WHITE PAPER: Mapping the IoT Security Foundation's Compliance Framework to ETSI TS 103 645 Standard

February 19

2019

Applying technical controls from the IoT Security Compliance Framework Release 2.0 to meet the ETSI TS 103 645 Standard

IoTSF Working Group Document

© 2019 IoT Security Foundation

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

Notices

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

Terms of Use

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

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

Disclaimer

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

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

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

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

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

Copyright, Trade Marks and Licensing

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

Copyright © 2019, IoTSF. All rights reserved.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit Creative Commons Attribution 4.0 International License.

Applying technical controls from the IoTSF Compliance Framework to meet the ETSI Standard TS 103 645

The IoT Security Compliance Framework [Framework] [ii] was first published in December 2016 by the IoT Security Foundation [IoTSF], and initially targeted at the Consumer/Smart Home markets. The Compliance Framework with its accompanying comprehensive checklist guides a vendor through an assurance process, gathering evidence in a structured process and conforming to contemporary best practice and applicable standards. The Framework has been updated in Release 2.0 in December 2019, so as to encompass all types IoT devices by adopting a risk based assessment process.

In February 2019, European Telecommunications Standards Institute (ETSI) published draft standard "CYBER; Cyber Security for Consumer Internet of Things" [the standard] [i].

The aim of this whitepaper is to show the mapping between the IoTSF Compliance Framework and the ETSI Standard TS 103 645.

The ETSI Standard provides clear, top-level requirements for Consumer devices that need to be met, yet translating these into practice can be technically complex. Many organisations developing IoT products are new to the world of product security design and management. They need a way to:

- Identify and understand the basic product / business security requirements
- Validate those security requirements have been considered / provisioned
- Ensure that security can be maintained over a life-cycle
- Communicate and verify all this to their customers.

This is the IoT Security Foundation's main objective: this white paper is written for Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers. It shows where the detailed requirements in the Compliance Framework correspond to the ETSI standard. It has been prepared using keywords in each of the standard's provisions and finding Framework sections that have relevant requirements.

Any organisation producing or procuring an IoT Product or service may use the Framework to address the requirements in the standard. The first step is to conduct a risk assessment to determine the risk appetite for the product in the proposed application before considering the specific requirements. The IoT product or service can be considered to be of low risk classification where there is no potential for harm should it be compromised or may be pose a critical risk where human life could be endangered.

At the time of writing, IoTSF provides two sets of documents comprising:

- A set of clear and simple Best Practice Guides, for all departments in a company to use as an aide-memoire, defining what they need to do to build security into their products, services and operations. Example: Vulnerability Disclosure Guidelines [iii] and Best Practice Guides [iv].

- The Framework, with an accompanying checklist of all the requirements that need to be assessed, both when a product is developed and put on the market and through its entire life-cycle, to make and keep it secure. These requirements are drafted so as to address every actor in the supply chain for IoT products and services, from the initial provider of technology components (such as processor cores and software modules) right through to the retailer and service provider. The Framework uses a common vocabulary to apply internally and to a supplier base, enabling a "supply chain of trust" to be communicated throughout the industry.

 © 2019 IoT Security Foundation

Cross Reference - ETSI TS 103 645 & IoTSF Compliance Framework

This section provides a detailed cross reference between the ETSI TS 103 645 standard and release 2.0 of the IoTSF Compliance Framework [ii].

