



BSI Standards Publication

Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT

National foreword

This British Standard is the UK implementation of ISO/IEC 27404:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/33/4, Security Controls and Services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 25953 7

ICS 35.030; 35.240.95

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



**International
Standard**

ISO/IEC 27404

**Cybersecurity — IoT security and
privacy — Cybersecurity labelling
framework for consumer IoT**

*Cybersécurité — Sécurité et protection de la vie privée pour l'IDO
— Cadre d'étiquetage de cybersécurité pour l'IDO grand public*

**First edition
2025-10**

Reference number
ISO/IEC 27404:2025(en)

Full document details: BS ISO/IEC 27404:2025

© ISO/IEC 2025



Documents
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviated terms	4
5 Overview of cybersecurity labelling for consumer IoT	5
5.1 Cybersecurity labelling for consumer IoT	5
5.2 Guiding principles	5
5.3 Programme objectives	6
5.4 Threats and risks to consumer IoT products	6
5.4.1 General	6
5.4.2 Assumptions	6
5.4.3 Risk considerations and high-level categories	7
5.4.4 Security threats and risks	7
5.4.5 Privacy threats and risks	8
5.5 Relevant standards and guidance documents	9
6 International alignment through a cybersecurity labelling framework	9
6.1 Objectives for international alignment	9
6.2 Determination of cybersecurity requirements through relevant standards and guidance documents	9
7 Requirements and guidance for the components of the cybersecurity labelling framework for consumer IoT	10
7.1 General	10
7.2 Requirements for the cybersecurity labelling framework components	10
7.3 Guidance on the core components of cybersecurity labelling framework	11
7.4 Guidance on key stakeholders' roles and responsibilities	12
7.5 Guidance on binary and multi-level labelling schemes	13
7.5.1 General	13
7.5.2 Binary versus multi-level labelling schemes	13
7.5.3 Basis for levels	14
7.6 Guidance on mutual- and cross-recognition	14
7.6.1 General	14
7.6.2 Benefits	14
7.6.3 Equivalency determination	15
7.7 Guidance on conformity assessment	15
7.7.1 General	15
7.7.2 Assessment activities considerations	15
7.8 Guidance on implementation considerations	16
8 Requirements and guidance for labelling issuance and maintenance for consumer IoT	16
8.1 General	16
8.2 Requirements for labelling issuance and maintenance for consumer IoT	17
8.3 Guidance on acceptance criteria and validation of application	17
8.4 Guidance on label validity	18
8.4.1 Scope of validity	18
8.4.2 Recommendations for labelled consumer IoT products during validity period	18
8.5 Guidance on surveillance and monitoring	18
8.6 Guidance on label maintenance and lifecycle of consumer IoT	19
8.7 Guidance on renewal of labels	19
8.8 Guidance on revocation of labels	19
8.9 Guidance on change of underlying standard	20
8.10 Guidance on label design and characteristics	20

8.10.1	General	20
8.10.2	Label design	20
8.10.3	Label characteristics	21
Annex A	(informative) Types and features of cybersecurity labels	22
Annex B	(informative) Illustrative examples of multi-level labelling schemes	25
Annex C	(informative) Illustrative examples of binary labelling schemes	34
Annex D	(informative) Determination of equivalency among labelling schemes	39
Annex E	(informative) Examples of cybersecurity baseline provisions	47
Annex F	(informative) Examples of security-by-design provisions	58
Annex G	(informative) Examples of privacy assessment requirements	60
Bibliography		62

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Globally, there is an accelerated increase in the number of IoT (Internet of Things) products. Consumer IoT products often have short time-to-market and quick obsolescence lifecycles. Coupled with low price-points and low profit margins for consumer items, it is often the case that such products are not designed or manufactured with adequate cybersecurity provisions, meaning that these products can have fundamental security weaknesses and common flaws. As these connected products proliferate, the lack of adequate provisions for cybersecurity in such products creates extensive attack surfaces, causing them to be susceptible to cyber attacks using malware and penetration testing tools that are easily available.

Consumer IoT labelling schemes are instances of conformity assessment programmes, providing information on whether labelled products are resilient to common cybersecurity attacks. These consumer IoT labelling schemes follow the concepts and functional approach defined in ISO/IEC 17000 and ISO/IEC 17067, providing guidance on essential security traits for consumer IoT that is intended to encourage developers to proactively incorporate cybersecurity when designing their products.

The development of individual consumer IoT labelling schemes, which are designed to address the cybersecurity concerns in a particular region or market, has the potential to create confusion in the international marketplace by making it difficult to compare across labelled products. A cybersecurity labelling framework is therefore needed to help align the concepts and cybersecurity requirements represented by each of the consumer IoT cybersecurity labels.

This document outlines a consumer IoT cybersecurity labelling framework that is intended to reduce the need for duplicative testing, reduce the cost of compliance, and help facilitate a global market for developers. In addition, this framework can help facilitate the development of mutual- and cross-recognition agreements by providing the basis for repeatable and meaningful comparison between the standards- and guidance-based requirements that underpin consumer IoT labelling schemes that use this framework.

