Security Foundation

IoT Security Assurance Framework

Release 4.0

af.iotsf.org

IoT Security Foundation
Security Assurance Framework

4.0.0

Table Of Contents:

Version: 4.0

IoT Security Assurance Framework

Release 4.0, November 2021

Notices, Disclaimer, Terms Of Use, Copyright And Trademarks 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, Trademarks And Licensing

Version: 4.0

Acknowledgements

Acknowledgements

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

- Abhay Soorya, Gemserv Ltd
- Alex Margulis, Intel Corp
- Amyas Phillips, Ambotec Ltd
- Andrew Bott, Secure Thingz Ltd
- Arun Sambordaran, Gemserv Ltd
- Chris Hills, Phaedrus Systems Ltd
- Chris Shire, Infineon Technologies Ltd
- David Long, Doulos
- Graham Markall, Embecosm Ltd
- Ian Pearson, Microchip Ltd.
- Ian Phillips, Roke Manor Research Ltd
- Ian Poyner, IoTSF
- Isaac Dangana, Red Alert Labs Ltd
- Jan Krueger, Intel Corp
- Jeff Day, BT plc
- Jeremy Bennett, Embecosm Ltd
- John Moor, IoT Security Foundation
- Lokesh Johri, Tantiv 4
- Mark Beaumont, Roke Manor Research Ltd
- Michael Richardson, Sandelman Software Works
- Nick Hayes, Thinkstream Ltd
- Pamela Gupta, Outsecure Inc
- Peter Burgers, DisplayLink Ltd
- Richard Marshall, Xitex Ltd
- Richard Storer, MathEmbedded Ltd
- Robert Dobson, Device Authority Ltd
- Roger Shepherd, Chipless Ltd
- Sean Gulliford, Gemserv Ltd
- Trevor Hall, Synaptics / DisplayLink Ltd

Peer Reviewers

- Andrew Bott, Secure Thingz Ltd
- Jeff Day, BT Plc
- James Willison, Unified Security Ltd
- Plus others – you know who you are!

Editors

- Ian Pearson, Chair Assurance Framework WG
- Trevor Hall, Co- Chair Assurance Framework WG
- Richard Marshall, Xitex Ltd

Version: 4.0

Introduction

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 Assurance Framework ('Framework') leads its user through a structured process of questioning and evidence gathering. This ensures suitable security mechanisms and practices are implemented. It was previously published as the IoT Security Compliance Framework up until Release 2.1, and this version remains fully backward compatible with the same sections and requirement numbering. The terminology better reflects the risk-based system and is better aligned with how governments and international bodies are approaching IoT security.

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

Since the first version of the Framework was published, various nations have developed legislation covering IoT cybersecurity, this document provided input to some of the regulations. Mapping of the government regulations to the Framework Requirements is being developed giving manufacturers and developers invaluable guidance on how to become compliant to the new legislations.

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 in the section References and Abbreviations.

Version: 4.0

Intended-Audience

1.2 Intended Audience

The Framework can be used internally in an organisation as a pre-compliance tool 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.). Documentary evidence may be assembled using this Framework as a guide or by completing the Assurance Questionnaire (see below 1.4 IoTSF Resources That Support The Framework). In this way, documentary evidence will be compiled to demonstrate assurance 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.

Scope

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 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. In line with regulations, specifically for the software elements of a product a Software Bill of Materials (SBoM) is required by multiple standards and regulations. This provides a hierarchical list and insight into dependencies of a software build usually via a Software Composition Analysis (SCA) tool. The SBoM also provides insight into risk factors within the codebase such as licence infringement, vulnerability exposure and code provenance [NTIA.GOV.SBOM][1] [IOTSF.SBOM][2].

During the development of a new product, the externally sourced components (both software and hardware) should be itemised and recorded in the product design portfolio, The software components are largely external function libraries (mostly Open Source) these can easily be listed using readily available commercial or free SCA scanning tools and generate an SBoM. The SBoMs from the supply chain can be concatenated into a single product master SBOM file. Many countries now require SBOMs to be available under their respective legislation, this has encouraged many large OEMs, retailers and government procurement services to also demand SBOMs as part of any product supplied to them. Automated scans of the product SBOMs enable a risk assessment of the security quality of the components through checking for out-of-date libraries or current CVE (Common Vulnerabilities and Exposures) reports [MITRE.CVE][3]. The resultant audits and risk reviews allow the complete product plus supply chain to be assessed against legislative or customer demands.

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"*** [IOTSF.SCW][4].

Footnotes

1. US National Telecommunications and Information Administration (NTIA) Guidance: "Software Bill Of Materials". https://www.ntia.gov/page/software-bill-materials. ↩

2. IoTSF Whitepaper "The Use of Software Bills of Materials for IoT and OT Devices", Release 1.1.0, February 2023. https://iotsecurityfoundation.org/the-use-of-software-bills-of-materials-for-iot-and-ot-devices/. ↩

3. "CVE® Program Mission". https://www.cve.org/. ↩

4. IoTSF Whitepaper "Securing the Internet of Things Supply Chain" Release 1.0.0, June 2022. https://iotsecurityfoundation.org/wp-content/uploads/2022/06/RELEASE-JUNE-2022-IoTSF-supply-chain-whitepaper-v5.pdf. ↩

Version: 4.0

IoTSF-Resources-That-Support-The-Framework

1.4 IoTSF Resources That Support The Framework

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

- **This Framework** document is a structured list of security requirements intended to aid the evidence gathering process to guide an organisation through assurance.
- The **Assurance Questionnaire** is a companion audit and assessment tool to the Framework to aid the setting of security objectives and thereafter the collection of documentation and evidence. This tool is available as an IoTSF members' benefit, without charge.
- Additional **Best Practice Guidelines** are provided by the Foundation to help understanding of the most important topics [IOTSF.SD-BPG][1].
- IoTSF Vulnerability Disclosure Guidelines [IOTSF.VDISC-BPG][2].
- 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 latest 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 **"Assurance Framework Feedback"**.

1.4.1.1 Assurance Questionnaire

The Assurance Questionnaire has filters on the requirements

1.4.2 Changes From Release 3.0 Of The Framework

Release 4.0 of the IoTSF IoT Security Assurance Framework has seen extensive review and updates to many requirements to provide clarity and/or ensure alignment with current industry practice. The Assurance Framework Questionnaire (available to IoTSF Members) includes expanded mapping to standards that have emerged since the last release.

Highlights for this release:

- Removed: Content of Supply Chain appendix – this is now a separate white paper in the IoTSF portfolio
- Added – Development Infrastructure section covering practices related to development environment security

- Changed Reference numbers to RFC2119 style alphanumeric format

The Assurance Applicability (requirements) elements detailed in section 2.4 and the numbering have been maintained where possible from prior releases of the Framework to maintain consistency.

Footnotes

1. IoTSF "Secure Design Best Practice Guides", Release 2, November 2019. https://iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf. ↩

2. IoTSF "Vulnerability Disclosure Best Practice Guidelines", Release 2.0, September 2021. https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf. ↩

Version: 4.0

The-Process

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 recorded, with supporting statements or evidence. The Assurance Questionnaire is available to IoTSF Members to facilitate evidence collation. 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 assurance process breaks down into a number of steps:

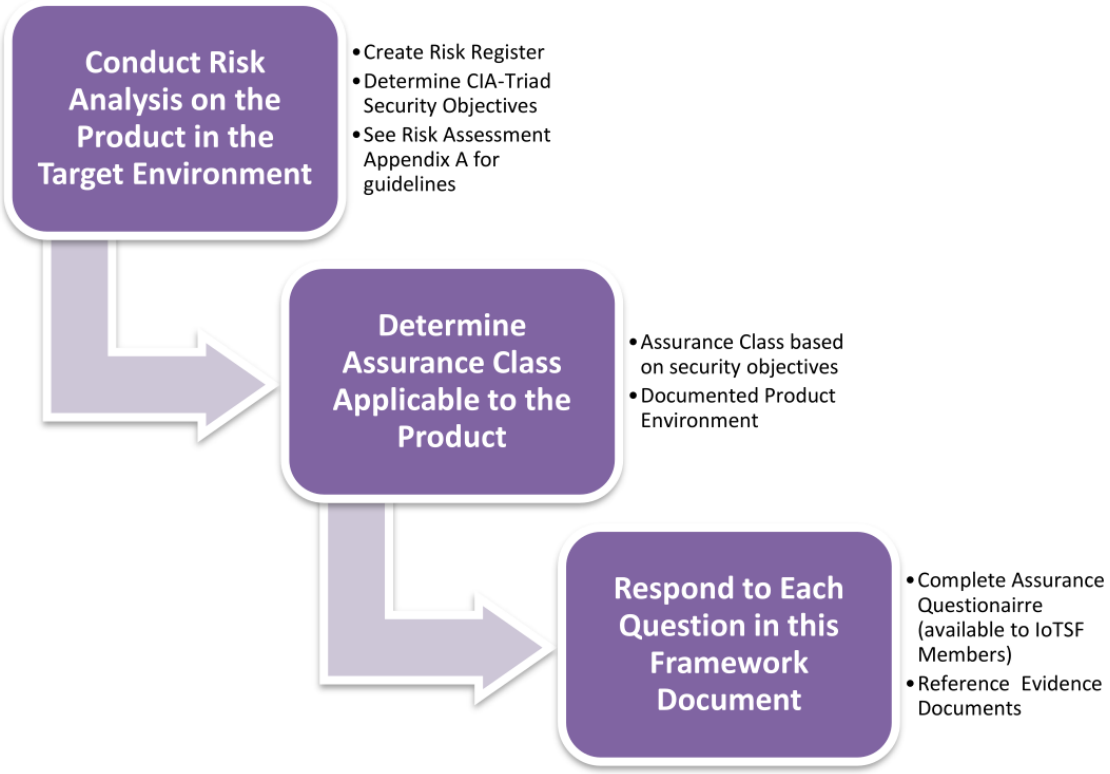

Figure 1 Assurance process steps

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 assurance 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 assurance class for the product/service.