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.1	**No universal default passwords**:		The IoTSF provides guidance regarding Credential Management (Part F) and Network Connections (Part H) as part of its best practice guides [iv].
4.1-1	All IoT device passwords must be unique and not resettable to any universal factory default value. Keywords used in mapping • Password • Reset • Unique	2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that should be assessed in regards to password management.
		2.4.8	Authentication and Authorisation: covering the security of the IoT systems interfaces and foundations of authentication. There are 17 requirements covering business processes, system software and system hardware that may need to be assessed, with over 10 directly related to passwords.
		2.4.10	Web User Interface: There are 15 requirements covering business policies, processes and system software that should be assessed in regards to password management.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.2	**Implement a means to manage reports of vulnerabilities:**		IoTSF Vulnerability Disclosure Guidelines [iii] provides manufacturers, integrators, distributors and retailers of IoT products and services with a set of guidelines for handling the disclosure of security vulnerabilities, based on best practice and international standards.
4.2-1	Companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Keywords used in mapping • Vulnerability • Policy • Contact	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
4.2-2	Disclosed vulnerabilities should be acted on in a timely manner.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
4.2-3	Companies should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate as part of the product security lifecycle.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.3	**Keep software updated**		The IoTSF provides advice on; Secure Operating Systems (Part D), Application Security (Part E), Credential Management (Part F), and Software Updates (Part J) as part of its best practice guides [iv].
4.3-1	Software components in internet-connected devices should be securely updateable. Keywords used in mapping • Software • Update • Life cycle	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
4.3-2	The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 related directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
4.3-3	When software components are updateable, updates shall be timely.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.

 © 2019 IoT Security Foundation

		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
4.3-4	When software components are updateable, an end-of-life policy shall be published for devices that 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. This policy shall be published in an accessible way that is clear and transparent to the consumer.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
4.3-5	When software components are updateable, the need for each update should be made clear to consumers and an update should be easy to implement.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
4.3-6	When software components are updateable, updates should, where possible, maintain the basic functioning of the device, which can be critical to remain available during an update.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.

© 2019 IoT Security Foundation

4.3-7	When software components are updateable, the provenance of software updates should be assured and security patches should be delivered over a secure channel.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
4.3-8	For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
4.3-9	For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period of hardware replacement support and an end-of-life policy should be published in an accessible way that is clear and transparent to the consumer.	2.4.3	Business Security Processes, Policies and Responsibilities: There are 25 requirements relevant to personnel who are responsible for governance of business developing and deploying of IoT Devices and related software management.
		2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.

 © 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.4	**Securely store credentials and security sensitive data**		The IoTSF provides advice on; Secure Operating Systems (Part D), Encryption (Part G) and Credential Management (Part F) as part of its best practice guides [iv].
4.4-1	Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable. Keywords used in mapping • Credentials • Sign • Store • Sensitive	2.4.5	Device Software: There are 36 direct requirements covering business processes, system software and system hardware that should be assessed, with over 25 directly related to software updates.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
		2.4.8	Authentication and Authorisation: covering the security of the IoT systems interfaces and foundations of authentication. There are 17 requirements covering business processes, system software and system hardware that should be assessed, with over 10 directly related to passwords.
		2.4.9	Encryption and Key Management for Hardware: There are 9 requirements covering business processes, and system software that should be assessed.
		2.4.11	Mobile Application: There are 9 requirements covering business processes, system software and system hardware that should be assessed.
		2.4.13	Cloud and Network Elements: There are 34 requirements covering business processes, system and software that should be assessed.
		2.4.15	Configuration: Business policies and processes that should be assessed relating to device set up.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.5	**Communicate securely**		The IoTSF provides advice on Network Connections (Part H) as part of its best practice guides [iv].
4.5-1	Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. Keywords used in mapping • Communication • Keys • Encryption • Provisioning	2.4.5	Device Software: There are 34 requirements covering business processes, system software and system hardware that should be assessed, with over 20 directly related to software updates.
		2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that may be need to be assessed with regards to communications management.
		2.4.9	Encryption and Key Management for Hardware: There are 9 requirements covering business processes, and system software that should be assessed.
		2.4.13	Cloud and Network Elements: There are 34 requirements covering business processes and system software that should be assessed.
4.5-2	All keys should be managed securely.	2.4.5	Device Software: There are 34 requirements covering business processes, system software and system hardware that should be assessed, with over 20 directly related to software updates.
		2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that should be assessed with regards to communications management.
		2.4.9	Encryption and Key Management for Hardware: There are 9 requirements covering business processes, and system software that should be assessed.
		2.4.13	Cloud and Network Elements: There are 34 requirements covering business processes and system software that should be assessed.