The cybersecurity labelling framework facilitates international alignment by providing guidance on selecting relevant standards and guidance documents (e.g. ETSI EN 303 645,^[1] ETSI TS 103 701,^[2] NIST IR 8259,^[3] NIST IR 8259A,^[4] NIST IR 8425,^[5] ISO/IEC 27400, ISO/IEC 27402 and ISO/IEC 27403) for labelling schemes to derive their cybersecurity requirements. Implementing a consumer IoT cybersecurity labelling scheme based on this framework can simplify the mutual- and cross- recognition process. Furthermore, the implementation of cybersecurity labelling schemes, which provide additional specificities (such as test cases and capacities) are complementary to this framework.

The document explains the fundamental concepts of the cybersecurity labelling framework and provides the underlying requirements to help producers and suppliers participate in the process of improving cybersecurity protections for consumer IoT products and to develop products which meet or exceed minimum cybersecurity requirements.

This cybersecurity labelling framework addresses the expected and intended use of consumer IoT products by consumers, that is, the general public and non-technical users. Due to potentially more serious implications if compromised, IoT products used in an enterprise context are not classified as consumer IoT products. Furthermore, threat models of consumer IoT products assume the products are not being centrally managed by a professional system administrator.

The cybersecurity labelling framework provides guidance for binary or multi-level schemes based on common requirements in relevant standards and guidance documents. Products developed referencing these labelling schemes can be mutually- or cross-recognized when scheme owners of the corresponding negotiated schemes have determined that they are compatible. Developers can develop products referencing these labelling schemes, and then achieve mutual- or cross- recognition by examining the interoperability among schemes.

The cybersecurity labelling framework seeks to achieve outcomes in the following aspects:

- Transparency for consumers: The cybersecurity provision of consumer IoT products is opaque to general consumers. The cybersecurity labelling framework for consumer IoT aims to specify the requirements for cybersecurity labelling to make such cybersecurity provisions transparent to consumers, and to enhance consumer awareness of cybersecurity risks. Through the use of cybersecurity labelling, consumers can

make informed choices when purchasing consumer IoT products and adopt a cybersecurity mindset in a digital world.

- Developer branding: Cybersecurity labelling can cultivate a more proactive and sustainable industry, with developers differentiating their products and enhancing their brand quality. It also incentivises developers to produce more secure products and monetise their efforts spent in provisioning cybersecurity in their products.
- Mutual- and cross-recognition for the economy/ecosystem: As the digital economy grows, compatibility of cybersecurity labelling can help to reduce the need for duplicated testing across borders, reduce the cost of compliance for developers for improved market access and pave the way for mutual- or cross-recognition of labelling initiatives across countries.

The cybersecurity labelling framework supports a basis to detail the security features in consumer IoT products. With a framework, scheme owners can specify their labelling schemes, developers are incentivised to identify common requirements and implement better security features, and consumers can make informed purchasing decisions. The result can lead to a safer and more secure cyberspace.

Cybersecurity labelling for consumer IoT products does not offer formal security assurance. Users seeking higher security assurance in sectors such as enterprises, manufacturing, industrial applications and healthcare are recommended to consider products certified under formal evaluation and certification schemes (e.g. as described in ISO/IEC 15408-1).

Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT

1 Scope

This document defines a cybersecurity labelling framework for the development and implementation of cybersecurity labelling programmes for consumer Internet of things (IoT) products. It provides requirements and guidance on the following topics:

- risks and threats associated with consumer IoT products;
- stakeholders, roles and responsibilities;
- relevant standards and guidance documents;
- conformity assessment;
- labelling issuance and maintenance;
- mutual recognition.

This document is limited to consumer IoT products, such as:

- IoT gateways, base stations and hubs to which multiple devices connect; smart cameras, televisions, and speakers;
- wearable devices;
- connected smoke detectors, door locks and window sensors;
- connected home automation and alarm systems;
- connected appliances, such as washing machines and fridges;
- smart home assistants; and
- connected children's toys and baby monitors.

Products that are not intended for consumer use are excluded from this document. Examples of excluded devices are those that are primarily intended for manufacturing, healthcare and other industrial purposes.

This document is applicable to consumers, developers, issuing bodies of cybersecurity labels and conformity assessment bodies.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

binary scheme

labelling scheme with a list of cybersecurity features which must be included for the device to pass and obtain a label

3.2

conformity assessment

demonstration that specified requirements are fulfilled

[SOURCE: ISO/IEC 17000:2020, 4.1, modified — notes to entry have been deleted.]

3.3

conformity assessment programme

conformity assessment scheme

set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing *conformity assessment* (3.2)

Note 1 to entry: A conformity assessment programme can be managed within a conformity assessment system.

Note 2 to entry: A conformity assessment programme can be operated at an international, regional, national sub-national, or industry sector level.