Risk Assessment is a documented process that starts by identifying the key “assets” of a product/service this could be encryption keys, intellectual Property (IP) or personal information (or other items of value). The next stage is to look at possible attacker characteristics and the threat they pose, then finally creation of a risk register table or database with the mitigations for each threat [SCHNEIER.AT][1] [SHOSTACK.TM][2] [TARANDACH.TM][3].

Section 2.2 has more details on assurance classes and how they relate to the Confidentiality, Integrity and Availability, otherwise known as the CIA Triad [VAN.DER.HAM][4] model, commonly used by security professionals. Generally, the highest possible assurance class should be adopted, considering not just the immediate context of the product, but also the potential hazards to the system(s) in the environment where the product/service will be used.

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 [GOV.UK.RISKMAN][5], ENISA [ENISA.RMF][6] and NIST [NIST.SP.800-30][7].

Footnotes

1. Schneier on Security – "Attack Trees" by Bruce Schneier December 1999. https://www.schneier.com/academic/archives/1999/12/attack_trees.html. ↩

2. Book "Threat Modeling: Designing for Security", Adam Shostack, 2014. https://shostack.org/books/threat-modeling-book. ↩

3. Book "Threat Modeling: A Practical Guide for Development Teams", Izar Tarandach & Matthew J. Coles, O'Reilly, 2021. https://threatmodeling.dev/. ↩

4. Jeroen van der Ham, "Toward a Better Understanding of “Cybersecurity”. ACM Digital Threats: Research and Practice , Volume 2, Issue 3, June 2021. https://dl.acm.org/doi/10.1145/3442445. ↩

5. NCSC Guidance "Risk management". https://www.ncsc.gov.uk/collection/risk-management. ↩

6. ENISA "Interoperable EU Risk Management Framework", January 2023. https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework. ↩

7. NIST Special Publication 800-30 "Guide for Conducting Risk Assessments", September 2012. https://www.nist.gov/publications/guide-conducting-risk-assessments. ↩

Version: 4.0

Assurance-Class

2.2 Assurance 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 [VAN.DER.HAM][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 assurance class 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 Assurance Class 1 requirements. However, when deployed into a hospital, with higher threat dependencies, it could be assessed to be under Assurance Class 4 requirements. A further example is provided in section 2.2.1.

In order to apply an appropriate level of security assurance to a product, the requirements in the Framework are classified using the following assurance 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 (requirements in ETSI. DCMS, NCSC CoP demand Class 1 at a minimum)* **Most of the current government guidance and legislation on consumer or commercial products are covered by the Class 1 requirements.**
- *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 Personally identifiable information (PII)*
- *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 assurance class, indicative levels of confidentiality, integrity and availability are shown in **Table 1** below.

Assurance 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: Assurance 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

> [[DODI.8500.2][2], [NIST.SP.800-22][3] and [ICO.DATAP][4] were used as the basis of the above definitions]

Please Note: The Framework Assurance 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 Assurance 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

> It should be noted that almost any connected IoT device will fall under some sort of government or federal legislation and consequently fall into Class 1 or above.

In the case of the thermostat described above, it may be classified as per the table below:

Assurance Class	Security Objective		
	Confidentiality	**Integrity**	**Availability**
Class 1	Basic	Medium	Medium

Table 2: Example of Assurance Class Security Objectives

Footnotes

1. Jeroen van der Ham, "Toward a Better Understanding of “Cybersecurity”. ACM Digital Threats: Research and Practice , Volume 2, Issue 3, June 2021. https://dl.acm.org/doi/10.1145/3442445. ↩
2. Department of Defense Instruction 8500.2, “Information Assurance (IA) Implementation”, E2.1.26 IA Control, February 6, 2003. https://irp.fas.org/doddir/dod/d8500_2.pdf. ↩
3. NIST Special Publication 800-22 Revision 1a, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", April 2010. https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final. ↩
4. Information Commissioner's Office, "Key data protection terms you need to know". https://ico.org.uk/for-organisations/advice-for-small-organisations/key-data-protection-terms-you-need-to-know/. ↩

Using-The-Assurance-Questionnaire

2.3 Using The Assurance Questionnaire

It is anticipated that assurance 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 audit and assessment tool (available to IoTSF Members), the Assurance Questionnaire, may be used at various stages in the product lifecycle. Firstly, by identifying the need for security at the concept stage; secondly listing evidence gathered; to finally signing off security requirements for production release.

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

Once the Assurance Class is determined, the applicable requirements are automatically derived by the accompanying Assurance Questionnaire tool as either mandatory (M) or advisory (A). The Assurance Questionnaire could also be used to optimise the product design and establish if a change would allow a lower Assurance 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 Assessment Methodology

The assessment method is determined by the context i.e. Business (process) or System (technical) and the Class. This determines both the type of assessment e.g. physical testing or document review, along with the degree of rigour from Self-Assessment for lower Classes to full third-party audit for high classes.

2.3.2 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 3*** 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 interchangeable in this document

2.3.3 Assurance Requirements Completion Responsibilities

The Assurance 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 specialist staff as suggested in ***Table 4*** below. Responsibility for any individual requirement may be determined by use of the associated keywords, which can be selected by filter, for users of the Assurance Questionnaire.

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 Hardware	Design and Production staff responsible for security of 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.
2.4.17	Development Infrastructure	Management and staff responsible for Business, Development operations and infrastructure.

Table 4: Assurance Responsibilities

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

The accompanying Assurance Questionnaire allows for entries, against each relevant requirement, of either the evidence gathered to prove assurance 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 be recorded.

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

Req. No	Requirement	Required Assessment Method	Evidence Type	Pre-Assurance	Evidence	Responsibility
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 and makes and monitors the security policy.	SA Document review + TP Inquiry	Organisational Chart and Job role description/documentation and Proof of Competence (certification/attestation)		URL or reference to document with Third party attestation	CIO name
2.4.3.2	There is a person or role, who takes ownership for adherence to this assurance framework process.	SA Document review + TP Inquiry	Organisational Chart and Job role description/documentation and Proof of Competence (certification/attestation)		URL or reference to document with Third party attestation	CIO name
2.4.3.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework, ISO27000 etc.).	SA Document review + TP Inquiry	Policy & process documentation		URL or reference to document with Third party attestation	CIO name

Figure 2: Assurance Questionnaire Partially Completed Example

2.3.4 Evidence

This Framework offers a comprehensive set of security requirements (see section 2.4 under Assurance Applicability) and should be used with the products or services design documentation including the Risk Register. Evidence of the mitigations made to address each risk line item must also be recorded. Users of the Framework should therefore create their own records and IoTSF members are encouraged to use the Assurance Questionnaire for the recording process.

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 assurance 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.

Version: 4.0

Assurance-Terminology-And-Applicability

2.4 Assurance 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 [RFC2119][1].

2.4.2 Level Of Assurance

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” assurance class, this means that the requirement is mandatory for the stated level and all higher levels i.e. 2, 3 & 4.

Footnotes

1. IETF RFC7525, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", May2015. https://tools.ietf.org/html/rfc7525. ↩

Version: 4.0

2.4.3 Business Process

Go to Detailed Requirements

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, which 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 (IOTSF.SD-BPG). The applicability of each requirement is defined as Advisory or Mandatory for the assessed risk level of any device, the default is Advisory.

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.3.1	There is a person or role, accountable to the Board, who takes ownership of and is responsible for product, service and business level security, and mandates and monitors the security policy.	business	responsibility	Mandatory for all classes
2.4.3.2	There is a person or role, who takes ownership for adherence to this assurance framework process.	business	responsibility	Mandatory for all classes
2.4.3.3	Intentionally left blank to maintain requirement numbering			-
2.4.3.4	The company follows industry standard cyber security recommendations.	business	policy	Mandatory for all classes
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.	business	policy	Mandatory for all classes
2.4.3.5.1	The third party policy shall be publicly available and include contact information for reporting issues and information on timelines to acknowledge and provide status updates.	business	policy	Mandatory for all classes
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. At a minimum this should include a threat model, risk analysis and security requirements for the product and its supply chain through its whole stated supported life. This should be maintained, communicated, prioritised and addressed internally as part of product development throughout the product support period.	business	policy	Mandatory for Class 2 and above
2.4.3.7	Processes and plans are in place based upon the IoTSF “Vulnerability Disclosure Guidelines” [IOTSF.VDISC-BPG][1], or a similar recognised process, to deal with the identification of a security vulnerability or compromise when they occur.	business	policy	Mandatory for all classes
2.4.3.8	A process is in place for	business	process	Mandatory for all classes