 © 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.6	**Minimise exposed attack surfaces**		The IoTSF provides advice on Physical Security (Part B), Device Secure Boot (Part C) and Secure Operating Systems (Part D) as part of its best practice guides [iv].
4.6-1	All devices and services should operate on the 'principle of least privilege'; unused ports should be closed, hardware should not unnecessarily expose access. Keywords used in mapping • Access • Attack • Tamper Resistant • Ports • Privilege	2.4.4	Device Hardware & Physical Security: There are 17 requirements covering system software and software that should be assessed to help minimise attack surfaces.
		2.4.5	Device Software: There are 34 business processes, system software and system hardware requirements that should be assessed.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
		2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that should be assessed.
		2.4.8	Authentication and Authorisation: covering the security of the IoT systems interfaces and foundations of authentication. There are 17 requirements covering business processes, system software and system hardware that should be assessed.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.7	**Ensure software integrity**		The IoTSF provides advice on Device Secure Boot (Part C), and Secure Operating Systems (Part D), as part of its best practice guides [iv].
4.7-1	Software on IoT devices should be verified using secure boot mechanisms, which require a hardware root of trust. Keywords used in mapping • Boot • Integrity • Recovery • Authorisation	2.4.4	Device Hardware & Physical Security: There are 17 requirements covering system software and software that should be assessed to help minimise attack surfaces.
		2.4.5.	Device Software: There are 34 business processes, system software and system hardware requirements that should be assessed.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
		2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that should be assessed.
4.7-2	If an unauthorised change is detected to the software, the device should alert the consumer and/or administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.	2.4.4	Device Hardware & Physical Security: There are 17 requirements covering system software and software that should be assessed to help minimise attack surfaces.
		2.4.5.	Device Software: There are 34 business processes, system software and system hardware requirements that should be assessed.
		2.4.6	Device Operating System: These requirements are for the selection of a third-party Operating System or assessing the quality of 'in-house' developed schedulers and control sequencers. They help to ensure technical management of software updates.
		2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that should be assessed.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.8	**Ensure that personal data is protected**		The IoTSF provides advice on Classification of Data (Part A) as part of its best practice guides [iv].
4.8-1	Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers. Keywords used in mapping • Privacy • Personal Data • GDPR	2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.
		2.4.16	Device Ownership Transfer: There are 6 requirements covering business policies, processes and system software that should be assessed.
4.8-2	Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.	2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that may need assessment.
		2.4.16	Device Ownership Transfer: There are 6 requirements covering business policies, processes and system software that should be assessed.
4.8-3	Consumers who gave consent for the processing of their personal data shall be given the opportunity to withdraw it at any time.	2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.
		2.4.16	Device Ownership Transfer: There are 6 requirements covering business policies, processes and system software that should be assessed.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.9	**Make systems resilient to outages**		
4.9-1	Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. Keywords used in mapping • Resilience • Recovery	2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that may that should be assessed with regards to device management.
		2.4.8	Authentication and Authorisation: covering the security of the IoT systems interfaces and foundations of authentication. There are 17 requirements covering business processes, system software and system hardware that should be assessed.
		2.4.13	Cloud and Network Elements: There are 34 requirements covering business processes, system and software that should be assessed.
4.9-2	As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power.	2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that may that should be assessed with regards to device management.
		2.4.8	Authentication and Authorisation: covering the security of the IoT systems interfaces and foundations of authentication. There are 17 requirements covering business processes, system software and system hardware that should be assessed.
		2.4.13	Cloud and Network Elements: There are 34 requirements covering business processes, system and software that should be assessed.
4.9-3	As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power.	2.4.7	Device Wired and Wireless Interfaces: There are 24 requirements covering business policies, processes and system software that may that should be assessed with regards to device management.