Note 3 to entry: A conformity assessment programme can cover all or part of the conformity assessment functions.

[SOURCE: ISO/IEC 17000:2020, 4.9, modified — “Annex A” has been removed from Note 3 to entry for contextual reasons.]

3.4

conformity assessment body

CAB

body that performs *conformity assessment* (3.2) activities, excluding accreditation

[SOURCE: ISO/IEC 17000:2020, 4.6]

3.5

consumer

natural person who is acting for purposes that are outside their trade, business, craft or profession

Note 1 to entry: This can include a person who is a potential buyer of a labelled product.

3.6

cyber attack

attack

malicious attempts to exploit vulnerabilities in information systems or physical systems in cyberspace and to damage, disrupt or gain unauthorized access to these systems

Note 1 to entry: Expression of an offensive operation in or through the cyberspace leading to unauthorized use of services, creating illicit services, orchestrating denial of service, altering or deleting data or resources.

Note 2 to entry: Common cyber attacks to consumer IoT are basic attacks that could be carried out by script kiddies and amateur hackers.

[SOURCE: ISO/IEC TS 27100:2020, 3.1, modified — Note 2 to entry has been added.]

3.7 developer

entity that creates an assembled final *Internet of things (IoT) device* (3.10) or *IoT product* (3.11)

Note 1 to entry: “Final” in this definition means the stage of delivery to the IoT service developer in the assembly process.

Note 2 to entry: A developer is usually the applicant for a cybersecurity label or the holder of the issued label, i.e. the party responsible for the security characteristics of a product.

3.8 evidence

directly measurable characteristics of an *Internet of things product* (3.11) that represent objective and demonstrable proof that a specific activity satisfies a specified requirement

Note 1 to entry: Test reports, handbooks, files, checklists, scripts or images.

[SOURCE: ISO/IEC 21827:2008, 3.19, modified — “process and/or product” has been replaced with “Internet of things product”; the Example has been added.]

3.9 Internet of Things IoT

infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2024, 3.2.8]

3.10 Internet of Things device IoT device

entity of an *IoT system* (3.13) or *IoT solution* (3.12) that interacts and communicates with the physical world through sensing or actuating

Note 1 to entry: In this document, an IoT device is usually a physical product, which can be bought off the shelf by a consumer, e.g. a router, bulb or toy.

[SOURCE: ISO/IEC 27400:2022, 3.3, modified — note 1 to entry has been added.]

3.11 Internet of Things product IoT product

Internet of Things good or service

Note 1 to entry: A good in this context can take the form of an *IoT device* (3.10), *IoT solution* (3.12), or *IoT system* (3.13) along with bundled software.

Note 2 to entry: Services can include connectivity, cloud computing resources, maintenance, technical support, etc.

3.12 Internet of Things solution IoT solution

seamlessly integrated bundle of technologies, potentially including sensors, gateways and actuators

Note 1 to entry: These can solve a specific problem or need, or they can be used to build additional functionality in other non-IoT solutions.

Note 2 to entry: Within the scope of this document, a solution typically combines hardware components (physical devices like a router, bulb, toy or sensors/actuators) and associated IoT services (e.g. an application for remote control or cloud space) and can be bought e.g. off the shelf by a consumer.

[SOURCE: ISO/IEC 27400:2022, 3.7, modified — note 2 to entry has been added.]

3.13

Internet of Things system

IoT system

system providing functionalities of Internet of Things

Note 1 to entry: IoT system is inclusive of *IoT devices* ([3.10](#)), *IoT solutions* ([3.12](#)), IoT gateways, sensors and actuators.

Note 2 to entry: In the context of this document, this also includes applications and backend that support IoT solutions.

[SOURCE: ISO/IEC 27400:2022, 3.6]

3.14

independent test laboratory

ITL

security testing body that conducts third-party security evaluations of products

3.15

labelling scheme

application or instantiation of the *conformity assessment programme* ([3.3](#)) for the labelling of consumer Internet of Things, taking into account the additional administrative or regulatory requirements of each nation or region

Note 1 to entry: A labelling scheme is an example of a conformity assessment scheme from ISO/IEC 17000.

3.16

object of labelling

Internet of Things product ([3.11](#)) seeking eligibility and currently being assessed for a particular cybersecurity label

3.17

product

any good or service

[SOURCE: ISO 14050:2020, 3.5.12]

4 Abbreviated terms

API	application programming interface
BOM	bill of materials
CAB	conformity assessment body
DAST	dynamic analysis security testing
DDoS	distributed denial of service
HCI	human computer interface
ITL	independent test laboratory
PII	personally identifiable information
SAST	static application security testing

5 Overview of cybersecurity labelling for consumer IoT

5.1 Cybersecurity labelling for consumer IoT

Consumer IoT cybersecurity labelling schemes designed and implemented based on this framework share common elements that contribute to greater cybersecurity outcomes for consumer IoT products within the target market. Furthermore, when this framework is used as the basis for mutual and cross-recognition agreements, these cybersecurity benefits can be realized across jurisdictions and markets.