	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.			
2.4.3.9	There is a secure notification process based upon the IoTSF "Vulnerability Disclosure Guidelines" [IOTSF.VDISC-BPG][1], ISO/IEC 29147 [ISO.IEC.29147][2], or a similar recognised process, for notifying partners/users of any security updates, and what vulnerability is addressed by the update.	business	process	Mandatory for all classes
2.4.3.9.1	There is a minimum support period during which security updates will be made available to all stakeholders.	business	process	Mandatory for all classes
2.4.3.10	A security threat and risk assessment of the entire system shall have been carried out using a standard methodology appropriate to IoT products and services, to determine the risks and evolving threats before a design is started.	business	process	Mandatory for Class 1 and above
2.4.3.11	As part of the Security Policy, include a specific contact and web page for Vulnerability Disclosure reporting.	business	policy	Mandatory for all classes
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.	business	policy	Mandatory for all classes
2.4.3.13	As part of the Security Policy, develop a conflict resolution process for Vulnerability Disclosures.	business	process	Mandatory for all classes
2.4.3.14	As part of the Security Policy, publish the organisation's conflict resolution process for Vulnerability Disclosures.	business	process	Mandatory for Class 1 and above
2.4.3.15	Intentionally left blank to maintain requirement numbering	business		
2.4.3.16	As part of the Security Policy, develop security advisory notification steps.	business	process	Mandatory for all classes
2.4.3.17	The Security Policy shall be	business	policy	Mandatory for Class 3 and

	compliant with ISO/IEC 30111 [ISO.IEC.30111][3] or similar standard.			above
2.4.3.18	Where the a device may be used in real-time or high-availability systems, a procedure must be defined for notifying operators of connected components and system management of impending downtime for updates. In such real time or high availability system the end user should be able to decide whether to automatically install updates or to chose to manually install an update at a time of their choosing (or to ignore an update).	business	process	Mandatory for Class 2 and above
2.4.3.19	Whilst overall accountability for the product or service remains with the person in 2.4.3.1, responsibility can be delegated for each domain involved in any system or device update process, e.g. new binary code to add features or correct vulnerabilities.	business	responsibility	Mandatory for Class 2 and above
2.4.3.20	Responsibility is allocated for control, logging and auditing of the update process.	business	process	Mandatory for Class 2 and above
2.4.3.21	There is a point of contact for third party suppliers and open source communities to raise security issues.	business	process	Mandatory for Class 1 and above
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.	business	process	Mandatory for Class 2 and above
2.4.3.22.1	Users must have the ability to disable updating.	business	process	Mandatory for Class 1 and above
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.	business	policy	Mandatory for Class 2 and above
2.4.3.24	There is a named owner responsible for assessing third party (including open-sourced) supplied components (hardware and software) used in the product	business	responsibility	Mandatory for Class 2 and above
2.4.3.25	Where a remote software upgrade can be supported by the device, there should be a transparent and	business	policy	Mandatory for Class 2 and above

	auditable policy with a schedule of actions of an appropriate priority, to fix any vulnerabilities in a timely manner.			
2.4.3.26	As part of the security policy, define a process for maintaining a central inventory of third party components and services, and their suppliers, for each product.	business	policy	Mandatory for all classes
2.4.3.27	As part of the security policy, define how security requirements on third party components and services (including open-source) will be established and assessed.	business	policy	Mandatory for all classes
2.4.3.28	As part of the procurement policy, a supplier should be awarded a higher score where they demonstrate that they implement secure design in accordance with industry implementation standards or guidelines.	business	policy	Mandatory for all classes
2.4.3.29	The organisation retains an enduring competency to revisit and act upon such information during product upgrades or in the event of a potential vulnerability being identified. (Key security design information and risk analysis is retained over the whole lifecycle of the product or service.)	business	process	Mandatory for all classes

Footnotes

1. IoTSF "Vulnerability Disclosure Best Practice Guidelines", Release 2.0, September 2021. https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf. ↩ ↩2

2. ISO/IEC 29147:2018 "Information technology — Security techniques — Vulnerability disclosure". https://www.iso.org/standard/72311.html. ↩

3. ISO/IEC 30111:2019 "Information technology — Security techniques — Vulnerability handling processes". https://www.iso.org/standard/69725.html. ↩

Version: 4.0

2.4.4 Device Hardware

Go to Detailed Requirements

This section’s intended audience is those personnel who are responsible for hardware and mechanical quality. Guidance is available from the IoTSF (IOTSF.SD-BPG) regarding Physical Security (part B) Device Secure Boot (part C) and Secure Operating Systems (part D).

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.4.1	The product's processor system has an irrevocable hardware Secure Boot process.	System	Hardware	Mandatory for all classes
2.4.4.2	The product's processor system has an irrevocable "Trusted Root Hardware Secure Boot".	System	Hardware	Mandatory for Class 2 and above
2.4.4.3	The product's processor boot process provides an appropriate level of trustworthiness by using a hardware root of trust (RoT) to verify trusted boot or measured boot methods. This may be referred to as 'secure boot', but absolute security cannot be assured.	System	Hardware	Mandatory for Class 3 and above
2.4.4.4	The Secure Boot process is enabled by default.	System	Hardware	Mandatory for all classes
2.4.4.5	Any debug interface only communicates with authorised and authenticated entities on the production devices. (Note: Requirements 2.4.4.6 - 8 should be considered as advisory) The functionality of any interface should be minimised to its essential task(s).	System	Hardware Software	Mandatory for Class 1 and above
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.	System	Hardware	Mandatory for Class 1 and above
2.4.4.7	The hardware incorporates physical, electrical and logical protection against tampering to reduce the attack surface. The level of protection must be determined by the risk assessment.	System	Hardware Physical	Mandatory for Class 2 and above
2.4.4.8	The hardware incorporates physical, electrical & logical protection against reverse engineering. The level of protection must be determined by the risk assessment.	System	Hardware	Mandatory for Class 3 and above
2.4.4.9	All communications port(s) which are not used as part of the product's normal operation are not physically accessible or only communicate with authorised and authenticated entities.	System	Hardware Physical Software	Mandatory for Class 1 and above

2.4.4.10	All the product's development test points are securely disabled or removed wherever possible in production devices.	System	Hardware Physical	Mandatory for Class 2 and above
2.4.4.11	Tamper Evident measures have been used to identify any interference to the assembly to the end user.	System	Hardware	Mandatory for Class 2 and above
2.4.4.12	Intentionally left blank to maintain requirement numbering			-
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.	System	Hardware	Mandatory for Class 1 and above
2.4.4.14	Where the product's 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.	System	Hardware	Mandatory for Class 1 and above
2.4.4.15	Where a production device has 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.	System	Hardware	Mandatory for Class 1 and above
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.	System	Hardware Software	Mandatory for Class 1 and above
2.4.4.17	The product shall have a hardware source for generating true random numbers.	System	Hardware	Mandatory for Class 2 and above

Version: 4.0

2.4.5 Device Software

Go to Detailed Requirements

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 (IOTSF.SD-BPG) regarding Secure Operating Systems (part D), Credential Management (part F), and Securing Software Updates (part J).

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.5.1	The product has measures to prevent unauthorised and unauthenticated software, configurations and files being loaded onto it. If the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.	System	Software	Mandatory for all classes
2.4.5.2	Where remote software updates can be supported by the device, the software images must be digitally signed by an appropriate signing authority - e.g. manufacturer/supplier or public. The Signing Authority should be clearly identified.	System	Software	Mandatory for all classes
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.	System	Software	Mandatory for all classes
2.4.5.4	If remote software upgrade is supported by a device, software images shall be encrypted or transferred over an encrypted channel.	System	Software	Mandatory for Class 2 and above
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 are securely disabled when shipped. When a port is initialised or 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.	System	Software	Mandatory for Class 2 and above
2.4.5.6	To prevent the stalling or disruption of the device's software operation, watchdog timers are present, and cannot be disabled.	System	Hardware Software	Mandatory for Class 1 and above
2.4.5.7	The product's software signing root of trust is stored in tamper-resistant memory.	System	Hardware	Mandatory for Class 1 and above
2.4.5.8	The product has protection against unauthorised reversion of the software to	System	Software	Mandatory for Class 2 and above

	reversion of the software to an earlier and potentially less secure version. Only authorised entities can restore the software to an earlier secure version.			
2.4.5.9	There are measures to prevent the installation of non-production (e.g. development or debug) software onto production devices.	Business	Process	Mandatory for Class 1 and above
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.	Business	Process	Mandatory for Class 1 and above
2.4.5.11	Development software versions have any debug functionality switched off if the software is operated on the product outside of the product vendor's trusted environment.	Business	Process	Mandatory for Class 2 and above
2.4.5.12	Steps have been taken to protect the product's software from sensitive information leakage, including at network interfaces during initialisation, and side-channel attacks.	System	Hardware	Mandatory for Class 3 and above
2.4.5.13	The product's software source code follows the basic good practice of a Language subset coding standard.	Business	Policy	Mandatory for Class 2 and above
2.4.5.14	The product's software source code follows the basic good practice of static vulnerability analysis [NIST.SAMATE][1] by the developer.	Business	Process	Mandatory for Class 2 and above
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.	Business	Process	Mandatory for Class 1 and above
2.4.5.16	Software source code is developed, tested and maintained following defined repeatable processes.	Business	Process	Mandatory for Class 1 and above

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.	Business	Process	Mandatory for Class 2 and above
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.	Business	Process	Mandatory for Class 2 and above
2.4.5.19	Where present, production software signing keys are under access control.	Business	Policy	Mandatory for all classes
2.4.5.20	The production software signing keys are stored and secured in a storage device compliant to FIPS-140-2 [FIPS.140-2][2]/FIPS-140-3 [FIPS.140-3][3] level 2, or equivalent or higher standard.	Business	Policy	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 2 and above
2.4.5.22	For a device with no possibility of a software update, the conditions for and period of replacement support should be clear. A replacement strategy must be communicated to the user, including a schedule for when the device should be replaced or isolated.	Business	Policy	Mandatory for all classes
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.	Business	Process	Mandatory for Class 2 and above
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 connected systems.	System	Software	Mandatory for Class 2 and above
2.4.5.25	Support for partially installing updates is provided for devices whose on-time is insufficient for the complete installation of	System	Software	Advisory for all classes

	a whole update (constrained devices).			
2.4.5.26	Support for partially downloading updates is provided for devices whose network access is limited or sporadic.	System	Software	Advisory for all classes
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, or notifying the user of the priority and duration of the update and with the option of postponing or disabling the update).	System	Software	Mandatory for all classes
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.	System	Hardware Software	Mandatory for all classes
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.	System	Software	Mandatory for all classes
2.4.5.30	An update to a device must be authenticated before it is installed. Where the update fails authentication, the device should, if possible, revert to the last known good (current stable) configuration/software image which was stored on the device.	System	Software	Mandatory for all classes
2.4.5.31	Withdrawn as duplicate requirement			
2.4.5.32	There is secure provisioning of cryptographic keys for updates during manufacture in accordance with industry standards.	Business	Policy	Mandatory for Class 1 and above
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 [CERT-C.MEM03][4], [ISO.IEC.24772][5], [MITRE.CWE-226][6], [MITRE.CWE-244][7]	System	Software	Mandatory for Class 2 and above

