sensitive data is sent over the connection. In a network, the client authenticates the server and vice-versa. It is a default mode of authentication in some protocols. SSH see https://tools.ietf.org/html/rfc4250) and optional in others: TLS see https://tools.ietf.org/html/rfc8446.
Nonce	Nonce is an abbreviation of the term "number used once. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications messages cannot be reused in replay attacks.
Operating System	An operating system (OS) is system software that manages device hardware and software resources and provides common services for software programs
Onboarding	The method to register a device into its service or solution to enable device registration [ref 16], configuration and data transfer.
Ownership Transfer	In case a device is transferred through a supply chain and changes owner, this method ensures a reliable and secure transfer of ownership.
Personal Information	Personal Information is defined by the EU General Data Protection Regulation (GDPR): https://ec.europa.eu/info/law/law-topic/data-protection_en. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a

	name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Secure Boot	Process that ensures a device only starts software that is trusted by the OEM.
Secure Protocol	The Method to exchanging information during registration and ownership transfer securely and reliably.
Software	Unless otherwise explicitly stated, for the purposes of this document the term software also includes any firmware elements in the product.
Strong Authentication	A procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) Something only the user or device knows, e.g. static password, code, personal identification number; ii) Something only the user or device possesses ,e.g. token, smart card, mobile phone; iii) Something the user or device is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data defined other examples include NIST Special Publication 800-63B see [ref 26] and European Central Bank: Recommendations For The Security Of Internet Payments http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf?95e6bba1ef875877ad3c35cf3b12399c
Supply Chain of Trust	Where an IoT system uses device or service components with more than one source, all sources demonstrate compliance with the relevant requirements of this framework. This will lead to the Devices and services in an IoT system exhibiting the following attributes: • Engender robust Root of Trust and secure identities • Safeguard application code at source Inhibit grey-manufacturing and protect IP • Ensure only valid applications are programmed • Integrate robust key structures for ownership delegation • Enable lifecycle updates and patching
Tamper Evident	The enclosure of the product has measures to ensure that any unauthorised attempt to open it leaves evidence of the attempt, for example, labelling across a product's enclosure joint that fragments when the joint is disturbed.
Tamper Resistant	The enclosure of the product has measures to prevent its unauthorised opening. Typically through the use of specialist fasteners or other features that require the use of specialist tooling, unique to the product.