The development of a consumer IoT cybersecurity labelling scheme involves deliberating on the core components presented in this framework and determining how these components will be employed by the scheme. Developing a labelling scheme involves:

- defining the objectives of the scheme (5.3);
- assessing the threats and risks associated with consumer IoT (5.4);
- identifying stakeholders and roles (7.4);
- selecting relevant standards and guidance documents to serve as the basis for requirements, controls and assessment (5.5 and 6.2);
- defining the type of scheme (single or multi-level) (7.5) and conformity assessment methodology or methodologies (7.7);
- developing the labelling and maintenance process (Clause 8).

5.2 Guiding principles

The guiding principles specified below provide the foundation for this framework and are intended to promote the benefits associated with cybersecurity labelling.

- Appropriateness with product characteristics and profile – The choice of relevant standards and guidance documents, number of labelling levels, conformity assessment options and label characteristics should be appropriate to the type of consumer IoT product, associated threats and risks and intended cybersecurity outcomes.
- Consistency – Labelling schemes leverage standards, guidance documents and conformity assessment programmes for alignment among certification bodies and testing laboratories to:
 - ensure consistency in test and assessment methods,
 - facilitate the acceptance of tests conducted across boundaries, and
 - promote mutual- or cross-recognition.
- Outcomes-based approach – Consumer IoT encompasses a plethora of applications which are developed by a variety of developer organizations. A minimum security baseline can be coupled with flexibility to define additional requirements or security levels to accelerate ecosystem improvements. If multiple labelling levels are available, attaining the requirements of the appropriate level of the cybersecurity labelling scheme are assessed based on outcomes and impact on cybersecurity, with flexibility that allows for additional security functional requirements to be assessed across different products. This can include the degree of quality in the implementation of the IoT device application software and security controls.
- Consumer awareness and understanding – Offering a cybersecurity label can make it easier for consumers to select an IoT product by enabling them to identify which IoT product has been evaluated to a specific security level. This can have a positive impact on the market for secure IoT solutions, thus indirectly helping to increase the overall level of security for the benefit of consumers and network infrastructures. Improving the security design of consumer IoT products can enable consumers to be better protected against cyber attacks. In addition, a visible label will lead to more IoT security awareness with consumers.

5.3 Programme objectives

Programme objectives capture the strategic purpose of a consumer IoT cybersecurity labelling programme and are often stated in terms of desired benefits. Along with the scope of covered consumer IoT products and the risks associated with those products, the programme objectives serve as a basis for selecting standards and guidelines documents that serve as source(s) of technical and non-technical requirements. Programme objectives also provide a way to measure the overall effectiveness of labelling once the programme is operational. In addition, programme objectives can be used as points of comparison when comparing consumer IoT labelling schemes for the purposes of negotiating mutual- and cross-recognition agreements.

Scheme owners can define one or more objectives that align to their strategic outcomes.

Examples of objectives include:

- facilitating IoT product consumers to make informed purchasing decisions;
- reducing the risks associated with consumer IoT products;
- providing a market incentive for IoT product developers to incorporate cybersecurity protection and controls into their consumer IoT products;
- protecting public and private infrastructure from threats associated with consumer IoT products;
- aligning to other consumer IoT labelling schemes, in order to promote cybersecurity and privacy-enhancing benefits across markets and jurisdictions;
- incentivising developer adoption by reducing the need for duplicative testing and assessments.

5.4 Threats and risks to consumer IoT products

5.4.1 General

Consumer IoT is subject to threats and risks beyond those traditionally associated with connected devices. The nature of consumer IoT products is that they are commonly integrated into people's homes and personal spaces, and sometimes even worn on people's bodies. As such, special consideration can be made to ensure that consumer IoT products are safe and secure for use in these conditions.

Threats and risks to consumer IoT products pertain to security and privacy, affecting the confidentiality, integrity and availability attributes of consumer IoT products and services. When considering threats and risks to consumer IoT products, it is important to address both technical vulnerabilities and potential misuse of the technology. For example, some consumer IoT products have recording and remote access components that can, when misused, have a direct impact on consumers' privacy and home networks. In addition, their high computing power and network resources makes them attractive targets for larger-scale exploits, such as botnets.

5.4.2 Assumptions

The following assumptions were used to differentiate risks associated with consumer IoT products from those associated with IoT products and connected devices used in other environments.

- Consumer IoT products are often used by individuals or families in the context of their personal lives.
- By purchasing and using the IoT product, consumers are assuming the product is secure and will not put them at risk.
- Consumer IoT products are most often not employed in managed environments and therefore not subject to enterprise management policies and oversight.
- It cannot be expected that the average consumer possesses a minimum level of cybersecurity knowledge or experience.

- Consumer IoT can be used by vulnerable populations, such as children, the elderly, or persons with mental or physical disabilities.
- A compromised IoT product can impact one or more person's privacy, health, comfort, safety, or wellbeing.