2.4.5.34	Any caches which potentially store sensitive material are cleared/flushed after memory locations containing sensitive material have been sanitised.	System	Hardware Software	Mandatory for Class 3 and above
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. At the end of the support period, the device should reduce the risk of a latent vulnerability being exploited. This could be by indicating an error condition to the user or curtailing functionality. This action should be clearly communicated to the user during the procurement stage.	Business	Policy	Mandatory for all classes
2.4.5.36	Updates should be provided for a period appropriate to the device, and this period shall be made clear to a user when supplying the device. Updates should, where possible, be configurable to be automatically or manually installed. The supply chain partners should inform the user that an update is required.	Business	Policy	Mandatory for all classes
2.4.5.37	The device manufacturer should ensure that shared libraries (e.g. Clib or Crypto libraries) that deliver network and security functionalities have been reviewed or evaluated (note that the actual review or evaluation does not have to be conducted by the manufacturer if it has been conducted by another reputable organisation or government entity). Cryptography libraries should be re-reviewed for known security vulnerabilities on each update of the device.	Business	Policy	Mandatory for Class 2 and above
2.4.5.38	Maintenance changes should trigger full security regression testing.	Business	Policy	Mandatory for Class 2 and above
2.4.5.39	IoT devices must allow software updates to maintain security over the product lifetime.	Business	Policy	Mandatory for Class 2 and above

2.4.5.40	Hard-coded critical/security parameters in device software source code shall not be used; if needed these should be injected in a separate (secure) process.	Business	Policy	Mandatory for all classes
2.4.5.41	Where the device is capable, it should check after initialization, and then periodically, whether security updates are available, either autonomously or as part of the support service. Otherwise, the support service should push updates to the device.	Business	Policy	Mandatory for Class 1 and above

Footnotes

1. NIST "Source Code Security Analyzers". https://www.nist.gov/itl/ssd/software-quality-group/source-code-security-analyzers. ↩
2. FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", May 2001. https://csrc.nist.gov/pubs/fips/140-2/upd2/final. ↩
3. FIPS PUB 140-3, "Security Requirements for Cryptographic Modules", Mar 2019. https://csrc.nist.gov/pubs/fips/140-3/final. ↩
4. 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. ↩
5. ISO/IEC 24772-1:2024 "Programming languages — Avoiding vulnerabilities in programming languages" - "7.27 Sensitive information not cleared before use [XZK]", October 2024. https://www.iso.org/standard/83629.html. ↩
6. MITRE CWE-226 "Sensitive Information in Resource Not Removed Before Reuse". https://cwe.mitre.org/data/definitions/226.html. ↩
7. CWE-244 "Improper Clearing of Heap Memory Before Release ('Heap Inspection')". https://cwe.mitre.org/data/definitions/244.html. ↩

Version: 4.0

2.4.6 Device OS

Go to Detailed Requirements

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 (IOTSF.SD-BPG) regarding Secure Operating Systems (part D).

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.6.1	The OS is implemented with relevant security updates prior to release.	Business	Process	Mandatory for Class 2 and above
2.4.6.2	Intentionally left blank to maintain requirement numbering			-
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 and tools.	System	Software	Mandatory for Class 1 and above
2.4.6.4	Files, directories and persistent data are set to minimum access privileges required to correctly function.	System	Software	Mandatory for Class 1 and above
2.4.6.5	Security parameters and passwords should not be hard-coded into source code or stored in a local file. If passwords absolutely must be stored in a local file, then the password file(s) are owned by, and are only accessible to and writable by, the Device's OS most privileged account and are obfuscated.	System	Software	Mandatory for Class 1 and above
2.4.6.6	All OS non-essential services have been removed from the product's software, image or file systems.	System	Software	Mandatory for Class 1 and above
2.4.6.7	All OS command line access to the most privileged accounts has been removed from the OS.	System	Software	Mandatory for Class 1 and above
2.4.6.8	All of the product's OS kernel and services or functions are disabled by default unless specifically required. Essential kernel, services or functions are prevented from being called by unauthorised external product level interfaces and applications.	System	Software	Mandatory for Class 1 and above
2.4.6.9	All software is operated at the least privilege level possible and only has access to the resources needed as controlled through appropriate access control mechanisms.	System	Software	Mandatory for Class 1 and above
2.4.6.10	All the applicable security features supported by the OS are enabled.	System	Software	Mandatory for Class 1 and above

2.4.6.11	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	System	Software	Mandatory for Class 1 and above
2.4.6.12	The OS implements a separation architecture to separate trusted from untrusted applications.	System	Software	Mandatory for Class 2 and above
2.4.6.13	The product's OS kernel is designed such that each component runs with the least security privilege required (e.g. a microkernel architecture), and the minimum functionality needed (2.4.6.6 - 2.4.6.8 requires non-essential components are disabled or removed).	System	Software	Mandatory for Class 2 and above
2.4.6.14	The Product OS should be reviewed for known security vulnerabilities particularly in the field of cryptography prior to each update and after release. Cryptographic algorithms, primitives, libraries and protocols should be updateable to address any vulnerabilities.	System	Software	Mandatory for Class 1 and above
2.4.6.15	As per 2.4.10.5, the user interface is protected by an automatic session idle logout timeout function.	System	Software	Mandatory for Class 1 and above

Version: 4.0

2.4.7 Device Interfaces

Go to Detailed Requirements

This section’s intended audience is for those personnel who are responsible for device security. Guidance is available from the IoTSF Best Practice Guidelines (IOTSF.VDISC-BPG) regarding Credential Management (part F) and Network Connections (part H).

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.7.1	The product prevents unauthorised connections to it or other devices the product is connected to.	System	Software	Mandatory for Class 1 and above
2.4.7.2	The network component and firewall (if applicable) configuration has been reviewed and documented for the required/defined secure behaviour.	Business	Process	Mandatory for Class 1 and above
2.4.7.3	To prevent bridging of security domains within products with network interfaces, forwarding functions should be blocked by default.	System	Software	Mandatory for Class 1 and above
2.4.7.4	Devices support only the versions of application layer protocols that have been reviewed and evaluated against publicly known vulnerabilities.	Business	Process	Mandatory for Class 1 and above
2.4.7.5	If a potential unauthorised change is detected (e.g.: an access fails authentication or integrity checks), the device should alert the user/administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function. Failed attempts should be logged, but without providing any information about the failure to the initiator.	System	Software	Mandatory for Class 1 and above
2.4.7.6	All the product's unused ports (or interfaces) are closed and only the necessary ones are active.	Business	Process	Mandatory for Class 1 and above
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.	Business	Process	Mandatory for all classes
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.	System	Software	Mandatory for Class 1 and above
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.	Business	Policy	Mandatory for all classes

2.4.7.10	For any Wi-Fi connection, WPA-2 AES [IEEE.802.11][1] or a similar strength encryption has been used. Migration to the latest standard should be planned.(e.g. WPA3). Older insecure protocols such as WEP, WPA/WPA2 (Auto), WPA-TKIP and WPA-2 TKIP/AES (Mixed Mode) are disabled.	System	Software	Mandatory for Class 1 and above
2.4.7.11	Where WPA-2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	System	Software	Mandatory for Class 1 and above
2.4.7.12	All network communications keys are stored securely, in accordance with industry standards.	System	Software	Mandatory for Class 1 and above
2.4.7.13	Where a TCP protocol, such as MQTT, is used, it is protected by a TLS connection with no known vulnerabilities.	System	Software	Mandatory for Class 1 and above
2.4.7.14	Where a UDP protocol is used, such as CoAP, it is protected by a DTLS connection with no known vulnerabilities.	System	Software	Mandatory for Class 1 and above
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 [NIST.SP.800-131A][2] or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	Business	Process	Mandatory for Class 1 and above
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.	Business	Process	Mandatory for Class 1 and above
2.4.7.17	Where there is a loss of communications or availability it shall not compromise the local integrity of the device.	System	Software	Mandatory for Class 1 and above
2.4.7.18	The product only initialises and enables the communications interfaces, network protocols, application protocols and network services necessary for the product's operation.	System	Software	Mandatory for Class 1 and above

2.4.7.19	Communications protocols should be latest versions with no publicly known vulnerabilities and/or appropriate for the product.	Business	Policy	Mandatory for Class 1 and above
2.4.7.20	Post product launch, communications protocols should be reviewed throughout the product life cycle against publicly known vulnerabilities and changed to the most secure versions available if appropriate.	Business	Policy	Mandatory for Class 1 and above
2.4.7.21	If a factory reset is made, the device should warn that secure operation may be compromised until updated.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Advisory for all classes
2.4.7.23	Protocol anonymity features are enabled in protocols (e.g., Bluetooth) to limit location tracking capabilities.	System	Software	Advisory for all classes
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.	System	Software	Mandatory for Class 1 and above
2.4.7.25	Following restoration of power or network connection, 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, which collectively could overwhelm a network.	System	Software	Mandatory for Class 1 and above

Footnotes

1. IEEE 802.11i-2004 "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)". ↩

2. NIST Special Publication 800-131A Revision 1, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", November 2015. https://csrc.nist.gov/pubs/sp/800/131/a/r2/final. ↩

Version: 4.0

2.4.8 Authentication & Authorisation

Go to Detailed Requirements

This section's intended audience is for those personnel who are responsible for the security of the IoT systems interfaces and authentication processes. Guidance is available from the IoTSF Best Practice Guides (IOTSF.SD-BPG) regarding Credential Management (part F).