		2.4.8	Authentication and Authorisation: covering the security of the IoT systems interfaces and foundations of authentication. There are 17 requirements covering business processes, system software and system hardware that should be assessed.
		2.4.13	Cloud and Network Elements: There are 34 requirements covering business processes, system and software that should be assessed.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.10	**Examine system telemetry data**		The IoTSF provides advice on Logging (Part K) as part of its best practice guides [iv].
4.10-1	If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be examined for security anomalies. Keywords used in mapping • Data • Communications	2.4.3	Business Security Processes, Policies and Responsibilities: specifically requirement 2.4.3.20 - responsibility is allocated for control, logging and auditing of the update process.
		2.4.14	Secure Supply Chain and Production: specifically requirement 2.4.14.3 - in manufacture, all the devices are logged by the product vendor, utilising unique tamper resistant identifiers such as serial number so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.
		2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.
4.10-2	If telemetry data is collected from IoT devices and services, the processing of personal data should be kept to a minimum and such data should be anonymised.	2.4.3	Business Security Processes, Policies and Responsibilities: specifically requirement 2.4.3.20 - responsibility is allocated for control, logging and auditing of the update process.
		2.4.14	Secure Supply Chain and Production: specifically requirement 2.4.14.3 - in manufacture, all the devices are logged by the product vendor, utilising unique tamper resistant identifiers such as serial number so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.
		2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.
4.10-3	If telemetry data is collected from IoT devices and services, consumers shall be provided with information on what telemetry data is collected and the reasons for this.	2.4.3	Business Security Processes, Policies and Responsibilities: specifically requirement 2.4.3.20 - responsibility is allocated for control, logging and auditing of the update process.
		2.4.14	Secure Supply Chain and Production: specifically requirement 2.4.14.3 - in manufacture, all the devices are logged by the product vendor, utilising unique tamper resistant identifiers such as serial number so that cloned or duplicated devices can be identified and either disabled or prevented from being used with the system.
		2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.11	**Make it easy for consumers to delete personal data**		
4.11-1	Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it, when the consumer wishes to remove a service from the device and/or when the consumer wishes to dispose of the device. Keywords used in mapping • Privacy • Control • Ownership	2.4.16	Device Ownership Transfer: There are 6 requirements covering business policies, processes and system software that should be assessed.
		2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.
4.11-2	Consumers should be given clear instructions on how to delete their personal data.	2.4.16	Device Ownership Transfer: There are 6 requirements covering business policies, processes and system software that should be assessed.
		2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.
4.11-3	Consumers should be provided with clear confirmation that personal data has been deleted from services, devices and applications.	2.4.16	Device Ownership Transfer: There are 6 requirements covering business policies, processes and system software that should be assessed.
		2.4.12	Privacy: There are 15 requirements covering business policies, processes and system software that should be assessed.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.12	**Make installation and maintenance of devices easy**		
4.12-1	Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device. Keywords used in mapping • Installation • Lifecycle • Maintenance	2.4.15	Configuration: Business policies and processes that should be assessed relating to device set up.
		2.4.16	Device Ownership Transfer: There are 6 requirements covering business policies, processes and system software that should be assessed.

© 2019 IoT Security Foundation

Provision No.	ETSI TS 103 645 Provision	Framework Section	Requirements and Applicability
4.13	**Validate input data**		
4.13-1	Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated. Keywords used in mapping • User Interface • Authentication	2.4.10	Web User Interface: There 15 requirements covering business policies, processes and system software that should be assessed with regards data management.
		2.4.11	Mobile Application; There are 9 requirements covering business processes, system software and system hardware that should be assessed.

© 2019 IoT Security Foundation

References

i. ETSI, “CYBER; Cyber Security for Consumer Internet of Things”, V1.1.1 February 2019.
https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

ii. IoTSF Compliance Framework: Release 2.0, December 2018.
https://www.iotsecurityfoundation.org/best-practice-guidelines

iii. IoTSF Vulnerability Disclosure Guidelines: Release 1.1, December 2017.
https://www.iotsecurityfoundation.org/best-practice-guidelines

iv. Secure Design Best Practice Guides: Release 1.2.1, December 2018.
https://www.iotsecurityfoundation.org/best-practice-guidelines

© 2019 IoT Security Foundation