5.4.3 Risk considerations and high-level categories

The risks associated with consumer IoT can be considered from two different perspectives:

- risks to individuals or families, and
- risks to communities or society in general.

Potential risks to individuals or families can include:

- Compromised privacy: Personal or sensitive information that was expected to be confidential is exposed through the use of a consumer IoT product, with potentially harmful impacts to the subject(s) of that information.
- Civil liberties: Information is obtained from the use of a consumer IoT product, which is then used to deny a person or persons fair treatment or access to benefits, rights, or services to which they are legitimately entitled.
- Well-being: The effects of a compromised consumer IoT product negatively impact the psychological, social, or physical well-being of a person or persons.
- Physical safety: The use of a consumer IoT product results in injury or death.

Potential risks to communities or society can include:

- Public safety: A compromised consumer IoT product impacts the safety of people in a public context.
- Public and private services: One or more compromised consumer IoT products are used to affect the confidentiality, availability or integrity of a public or private service, such as in the case of a DDoS attack.
- National security: Data collected from consumer IoT products is used to compromise some aspect of national security, such as the aggregation of anonymised data to identify a secret location or expose confidential information.

5.4.4 Security threats and risks

The security threats and risks associated with consumer IoT products can include:

- Weak credential management and authentication: Weak credential management and a lack of multi-factor authentication for the user and administrative interfaces of products, devices, gateways or back-ends is a common vulnerability.

EXAMPLE Consumer IoT products that do not require users to change default usernames (e.g. "admin") and passwords on first use are easy targets for attackers.

- Security vulnerabilities in product software: Consumer IoT products depend on software that can contain poor design choices or security bugs such as buffer overflows and improper exception handling. This makes them vulnerable to many different attacks that can compromise data confidentiality or integrity. Vulnerable software in products can be exploited by hackers to gain unauthorized access, launch attacks, or take control of the product. Furthermore, it is possible that developers do not provide timely security updates or patches, leaving products vulnerable to newly discovered vulnerabilities.
- Malware: Products can be infected with programmes designed to carry out unauthorized actions on a system, possibly using existing vulnerabilities in software or firmware. This can inflict significant damage as the infection of one product can potentially impact other products and systems in the same network.

- Denial of Service: Consumer IoT products are susceptible to denial of service attacks launched by attackers sending continuous requests to deplete product resources. On the other hand, compromised products can themselves be recruited by botnets and used to disrupt the operation of other networks or systems via a DDoS attack.
- Eavesdropping: If the communication channel is not sufficiently protected with encryption or authentication, communication over an IoT network can be intercepted, deciphered and tampered with (e.g. security parameters, or configuration settings). Related attacks include man-in-the-middle, session hijacking, or message replay. This can affect the confidentiality and integrity of data in consumer IoT products.
- Supply chain and third-party threats: Compromised components or software from third-party suppliers can introduce vulnerabilities.
- Weak physical security measures: Lack of secure hardware design can make it easier for attackers to physically manipulate or tamper with products.

5.4.5 Privacy threats and risks

The privacy threats and risks to consumer IoT products can include:

- Unauthorized access and data leakage: Inadequate data protection measures can result in unintended data sharing to unauthorized parties, leading to privacy breaches. Confidential data can be captured by an attacker from individual devices (at rest), during transit, or from the back-end.
- Device and user tracking: Device location tracking poses a privacy risk to users as an attacker can infer sensitive information from data gathered and communicated by devices. Such information can be sold to interested parties for marketing purposes or used for unauthorized surveillance. Furthermore, it is possible that devices do not adhere to necessary privacy regulations, putting consumers and their confidential data (medical, financial, PII) at risk.
- Manipulation or intimidation: Data collected or processed by a consumer IoT product has been altered in order to manipulate a person's behaviour. An example is the alteration of health data, which can result in a person not taking medical action when it is actually necessary. The configuration or functioning of a consumer IoT product can also be changed without the user's knowledge or permission, for example, by overriding the settings on a smart refrigerator and causing medicines or food to spoil. A consumer IoT product's functionality can also be reconfigured to intimidate or threaten the user, for example, by taking over the speaker function of a baby monitor and using it to make threatening or offensive speech.
- Overcollection: Data are collected or processed by a consumer IoT product without end user notification. For example, a microphone can be set to be always on rather than when triggered. This type of overcollection violates the core privacy principles of data minimization and transparency.

To mitigate the risks arising from such threats, it is important for cybersecurity labelling schemes to specify:

- requirements for consumer IoT products,
- how compliance with such requirements are assessed; and
- the roles and responsibilities of key stakeholders throughout the entire labelling issuance and maintenance lifecycle.

Consumer IoT cybersecurity labelling schemes play a valuable role in encouraging developers to employ cybersecurity and privacy-protecting capabilities to help protect consumers and the public infrastructure from risks associated with these products. Furthermore, mutual- or cross-recognition among labelling schemes ensures these cybersecurity and privacy-enhancing benefits are maintained across markets and jurisdictions.