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
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 to bind code and data to a specific device hardware. This is to mitigate threats from cloning and also to ensure authentication may be done assuredly using the device identifier e.g. using a device certificate containing the device identifier.	System	Hardware	Mandatory for all classes
2.4.8.2	Where the product has a secure source of time there is a method of validating its integrity.	System	Software	Mandatory for Class 1 and above
2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is randomly unique for every device in the product family. If a password-less authentication is used the same principles of uniqueness apply.	System	Software	Mandatory for all classes
2.4.8.4	The product does not accept the use of null or blank passwords.	System	Software	Mandatory for all classes
2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	System	Software	Mandatory for all classes
2.4.8.6	Password entry follows industry standard practice on password length, characters from the groupings and special characters.	System	Software	Mandatory for all classes
2.4.8.7	The product has defence against brute force repeated login attempts, such as exponentially increasing retry attempt delays.	System	Software	Mandatory for Class 1 and above
2.4.8.8	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above

2.4.8.10	The access control privileges are defined, justified and documented.	Business	Process	Mandatory for Class 1 and above
2.4.8.11	The product only allows controlled user account access; access using anonymous or guest user accounts is not supported without justification.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Advisory for all classes
2.4.8.13	The product supports having any or all of the factory default user login passwords altered when installed or commissioned.	Business	Process	Mandatory for all classes
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.	Business	Process	Mandatory for Class 1 and above
2.4.8.15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.	System	Software	Mandatory for Class 1 and above
2.4.8.16	The product allows an authorised and complete factory reset of all of the device's authorisation information.	System	Software	Advisory for all classes
2.4.8.17	Where the product has the ability to remotely recover from attack, it should rely on a known good state, to enable safe recovery and updating of the device, but should limit access to sensitive assets until the devices is in a known secure condition.	System	Software	Mandatory for Class 1 and above
2.4.8.18	Devices are provided with a RoT-backed unique authenticable logical identity.	System	Software	Mandatory for Class 1 and above

Version: 4.0

2.4.9 Encryption & Key Management

Go to Detailed Requirements

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 (IOTSF.SD-BPG) regarding Encryption (Part G).

Req No	Requirement	Compliance Class And Applicability
2.4.9.1	Intentionally left blank to maintain requirement numbering	-
2.4.9.2	If present, a true random number generator source has been validated for true randomness.	Mandatory for Class 2 and above
2.4.9.3	There is a process for secure provisioning of security parameters and keys that includes random and individual (unique) generation, distribution, update, revocation and destruction.	Mandatory for Class 2 and above
2.4.9.4	There is a secure method of key insertion that protects keys against copying.	Mandatory for Class 1 and above
2.4.9.5	All the product related cryptographic functions have no publicly known unmitigated weaknesses in the algorithms or implementation, for example MD5 and SHA-1 are not used.	Mandatory for Class 1 and above
2.4.9.6	All the product related cryptographic functions are sufficiently secure for the lifecycle of the product, or cryptographic algorithms and primitives should be updateable ("cryptoagility")".	Mandatory for Class 1 and above
2.4.9.7	The product stores all sensitive unencrypted parameters (e.g. keys) in a secure, tamper-resistant location.	Mandatory for Class 1 and above
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.	Advisory for all classes
2.4.9.9	In device manufacture, all asymmetric encryption private keys that are unique to each device are secured. They must be truly randomly internally generated or securely programmed into each device.	Mandatory for Class 2 and above
2.4.9.10	All key lengths are sufficient for the level of assurance required.	Mandatory for Class 2 and above
2.4.9.11	In systems with many layered sub devices, key management should follow best practice.	Mandatory for all classes

Version: 4.0

2.4.10 Web User Interface

Go to Detailed Requirements

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 (IOTSF.SD-BPG) regarding Application Security (part E), and Credential Management (part F).

Req No	Requirement	Primary Keyword	Compliance Class And Applicability
2.4.10.1	Where the product or service provides a web based user interface, Authentication is secured using current best practice cryptography.	System	Mandatory for Class 1 and above
2.4.10.2	Where the product or service provides a web browser based interface, access to any restricted/administrator area or functionality shall require authentication.	System	Mandatory for Class 1 and above
2.4.10.3	Where the product or service provides a web based management interface, Authentication is secured using current best practice cryptography.	System	Mandatory for Class 1 and above
2.4.10.4	Where a web user interface password is used for login authentication, the initial password or factory reset password is unique for every device in the product family.	System	Mandatory for all classes
2.4.10.5	The web user interface is protected by an automatic session idle logout timeout function.	System	Mandatory for Class 1 and above
2.4.10.6	User passwords are not stored in plain text.	System	Mandatory for all classes
2.4.10.6.1	Strong passwords are required, and a random salt value is incorporated with the password.	System	Mandatory for Class 1 and above
2.4.10.7	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	System	Mandatory for Class 1 and above
2.4.10.8	The web user interface shall follow good practice guidelines.	Business	Mandatory for Class 1 and above
2.4.10.9	A vulnerability assessment has been performed before deployment, and is repeated periodically throughout the lifecycle of the service or product.	Business	Mandatory for Class 1 and above
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.	System	Mandatory for Class 1 and above
2.4.10.11	Sanitise input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script.	System	Mandatory for Class 1 and above
2.4.10.12	All inputs and outputs are validated	System	Mandatory for Class 1 and above

	using for example an allow list (formerly 'whitelist') containing authorised origins of data and valid attributes of such data.		
2.4.10.13	Administration Interfaces are accessible only by authorised operators. Mutual Authentication is used over administration interfaces, for example, by using certificates.	System	Mandatory for Class 1 and above
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).	System	Mandatory for Class 1 and above
2.4.10.15	All inputs and outputs are checked for validity. Tests to include both expected (valid) and unexpected (invalid) input stimuli.	Business	Mandatory for Class 1 and above
2.4.10.16	Web Interfaces should be developed using best practice secure coding techniques and server frameworks.	Business	Mandatory for Class 1 and above
2.4.10.17	Password entry follows industry standard practice.	Business	Mandatory for all classes
2.4.10.18	Web interface should provide a simple method (one to two clicks) to initiate any security update to the end device.	Business	Mandatory for all classes
2.4.10.19	Any personal data communicated between the web interface and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Business	Mandatory for all classes

Version: 4.0

2.4.11 Mobile Application

Go to Detailed Requirements

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 (IOTSF.SD-BPG) regarding Application Security (part E) and Credential Management (part F).

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
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.	System	Software	Mandatory for all classes
2.4.11.2	Password entry follows industry standard practice.	System	Software	Mandatory for all classes
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.	System	Software	Mandatory for Class 1 and above
2.4.11.4	Where the application communicates with a product-related remote server(s), or device, it does so over a secure connection.	System	Software	Mandatory for Class 1 and above
2.4.11.5	The product securely stores any passwords using an industry standard cryptographic algorithm.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above
2.4.11.9	All application inputs and outputs are validated using for example an allowed-list containing authorised origins of data and valid attributes of such data.	System	Software	Mandatory for Class 1 and above
2.4.11.10	Mobile Apps should be	System	Software	Mandatory for Class 1 and

	developed using best practice secure coding techniques and server frameworks.			above
2.4.11.11	App interface should provide a simple method (one to two clicks) to initiate any security update to the end device.	System	Software	Mandatory for Class 1 and above
2.4.11.12	Access to device functionality via a network/web browser interface in the initialized state should only be permitted after successful Authentication using current best practice secure cryptographic modules.	System	Software	Mandatory for Class 1 and above
2.4.11.13	Any personal data communicated between the mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	System	Software	Mandatory for Class 1 and above

Version: 4.0

2.4.12 Privacy

Go to Detailed Requirements

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

Req No	Requirement	Primary Keyword	Compliance Class And Applicability
2.4.12.1	The product/service stores the minimum amount of Personal Information from users required for the operation of the service.	Business	Mandatory for Class 1 and above
2.4.12.2	The product/service ensures that all Personal Information is encrypted for confidentiality (both when stored and if communicated out of the device) and only accessible after successful authentication and authorisation. Note: authentication only proves who you are, but authorisation confirms if you are allowed access to the PI. The cryptography must be of sufficient strength to protect the Personal Information for however long it is expected to be retained (or remain confidential).	Business	Mandatory for Class 3 and above
2.4.12.3	The product/service ensures that only authorised personnel have access to personal data of users.	Business	Mandatory for Class 1 and above
2.4.12.4	The product/service ensures that Personal Information is anonymised whenever possible and in particular in any reporting.	Business	Mandatory for Class 1 and above
2.4.12.5	The Product Manufacturer or Service Provider shall ensure that a data retention policy is in place and documented for users.	Business	Mandatory for Class 1 and above
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 and processed, and by whom and for what purposes. This includes sensing capabilities, such as sound or video recording, biometrics, location, etc.	Business	Mandatory for Class 1 and above
2.4.12.7	There is a method or methods for each user to check/verify what Personal Information is collected.	Business	Mandatory for Class 1 and above
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 [ICO.GDPR][1] [EU.GDPR][2] or NIST PII [NIST.SP.800-122][3].	Business	Mandatory for Class 1 and above
2.4.12.9	The supplier or manufacturer of any device shall provide documented information to end users about how the device(s) functions within the end user's network may affect their privacy.	Business	Advisory for all classes
2.4.12.10	The supplier or manufacturer of any devices or devices shall provide clear information about how the device(s) should be set up to	Business	Mandatory for all classes

	maintain the end user's privacy and security.		
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 or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all personal information from the device and any associated services.	Business	Mandatory for Class 1 and above
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.	Business	Mandatory for Class 1 and above
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 privacy and security).	System	Mandatory for Class 1 and above
2.4.12.14	The product or service only records audio/visual/or any other data in accordance with the authorisation of the user (e.g., no passive recording without explicit authorisation).	System	Mandatory for Class 1 and above
2.4.12.15	The supplier or manufacturer performs a privacy impact assessment (PIA) to identify Personally Identifiable Information (PII) [NIST.SP.800-122][3] and design approaches for safeguarding user privacy compliant with the legal requirements of the user's location (e.g. GDPR [EU.GDPR][2]). This should extend to data gathered via Web APIs from third party platform suppliers.	Business	Advisory for all classes