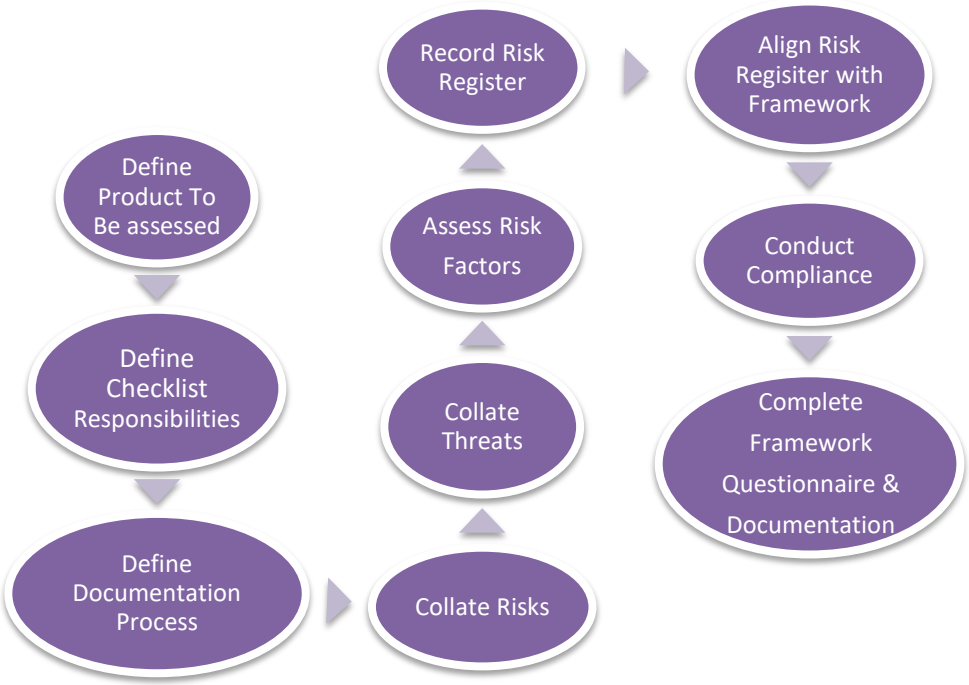
3.2.2 Abbreviations

CoAP	Constrained Application Protocol
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
EAL	Evaluation Assurance Level
ERP	Effective Radiated Power
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
MD	Message Digest
MQTT	Message Queue Telemetry Transport - ISO standard ISO/IEC PRF 20922
OEM	Original Equipment Manufacturer
PRNG	Pseudo Random Number Generator
SHA	Secure Hash Algorithm
SSH	Secure Socket Shell
TRNG	True Random Number Generator
TBC	To Be Confirmed
TBD	To Be Determined
TCP	Transmission Control Protocol
TLS	Transport Layer Security
T3P	Trusted Third Party
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WPS	Wi-Fi Protected Setup

Appendix A Risk Assessment

1. Risk Assessment Steps

The core of the security process is to understand what is being protected and from what or whom. It is also important to identify what is not being protected. There are many ways to accomplish this procedure, but it is recommended to use well known, best practice, risk management standards [Ref 39, 40 and 41]. Risk management techniques can also be found in several common business training publications. An outline of the Risk Assessment process seen in the flow diagram and bullet list below:



- Create a list of security risks to the product
    - Use brainstorming techniques, mind mapping or other Group Creativity techniques.
    - Generate a list covering both business and technical threats:
        - E.g. “Brand Image damage due to adverse publicity”, “cost of product recall”, “product exposes users Wi-Fi credentials”
        - Safety aspects of the product that affect users if the security is compromised
        - The Framework can be used to support the creation of the list of risks by considering the Compliance Class criteria
- Assess the “probability” of each item on the Risk List happening
- Assess the “Cost” (impact in terms of the detectability and recovery) of each item on the Risk List – if it happens

- Multiply the Cost by the Probability, this gives a “Risk Factor”
- Order list by “Risk Factor”. This could be a percentage or simply Probability x Impact

This list becomes the “Risk Register” document and may then be used to guide and justify the work needed to address product security. The aim of the work is to reduce the risk “probability” factor to an acceptable level.

Example of Simplified Risk Register

Threat **High=H, Low =L**	Probability	Impact/Cost	Risk Factor
Encryption and Key Management threats	L	H	LH
Web User Interface threats	H	H	HH
Mobile Application threats	L	L	LL
Privacy threats	L	H	LH

2. Security Objectives and Requirements

The next step is to identify the security objectives and security non-objectives for the product. Items with high risk factors that need mitigation by design are usually considered as security objectives and items with low risk factors for which investment in mitigation is not justified are considered as non-objectives. Each objective must clearly state the asset that needs protection and relevant threats. Any excluded objectives should also be stated and explained, to make clear that they have been considered.

Security requirements are then derived from the security objectives. The main difference between those two is that security objectives specify what need to be protected and security requirements are the means to achieve the required protection. The Security requirements document is a major milestone in the product development life cycle and should be ready before design is started.

3. Security Requirements Design and Implementation

The Security requirements document feeds the design and validation teams. Design methodology of security features is not different from the general design methodology of regular functional requirements. However, this is not true for validation methodology. The aim of the functional requirements validation is to verify that a system is able to do properly what it was designed to do. Security validation shall also try to simulate illegal or unexpected scenarios (e.g. writing to reserved bits in a register or applying an incorrect power up sequence) and verify that a system behaviour is predictable and security assets are not compromised.

www.iotsecurityfoundation.org