5.5 Relevant standards and guidance documents

Consumer IoT cybersecurity labelling schemes can reference one or more standards, technical specifications or guidance documents as the basis for their technical and non-technical (business process) requirements. The selection of standards and guidance documents is based on the following considerations.

- The document is an international, regional or national standard, technical specification, or guidance document.
- The document supports the consumer IoT cybersecurity labelling scheme's stated objectives and outcomes.
- The document is relevant to the consumer IoT products covered by the labelling scheme.
- The document is used by other consumer IoT cybersecurity labelling schemes and can facilitate alignment with those schemes.

Examples of relevant standards and guidance documents are provided in [6.2](#). See References [\[1\]](#) to [\[9\]](#).

6 International alignment through a cybersecurity labelling framework

6.1 Objectives for international alignment

At present, a large number of consumer IoT products from different developers are already connected to the Internet. To test and evaluate at such a scale is beyond the ability of a single labelling authority or organization, making international collaboration necessary. It is therefore important that schemes developed for labelling be transferable and facilitate mutual- or cross-recognition agreements internationally. To aid such mutual- and cross-recognition, a high-level classification of potential IoT product cybersecurity requirements is provided in [Annex D](#).

If this approach to international alignment is followed, it can achieve the following objectives.

- Eradicate duplicated testing – The schemes are well-documented, using standard terminology and clearly described requirements, that can be matched or aligned with relevant standards and guidance documents. This can facilitate mutual- or cross-recognition agreements on conformity assessment as well as interoperable schemes, alleviating the need for repeated testing across different schemes and jurisdictions.
- Improve market access – The labelling process, markings and actual labels used can meet the requirements of different markets to avoid technical barriers of trade. Information to be displayed on the label should be determined according to the requirements of target markets. International recognition for the cybersecurity label can help product developers gain access to additional markets.
- Increase industry and market buy-in – In addition to the assessment and labelling process, developers and consumers should be educated on the concepts behind the labels to incentivise product developers to produce more secure products and to empower consumers to be cybersecurity-minded and make informed choices when purchasing consumer IoT products. As consumers start to demand for more cybersecure consumer IoT products, developers are able to monetise their efforts in providing cybersecurity in their products, thus strengthening brand quality.

All these factors can contribute to the increase in the overall hygiene level of cybersecurity for the products deployed, improving security in cyberspace and reducing risks for consumers using consumer IoT products.

6.2 Determination of cybersecurity requirements through relevant standards and guidance documents

By adopting relevant standards and guidance documents as the basis for technical and non-technical requirements of consumer IoT products, scheme owners can simplify the mutual- and cross-recognition process.

ETSI EN 303 645,^[1] NIST IR 8259,^[3] NIST IR 8259A,^[4] NIST IR 8425,^[5] ISO/IEC 27400, ISO/IEC 27402 and ISO/IEC 27403 are examples of documents that seek to address common IoT problems. Each document describes the capabilities that secure consumer IoT products should have. Scheme owners select standards and guidance documents based on their scheme objectives, in-scope consumer IoT products, and associated risks.

In one possible scenario where a multi-level scheme is used, products at higher level labels can demonstrate achieving more capabilities and offer a higher burden of proof or conformity to additional provisions provided in the adopted document. Examples of how higher level labels incorporate a greater number of provisions of an underlying standards and guidance document are provided in [Annexes B, E](#) and [G. Annex F](#) provides examples of security-by-design provisions, with these provisions mapped to relevant standards and guidance documents with compatible provisions.

7 Requirements and guidance for the components of the cybersecurity labelling framework for consumer IoT

7.1 General

Policies for labelling components and labelling issuance and maintenance (as shown in [Figure 1](#)) encompass a set of definitions, roles and responsibilities and implementation rules. The requirements for labelling components and labelling issuance and maintenance are found in [7.2](#) and [8.2](#), respectively. In addition, the guidance for labelling components and labelling issuance and maintenance is found in [7.3](#) to [7.8](#) and [8.3](#) to [8.10](#), respectively.

Components of labelling

Labelling issuance and maintenance

7.3 core components a)	objects of labelling	pre-application	8.3 acceptance criteria and validation of application
7.3 core components b)	cybersecurity requirements	application	8.4 label validity
7.3 core components c)	conformity assessment requirements	conclusion and issuance	8.5 surveillance and monitoring
7.4 key stakeholders' roles and responsibilities	key stakeholders	monitoring and maintenance	8.6 label maintenance and life cycle
7.5 binary or multi-level schemes	type of scheme	renewal	8.7 renewal of labels
7.6 mutual- and cross-recognition	equivalency determination	invalidity	8.8 revocation of labels
7.7 conformity assessment	conformity assessment types and policy	change of standard	8.9 change of underlying standard
7.8 other considerations	implementation considerations	label design	8.10 label design

Figure 1 — Cybersecurity labelling framework in terms of components and labelling issuance and maintenance aspects

7.2 Requirements for the cybersecurity labelling framework components

The requirements for the cybersecurity labelling framework components are specified in a) to g). The relevant stakeholders shall provide the necessary evidence or documentation that the requirements have been met.