Footnotes

1. Information Commissioner's Office, "UK GDPR guidance and resources". https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/. ↩

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). ↩ ↩2

3. NIST Special Publication 800-122 "Guide to Protecting the Confidentiality of Personally Easily Identifiable Information (PII)", April 2010. https://csrc.nist.gov/pubs/sp/800/122/final. ↩ ↩2

Version: 4.0

2.4.13 Cloud And Network Elements

Go to Detailed Requirements

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	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
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.	Business	Process	Mandatory for Class 2 and above
2.4.13.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	System	Software	Mandatory for Class 1 and above
2.4.13.3	All product related web servers have their webserver HTTP trace and trace methods disabled.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above
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.	Business	Process	Mandatory for Class 1 and above
2.4.13.6	The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers.	System	Software	Advisory for all classes
2.4.13.7	The product related web servers have repeated renegotiation of TLS connections disabled.	System	Software	Mandatory for Class 1 and above
2.4.13.8	The related servers have unused IP ports disabled.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above
2.4.13.10	Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented.	System	Software	Advisory for all classes

2.4.13.11	All the related servers and network elements prevent the use of null or blank passwords.	System	Software	Mandatory for Class 1 and above
2.4.13.12	Intentionally left blank to maintain requirement numbering			-
2.4.13.13	Intentionally left blank to maintain requirement numbering			-
2.4.13.14	All the related servers and network elements enforce passwords that follows industry good practice.	System	Software	Mandatory for Class 1 and above
2.4.13.15	Brute force attacks are impeded by introducing escalating delays following failed user account login attempts, and/or a maximum permissible number of consecutive failed attempts.	System	Software	Mandatory for Class 1 and above
2.4.13.16	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above
2.4.13.18	All the related servers and network elements prevent anonymous/guest access except for read only access to public information.	System	Software	Mandatory for Class 1 and above
2.4.13.19	If run as a cloud service, the service meets industry standard cloud security principles.	System	Software	Advisory for all classes
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.	System	Software	Mandatory for Class 2 and above
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.	System	Software	Mandatory for Class 1 and above

2.4.13.22	Input data validation should be maintained in accordance with industry best practice methods.	System	Software	Mandatory for Class 1 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.	System	Software	Mandatory for Class 1 and above
2.4.13.24	If run as a cloud service, UDP-based communications are encrypted using the latest Datagram Transport Layer Security (DTLS).	System	Software	Mandatory for Class 1 and above
2.4.13.25	Where device identity and/or configuration registries (e.g., "thing shadows") are implemented to "on-board" devices within a cloud service, the registries are configured to restrict access to only authorized administrators.	System	Software	Mandatory for Class 1 and above
2.4.13.26	Product-related cloud services bind API keys to specific IoT applications and are not installed on non-authorised devices.	System	Software	Mandatory for Class 2 and above
2.4.13.27	Product-related cloud services API keys are not hard-coded into devices or applications.	System	Software	Mandatory for all classes
2.4.13.28	If run as a cloud service, privileged roles are defined and implemented for any gateway/service that can configure devices.	System	Software	Mandatory for Class 2 and above
2.4.13.29	Product-related cloud service databases are encrypted during storage.	System	Software	Mandatory for Class 1 and above
2.4.13.30	Product-related cloud service databases restrict read/write access to only authorized individuals, devices and services.	System	Software	Mandatory for Class 1 and above
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.	System	Software	Mandatory for Class 1 and above
2.4.13.32	When implemented as a cloud service, all remote access to cloud services is via secure means (e.g.	System	Software	Mandatory for Class 1 and above

	SSH).			
2.4.13.33	Product-related cloud services monitor for compliance with connection policies and report out-of-compliance connection attempts.	System	Software	Mandatory for Class 2 and above
2.4.13.34	IoT edge devices should connect to cloud services using secure hardware and services (e.g. TLS using private keys stored in secure hardware).	System	Hardware	Mandatory for Class 1 and above
2.4.13.35	Any personal data communicated between the mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	System	Software	Mandatory for Class 2 and above
2.4.13.36	Subject to user permission, telemetry data from the device should be analysed for anomalous behaviour to detect malfunctioning or malicious activity.	System	Software	Mandatory for Class 2 and above

Version: 4.0

2.4.14 Secure Supply Chain Production

Go to Detailed Requirements

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

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.14.1	Ensure the entire production test and calibration software used during manufacture is 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 removed upon completion of any servicing activities.	System	Software	Mandatory for Class 2 and above
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.	Business	Process	Advisory for all classes
2.4.14.3	In manufacture, all the devices are logged by the product vendor, utilizing 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.	Business	Process	Mandatory for Class 1 and above
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.	Business	Process	Mandatory for Class 1 and above
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.	Business	Process	Advisory for all classes
2.4.14.6	A securely controlled area and process shall be used for device provisioning where the production facility is untrusted.	Business	Process	Advisory for all classes
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 such as	Business	Process	Mandatory for Class 1 and above

	Enhanced Privacy ID, Certificates per definition in ISO 20008/20009 [ISO.IEC.20008][1].			
2.4.14.8	An auditable manifest of all libraries used within the product (open source, etc.) is maintained to inform vulnerability management throughout the device lifecycle and whole of the support period.	Business	Process	Advisory for all classes
2.4.14.9	In manufacture, all encryption keys that are unique to each device are either securely and truly randomly internally generated or securely programmed into each device in accordance with industry standard FIPS140-2 [FIPS.140-2][2] or equivalent. Any secret key programmed into a product at manufacture is unique to that individual device, i.e. no global secret key is shared between multiple devices, unless this is required by a licensing authority.	Business	Process	Mandatory for Class 2 and above
2.4.14.10	An authorised actor in physical possession of a device can discover and authenticate its RoT-backed logical identity e.g. for inspection, verification of devices being onboarded (this may need electrical connection).	Business	Process	Mandatory for Class 2 and above
2.4.14.11	Devices are shipped with readily-accessible physical identifiers derived from their RoT-backed IDs. This is to facilitate both tracking through the supply chain and for the user to identify the device-type/model and SKU throughout the support period.	Business	Process	Mandatory for Class 1 and above
2.4.14.12	IoT devices' RoT-backed logical identity is used to identify them in logs of their physical chain of custody. This is to facilitate tracking through the supply chain.	Business	Process	Mandatory for Class 2 and above
2.4.14.13	Products ship with information (documents or URL) about their operations and normal behaviour e.g. domains contacted, volume of messaging, Manufacturer Usage Description (MUD).	Business	Process	Mandatory for Class 2 and above
2.4.14.14	Procedures for proper disposal of scrap product exist at manufacturing facilities, and compliance is monitored. This is to	Business	Process	Mandatory for Class 2 and above

	prevent scrap entering grey markets.			
2.4.14.15	Production assets are encrypted during transport to the intended production facility, area or system, or delivered via private channel. Examples of production assets include firmware images, device certificate CA keys, onboarding credentials, production tools and manufacturing files.	Business	Process	Mandatory for Class 2 and above
2.4.14.16	Device firmware images and configuration data are secured against unauthorised modification in manufacturing environments, including during programming. If IP protection is required then the images and data need to be protected against unauthorised access.	Business	Process	Mandatory for Class 2 and above
2.4.14.17	Steps have been taken to prevent inauthentic devices from being programmed with confidential firmware images and configuration data. This is to prevent IP theft and reverse engineering.	Business	Process	Mandatory for Class 2 and above
2.4.14.18	Steps have been taken to prevent inauthentic devices from being signed into certificate chains of trust or otherwise onboarded. For example, a policy or checklist describing which devices may be onboarded exists and is followed.	Business	Process	Mandatory for Class 2 and above
2.4.14.19	Device certificate signing keys and other onboarding credentials are secured against unauthorised access. For example, they may be stored encrypted and managed or created by an HSM and delivered by the secure signing process.	Business	Process	Mandatory for Class 2 and above
2.4.14.20	If time critical delivery of products is needed, availability of production resources accessed in real time over the Internet is assured, by providing them with alternative access channels not susceptible to DOS attacks.	Business	Process	Mandatory for all classes
2.4.14.21	Operators of production servers, computers and network equipment keep their software up to date and monitor them for signs of compromise e.g. unusual activity.	Business	Process	Mandatory for Class 2 and above
2.4.14.22	The OEM maintains	Business	Process	Mandatory for Class 2 and

2.4.14.22	The OEM retains authorisation of secure production control methods to prevent a third party manufacturer (CEM etc.) from producing overproduction and/or unauthorised devices.	Business	Process	Mandatory for Class 2 and above
2.4.14.23	The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all personal information from the device and any associated services.	Business	Process	Mandatory for Class 2 and above
2.4.14.24	An end of life disposal process shall be provided to ensure that retired devices are permanently disconnected from their cloud services and that any confidential user data is securely erased from both the device and the cloud services.	Business	Process	Mandatory for Class 1 and above
2.4.14.25	Where contractual supply arrangements and software licence agreements allow, a software bill of materials (SBOM) shall be available and notified (URL) to customers with product documentation.	Business	Process	Mandatory for Class 2 and above