- The scheme owner shall develop the policies for each component covered in [7.3](#) to [7.8](#) (see [Figure 1](#)).
- The scheme owner shall define three core components for the consumer IoT labelling scheme based on the considerations of objects of labelling, cybersecurity requirements and conformity assessment requirements (see [7.3](#)).

- c) The scheme owner shall identify the various roles and clearly define the associated responsibilities based on the objectives of the consumer IoT cybersecurity labelling scheme and the nature of the consumer IoT market in which the scheme will be operating (see [7.4](#)).
- d) The scheme owner shall define the type of labelling scheme to be implemented, taking into consideration the characteristics of binary and multi-level labelling schemes (see [7.5](#)).
- e) The governing/policy body or scheme owner shall define a policy on if and how to handle mutual- and cross-recognition with other consumer IoT labelling schemes (see [7.6](#)).
- f) The scheme owner shall develop a conformity assessment methodology that defines a clear set of conformity requirements appropriate for the security targets of the labelling scheme (see [7.7](#)).
- g) The governing/policy body or scheme owner shall determine if regulations of mutual- or cross-recognized schemes apply to its market and scheme (see [7.8](#)).

7.3 Guidance on the core components of cybersecurity labelling framework

The three core components should be defined by the scheme owner in consideration of the following.

- a) **Objects of labelling:** A consumer IoT cybersecurity labelling scheme's scope statement identifies the types of consumer IoT products eligible for labels under the scheme. The intention of the scope statement is to provide clarity to developers and consumers whether a particular IoT product is covered by the cybersecurity labelling scheme. Depending on the objectives of the labelling scheme, products in-scope can be further broken down into categories, such as home security systems, health trackers, etc.

Upon successful completion of the label application process, an object of labelling is eligible to display the label. Objects of labelling can include:

- i) Physical products as they can be bought by a consumer, e.g. a router, smart bulb or toy. In this case the product is a specific device.
 - ii) Associated services or software delivered through a consumer product (such as a mobile or cloud service).
 - iii) Solutions providing a seamlessly integrated small bundle of technologies combining both hardware components and associated services, e.g. an application for remote control or cloud space or any backend services. In this case, all elements of the solution fulfil the same security requirement at the same level. A solution can be bought off-the-shelf by a consumer. The label applies to the set of elements as predefined by the developer.
- b) **Cybersecurity requirements:** Consumer IoT cybersecurity labelling schemes reference suitable technical and non-technical cybersecurity requirements for in-scope objects of labelling. Depending on the design of the labelling scheme, different product categories can be subject to different cybersecurity requirements. The scheme owner can define dedicated cybersecurity requirements for different product categories, where necessary.

The selection of cybersecurity requirements can be subject to various parameters such as legislation, industry requirements, market expectations, and limits of implementation and resources. Widely referenced standards such as those published by ISO can facilitate the alignment of cybersecurity requirements of labelling schemes across jurisdictions for mutual- or cross-recognition.

- c) **Conformity assessment requirements:** A consumer IoT cybersecurity labelling scheme's conformity assessment requirements define the process(es) that developers must follow in order to demonstrate conformance to the terms and cybersecurity requirements of the scheme.

Acceptable conformity assessment methods are chosen based on the labelling scheme's stated objectives and outcomes, considering factors such as level of rigour, burden on the developer, and overall cost-effectiveness in delivering cybersecurity outcomes. Depending on the design and structure of the labelling scheme (i.e. single or multi-level, different product categories), different conformity

assessment types can be acceptable. See [7.7](#) for guidance on determining the conformity assessment types and policy for the labelling scheme.

7.4 Guidance on key stakeholders' roles and responsibilities

An effective consumer IoT cybersecurity labelling scheme depends on a series of clearly defined interactions between the various stakeholders associated with the scheme.

A consumer IoT cybersecurity labelling scheme can recognize any or all of the following roles:

- governing/policy body, which identifies the need and goals for cybersecurity labels for consumer IoT products in relation to national or regional infrastructure to ensure quality and facilitate the cross-recognition of international cybersecurity labels for consumer IoT products. The governing/policy body can implement legislation that codifies the scope, roles, and responsibilities associated with the scheme. In addition, a governing/policy body can define categories or classes of consumer IoT products for which IoT labelling is mandatory. The governing/policy body can be the scheme owner or authorize the scheme owner to develop IoT labelling policy.
- scheme owner, who is tasked with implementing the labelling regulations and requirements issued by the governing/policy body, certification bodies or trade associations. The scheme owner is also responsible for developing and maintaining a specific labelling scheme. Depending on local requirements, after a successful application, the scheme owner issues the cybersecurity label or can delegate to a scheme operator or another suitable party to issue the label. In addition, the scheme owner is responsible for the further development of the scheme.
- scheme operator, who executes the application and issuance procedures, reviews, and validates work performed by conformity assessment bodies to ensure consistency and quality of the testing. The scheme operator performs system updates and random checks to ensure its list of labelled products is correct, the products' cybersecurity have not changed and cybersecurity labels are correctly used. In areas where there is non-compliance, the scheme operator can revoke labels for such consumer IoT products.