Footnotes

1. ISO/IEC 20008-1:2013 "Information technology — Security techniques — Anonymous digital signatures". https://www.iso.org/standard/57018.html. ↩

2. FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", May 2001. https://csrc.nist.gov/pubs/fips/140-2/upd2/final. ↩

Version: 4.0

2.4.15 Configuration

Go to Detailed Requirements

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	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.15.1	The configuration of the device and any related web services is secure and 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 e.g. Owners / Guests). Sensitive parameters include cryptographic configuration settings.	Business	Process	Mandatory for Class 1 and above
2.4.15.2	Updates to configuration should be provisioned securely and just-in-time, maintaining consistency . Irrelevant components of the configuration must be removed at the same time.	Business	Process	Mandatory for Class 1 and above
2.4.15.3	The manufacturer should provide users with guidance on how to check whether their device is securely set up.	Business	Process	Mandatory for Class 1 and above

Version: 4.0

2.4.16 Device Ownership Transfer

Go to Detailed Requirements

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

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.16.1	Where a device may have its ownership transferred to a different owner, the supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including deletion of all Personal Information from the device and any associated 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.	Business	Process	Mandatory for Class 1 and above
2.4.16.2	Where a device User wishes to dispose of the device or end the service, the supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal or replacement shall be carried out to maintain the end user's privacy and security, including secure erasure of all Personal Information from the device and deletion of personal information from any associated services (other than that required for legitimate reasons such as billing). A clear confirmation is provided to the user. Examples of a user include a renter of accommodation, a vehicle or medical aids.	Business	Process	Mandatory for Class 1 and above
2.4.16.3	The Service Provider should not have the ability to do a reverse lookup of device ownership from the device identity.	Business	Process	Mandatory for Class 1 and above
2.4.16.4	If ownership change is required/allowed, the device must have an irrevocable method of decommissioning and recommissioning.	System	Software	Mandatory for Class 1 and above
2.4.16.5	The device registration with the Service Provider shall use a secure connection.	Business	Process	Mandatory for Class 1 and above
2.4.16.6	The device manufacturer ensures that the exposed identity of the device cannot be linked by unauthorised actors to the end user, to ensure anonymity and comply with relevant local data privacy	Business	Policy	Mandatory for Class 1 and above

	laws e.g. GDPR [EU.GDPR][1] in the EU.			
2.4.16.7	Where transfer of a device to a new end user is supported, user settings and confidential user data on the device should be reliably erasable by triggering a user reset function. This is so the new user can be confident in the device state and also so the previous user can be confident their data has been unrecoverably erased to maintain confidentiality (see alongside 2.4.12.13 and 2.4.12.11).	Business	Policy	Mandatory for Class 1 and above

Footnotes

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). ↩

Version: 4.0

2.4.17 Development Infrastructure

Go to Detailed Requirements

This Section covers the infrastructure requirement needed for a secure development and manufacturing site. The requirements include recommendations for physical security and processes for asset management, development and release for the products.

Req No	Requirement	Primary Keyword	Secondary Keyword	Compliance Class And Applicability
2.4.17.1	A documented Software Development Lifecycle (SDLC): this should be in diagram or words and should cover the security aspects, threats and mitigations	Business	Process	Mandatory for Class 1 and above
2.4.17.2	A documented final release process: There is a controlled release process with unique version tagging, release checklist and stakeholder signoff	Business	Process	Mandatory for Class 1 and above
2.4.17.3	An Asset management policy for security related equipment: There is a controlled record of development hardware equipment, how is the equipment tracked and maintained? e.g. development PCs/Laptops and secure hardware build servers, HSMs etc	Business	Policy	Mandatory for Class 1 and above
2.4.17.4	There is a defined Document Management classification process and management plan for material that contains security related information: Document Marking "Confidential", "Secret" etc and a definition of these classes, along with a management policy for the classes , and staff awareness	Business	Process	Mandatory for Class 1 and above
2.4.17.5	There are Data Backup processes for critical and secret data: There is a process to backup critical code and secret assets. The secret assets should be segregated and backed up securely. The backups should follow backup policy and procedures and should be tested for resilience and recoverability	Business	Process	Mandatory for Class 1 and above
2.4.17.6	Access Control, both Physical and for code repositories, and build artifacts: There is physical security in the office (locked doors, access logs) to limit access to authorised people only. Corporate data networks shall be secured and managed (i.e. secure login, data access control and logs).	Business	Process	Mandatory for Class 1 and above
2.4.17.7	Secure Assets and Key Management: A Policy and process to manage and keep assets secure e.g. secure signing facility, access control logs, audit	Business	Policy	Mandatory for Class 1 and above

	trail of access, policy when assets moved/copied from secure facility			
2.4.17.8	Security Risk Assessment: All work must be covered by an up to date risk assessment (RA), including a process to create and maintain it. The RA is reviewed during the project, and at the release point to accept the severity of all risks based on product expectations and risk appetite.	Business	Process	Mandatory for Class 1 and above
2.4.17.9	Data destruction: There is a policy regarding the lifetime of secure and/or private data and a process for its destruction. This should align with relevant geographic regulations/policies.	Business	Policy	Mandatory for Class 1 and above
2.4.17.10	HR Security Policy: There is a policy and process to manage employees and any authorised visitors (i.e. ID checks, signed agreements on confidentiality, non disclosure, code of conduct, ethics etc) - this should cover both on-boarding and termination.	Business	Policy	Mandatory for Class 1 and above

Version: 4.0

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)

References And Bibliography

3GPP.TS33.117. 3GPP Portal, TS33.117 V19.1.0, "Catalogue of general security assurance requirements", March 2025. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928.

CCPART1V3. "Common Criteria for Information Technology Security Evaluation Part 2: Security functional components", Version 3.1 Revision 4, September 2012. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf.

CCPART3V3. "Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components", Version 3.1 Revision 4, September 2012. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf.

CERT-C.MEM03. 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.

CISA.CIR. CISA "Cybersecurity Incident Response". https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response.

CSA.HOME. Cloud Security Alliance Web Home Page. https://cloudsecurityalliance.org.

DODI.8500.2. Department of Defense Instruction 8500.2, “Information Assurance (IA) Implementation”, E2.1.26 IA Control, February 6, 2003. https://irp.fas.org/doddir/dod/d8500_2.pdf.

ENISA.ALERT. ENISA "Alerts, Warnings and Announcements Best Practices Guide", November 2013. https://www.enisa.europa.eu/sites/default/files/publications/AlertsWarningsAnnouncements_final.pdf.

ENISA.RMF. ENISA "Interoperable EU Risk Management Framework", January 2023. https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

ETSI.EN.303645. ETSI EN 303 645 v2.1.1 "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements" June 2020. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

EU.GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.

FIPS.140-2. FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", May 2001. https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

FIPS.140-3. FIPS PUB 140-3, "Security Requirements for Cryptographic Modules", Mar 2019. https://csrc.nist.gov/pubs/fips/140-3/final.

GOV.UK.CYBER. National Cyber Security Centre (NCSC) "Cyber Essentials" (UK government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks). https://www.ncsc.gov.uk/cyberessentials.

GOV.UK.NCSC. National Cyber Security Centre (NCSC) - Provides cyber security support for consumers and providers of cloud services. https://www.ncsc.gov.uk/.

GOV.UK.PG. UK Government advice, "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.

GOV.UK.PSWD. NCSC guidance: "Password administration for system owners". https://www.ncsc.gov.uk/guidance/password-collection.

GOV.UK.RISKMAN. NCSC Guidance "Risk management". https://www.ncsc.gov.uk/collection/risk-management.

GOV.UK.TLS. NCSC guidance "Using TLS to protect data", July 2021. https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data.

GOV.UK.VDISC-TK. NCSC "Vulnerability Disclosure Toolkit". https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf.

ICO.DATAP. Information Commissioner's Office, "Key data protection terms you need to know". https://ico.org.uk/for-organisations/advice-for-small-organisations/key-data-protection-terms-you-need-to-know/.

ICO.GDPR. Information Commissioner's Office, "UK GDPR guidance and resources". https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

IEEE.802.11. IEEE 802.11i-2004 "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) s.

IOTSF.SBOM. IoTSF Whitepaper "The Use of Software Bills of Materials for IoT and OT Devices", Release 1.1.0, February 2023. https://iotsecurityfoundation.org/the-use-of-software-bills-of-materials-for-iot-and-ot-devices/.

IOTSF.SCW. IoTSF Whitepaper "Securing the Internet of Things Supply Chain" Release 1.0.0, June 2022. https://iotsecurityfoundation.org/wp-content/uploads/2022/06/RELEASE-JUNE-2022-IoTSF-supply-chain-whitepaper-v5.pdf.

IOTSF.SD-BPG. IoTSF "Secure Design Best Practice Guides", Release 2, November 2019. https://iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf.

IOTSF.VDISC-BPG. IoTSF "Vulnerability Disclosure Best Practice Guidelines", Release 2.0, September 2021. https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf.

ISO.IEC.20008. ISO/IEC 20008-1:2013 "Information technology — Security techniques — Anonymous digital signatures". https://www.iso.org/standard/57018.html.

ISO.IEC.24772. ISO/IEC 24772-1:2024 "Programming languages — Avoiding vulnerabilities in programming languages" - "7.27 Sensitive information not cleared before use [XZK]", October 2024. https://www.iso.org/standard/83629.html.

ISO.IEC.29147. ISO/IEC 29147:2018 "Information technology — Security techniques — Vulnerability disclosure". https://www.iso.org/standard/72311.html.

ISO.IEC.30111. ISO/IEC 30111:2019 "Information technology — Security techniques — Vulnerability handling processes". https://www.iso.org/standard/69725.html.

MITRE.CVE. "CVE® Program Mission". https://www.cve.org/.

MITRE.CWE-226. MITRE CWE-226 "Sensitive Information in Resource Not Removed Before Reuse". https://cwe.mitre.org/data/definitions/226.html.

MITRE.CWE-244. CWE-244 "Improper Clearing of Heap Memory Before Release ('Heap Inspection')". https://cwe.mitre.org/data/definitions/244.html.

NIST.8259A. NIST 8259A "IoT Device Cybersecurity Capability Core Baseline", May 2020. https://csrc.nist.gov/pubs/ir/8259/a/final.

NIST.CSF. NIST Cyber Security Framework. https://www.nist.gov/cyberframework.

NIST.HOME. National Institute of Standards and Technology (NIST). https://www.nist.gov/.

NIST.SAMATE. NIST "Source Code Security Analyzers". https://www.nist.gov/itl/ssd/software-quality-group/source-code-security-analyzers.

NIST.SP.1500-201. NIST Special Publication 1500-201, "Framework for Cyber-Physical Systems: Volume 1, Overview", June 2017. https://doi.org/10.6028/NIST.SP.1500-201.

NIST.SP.1800-36. NIST SP 1800-36 "Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management", May 2024, https://csrc.nist.gov/pubs/sp/1800/36/ipd.

NIST.SP.800-121. NIST Special Publication 800–121 Rev. 2 "Guide to Bluetooth Security" - "Numeric Comparison" in "3.1.1.2 Secure Simple Pairing", January 2022. https://csrc.nist.gov/pubs/sp/800/121/r2/upd1/final.

NIST.SP.800-122. NIST Special Publication 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", April 2010. https://csrc.nist.gov/pubs/sp/800/122/final.

NIST.SP.800-131A. NIST Special Publication 800-131A Revision 1, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", November 2015. https://csrc.nist.gov/pubs/sp/800/131/a/r2/final.

NIST.SP.800-167. NIST Special Publication 800–167 "Guide to Application Whitelisting", October 2015. https://csrc.nist.gov/pubs/sp/800/167/final.

NIST.SP.800-22. NIST Special Publication 800-22 Revision 1a, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", April 2010. https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final.

—. NIST Special Publication 800-22, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", April 2010. https://csrc.nist.gov/pubs/sp/800/122/final.

NIST.SP.800-30. NIST Special Publication 800-30 "Guide for Conducting Risk Assessments", September 2012. https://www.nist.gov/publications/guide-conducting-risk-assessments.

NIST.SP.800-37. NIST SP 800-37 Rev.2 "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy", December 2018. https://csrc.nist.gov/pubs/sp/800/37/r2/final.

NIST.SP.800-53.SC-5. NIST Special Publication 800-53, Rev 5.1.1, "Security and Privacy Controls for Federal Information Systems and Organizations" – "SC-5 Denial of Service Protection". https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

NIST.SP.800-53.SI-10. NIST Special Publication 800-53, Rev 5.1.1, "Security and Privacy Controls for Federal Information Systems and Organizations" - "SI-10 Information Input Validation". https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

NIST.SP.800-57P1. NIST Special Publication SP800-57 Part 1, "NIST Special Publication 800–57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General", May 2020. https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final.

NIST.SP.800-57P3. 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. https://csrc.nist.gov/pubs/sp/800/57/pt3/r1/.

NIST.SP.800-63B. 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

NIST.SP.800-90A. NIST Special Publication 800-90A Revision 1, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", June 2015. https://csrc.nist.gov/pubs/sp/800/90/a/r1/final.

NTIA.GOV.SBOM. US National Telecommunications and Information Administration (NTIA) Guidance: "Software Bill Of Materials". https://www.ntia.gov/page/software-bill-materials.

NTPSEC. The Secure Network Time Protocol (NTPSec). https://www.ntpsec.org/.

ONEM2M.TP-2017-0200. OneM2M Technical Presentation, "AppID Registry: A Foundation for Trusted Interoperability", July 2017. https://www.onem2m.org/images/ppt/TP-2017-0200-AppID_Registry_A_Foundation_for_Trusted_Interoperability.pdf.

ONEM2M.TS-0003. OneM2M Technical Specification TS-0003-V2.21.1, "Security Solutions" - "Annex J (normative): List of Privacy Attributes" & "Clause 11 Privacy Protection Architecture using Privacy Policy Manager (PPM)", https://onem2m.org/technical/published-specificatio.

OWASP.ASVS. OWASP "Application Security Verification Standard Version 5.0.0", "V4 API and Web Service", May 2025. https://owasp.org/www-project-application-security-verification-standard/.

OWASP.PIN. OWASP, "Certificate and Public Key Pinning". https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning.

OWASP.TLS-CS. OWASP "Transport Layer Security Cheat Sheet". https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Security_Cheat_Sheet.html.

OWASP.TOP10. OWASP "Top 10 Web Application Security Risks", 2021. https://owasp.org/Top10/.

RFC2119. IETF RFC7525, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", May 2015. https://tools.ietf.org/html/rfc7525.

SCHNEIER.AT. Schneier on Security – "Attack Trees" by Bruce Schneier December 1999. https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

SEI.OCTAVE. "Introduction to the OCTAVE Approach", Alberts C.J. et al, August 2003. https://insights.sei.cmu.edu/library/introduction-to-the-octave-approach/.

SHOSTACK.TM. Book "Threat Modeling: Designing for Security", Adam Shostack, 2014. https://shostack.org/books/threat-modeling-book.

SSLLABS.TLS. SSL Labs "SSL-and-TLS-Deployment-Best-Practices", 15 January 2020. https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices.

TARANDACH.TM. Book "Threat Modeling: A Practical Guide for Development Teams", Izar Tarandach & Matthew J. Coles, O'Reilly, 2021. https://threatmodeling.dev/.

VAN.DER.HAM. Jeroen van der Ham, "Toward a Better Understanding of “Cybersecurity”. ACM Digital Threats: Research and Practice , Volume 2, Issue 3, June 2021. https://dl.acm.org/doi/10.1145/3442445.

Version: 4.0

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 may 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 recognising 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, super user or privilege accounts that permit system configuration 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, such as: SSH (see https://tools.ietf.org/html/rfc4250) and optional in others, such as 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.
On boarding	The method to register a device into its service or solution to enable device registration [NIST.SP.1800-36][2], 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. Other jurisdictions may have different definitions.
Secure Boot	Process that ensures a device only starts software that is trusted by the OEM.
Secure Protocol	The method of exchanging information that ensures protection and reliability of the data (usually though cryptographic techniques).
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 [NIST.SP.800-63B][1] 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 assurance 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, with specialist fasteners or other

	features that require the use of specialist tooling, unique to the product.

3.2.2 Acronyms

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
IoT	Internet of Things
IP	Internet Protocol
MD	Message Digest
MQTT	Message Queue Telemetry Transport – ISO standard ISO/IEC PRF 20922
OEM	Original Equipment Manufacturer
OWASP	Open Web Application Security Project
PRNG	Pseudo Random Number Generator
RoT	Root Of Trust
SBoM	Software Bill of Materials
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

---

1. 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 ↩
2. NIST SP 1800-36 "Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management", May 2024, https://csrc.nist.gov/pubs/sp/1800/36/ipd. ↩

Version: 4.0

Risk-Assessment-Steps

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 [GOV.UK.RISKMAN][1] [NIST.SP.800-30][2] [ENISA.RMF][3]. Risk management techniques can also be found in several common business training publications. An outline of the Risk Assessment process used in this document can be seen in the flow diagram and bullet list below:

Figure 3 Outline risk assessment process steps

- Create a list of valuable assets contained or associated with the product
- 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 to the assets:
        - 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 Assurance 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 number

This list becomes the “Risk Register” document and may then be used to guide and justify the work needed to mitigate the risks to product security. Each time a mitigation task is completed, the probability of the risk happening should be reduced so the risk register can be updated and reordered. The aim of the work is to reduce the risk “probability” factor to an acceptable level.

Example of simplified Risk Register

Threat Description	Probability (0-100%)	Impact/Cost to company of threat happening (0-5)	**Risk Factor**
Compromise of Encryption and Key Management	5%	5	(0.05*5) = 0.25
Web User Interface subversion	90%	4	(0.9*4) =3.6
Mobile Application hacked	15%	2	(0.15*2) = 0.3
Leakage of Private personal data	15%	5	(0.15*5) = 0.75

Table 5

This is showing the biggest risk is the web User Interface, so the priority should be on mitigating this to reduce the probability.

Footnotes

1. NCSC Guidance "Risk management". https://www.ncsc.gov.uk/collection/risk-management. ↩
2. NIST Special Publication 800-30 "Guide for Conducting Risk Assessments", September 2012. https://www.nist.gov/publications/guide-conducting-risk-assessments. ↩
3. ENISA "Interoperable EU Risk Management Framework", January 2023. https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework. ↩

Version: 4.0

Security-Objectives-And-Requirements

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 needs 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.

Version: 4.0

Security-Requirements-Design-And-Implementation

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 can properly do what it was designed to. 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.

The Risk Register should be maintained throughout the project, and the threat probabilities reassessed given the mitigations put in place to reduce the Risk Factor to an Acceptable level.

What is Acceptable? This is a qualitative assessment that needs to be made by the product owner against risk to reputation, customer expectation and cost of rectification in case of a security failure.

Version: 4.0

Appendix B Introduction To Supply Chain Security Requirements

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. A full explanation is provided in the IoTSF publication “Securing the Internet of Things Supply Chain” https://iotsecurityfoundation.org/best-practice-guidelines/

www.iotsecurityfoundation.org