NOTE 1 Scheme owner and scheme operator roles can be performed by the same entity. [Clause 8](#) specifies more details on the responsibilities of the scheme owner and scheme operator in the process of obtaining the cybersecurity label.

- developer, usually the applicant or label holder, provides the implementation of the controls to meet the cybersecurity requirements of the labelling scheme. The developer can interact with the conformity assessment bodies, scheme operators or scheme owners to implement changes resulting from policy changes or errors in the original implementation of the controls and addresses detected vulnerabilities. The developer can work with retailers to reinforce end user/consumer understanding of the cybersecurity labels being awarded for its consumer IoT products and the appreciation of cybersecurity labels.

NOTE 2 With authorization from the developer, a product distributor or importer can play the role of the applicant on its behalf.

- conformity assessment body, who is responsible for carrying out conformity assessment activities according to applicable regulations and policies. The role of a conformity assessment body can vary, depending on the design of a labelling scheme and be incorporated by different parties such as governing/policy bodies. The conformity assessment body can play the role of an independent test laboratory (ITL), acting as a security testing body that conducts third-party security evaluations for products under the supervision of the scheme operator. The conformity assessment body can be accredited by an accreditation body, which derives its authority from government, public authorities, contracts, market acceptance or scheme owners. In some instances, the accreditation body role can be performed by the scheme owner.
- end users/consumers, who purchase or use a labelled consumer IoT product. When designing a consumer IoT cybersecurity labelling scheme, assumptions made about the nature of IoT product consumers are documented, together with any scheme objectives targeted toward these consumers. An example of a labelling scheme objective can be "to enable the IoT product consumer to make informed purchasing decisions."

7.5 Guidance on binary and multi-level labelling schemes

7.5.1 General

A consumer IoT cybersecurity labelling scheme can employ either a binary or multi-level labelling structure.

The characteristics of binary level schemes are as follows.

- The label is only available if all cybersecurity requirements have been fulfilled.
- There are no progressive levels, with all labelled products of the scheme or in the same product category demonstrating the same level of cybersecurity. To provide for flexibility and support local cybersecurity requirements, the binary label scheme can be implemented differently in unique product categories.
- One set of conformity assessment requirements applies to all products in the scheme or a specific product category.

The characteristics of multi-level schemes are as follows.

- Different levels are available for products, so that similar products can receive labels on different levels as they fulfil different cybersecurity or conformity assessment requirements.
- Each higher level builds upon the previous one and contains either additional cybersecurity requirements or different conformity assessment methods, or both.

Both binary and multi-level labelling schemes can have various product categories where all products of a specific product category fulfil the same cybersecurity requirements [see [7.3 b\)](#)]. Cybersecurity requirements can differ among product categories but are not required to be compatible at the same level. Examples of multi-level labelling schemes are shown in [Annex B](#) while examples of binary labelling schemes, with and without product categories, are shown in [Annex C](#).

7.5.2 Binary versus multi-level labelling schemes

In deciding the type of labelling scheme to develop and implement, scheme owners or scheme operators can take the following into consideration.

- Scheme objectives: These capture the strategic purpose of a consumer IoT cybersecurity labelling scheme and are often stated in terms of desired benefits.
- Scope of the covered consumer IoT products: The scheme owner is expected to determine the scope of the scheme, whether it is a broad-based scheme that covers all kinds of consumer IoT products or a targeted scheme that focuses on a specific type of consumer IoT product. This decision can also be influenced by the administrative or regulatory requirements of each jurisdiction or region.
- Product complexity and risk profile: Consumer IoT products vary in complexity, with some being relatively simple (e.g. smart plugs) and others with more interfaces and interdependencies with associated services (e.g. smart home security systems). For a consumer IoT product line with a specific and limited scope of use, a single-level label can suffice to provide information on the cybersecurity hygiene of the product. For a more complex consumer IoT product line with varying degree of features offered by developers, a multi-level approach can be needed to explain the granularity of security hygiene across the spectrum of such consumer IoT products.
- Consumer understanding and culture: Consumer IoT labels should be clear, simple and easily understandable by non-technical users. A binary labelling scheme should convey essential information about the cybersecurity hygiene of the consumer IoT without overwhelming users. Multi-level labelling schemes can require more educational resources such as user guides, FAQs and online resources to help consumers understand the differences among the cybersecurity levels and enable them to make informed decisions. Another related consideration is the consumer culture, which relates to their choice of the type of labelling schemes. In a consumer culture that values simplicity and convenience, a binary scheme can be preferred as it provides a straightforward form of security information to consumers. In