

AS/NZS ISO/IEC 27400:2024
ISO/IEC 27400:2022



Australian/New Zealand Standard™

Cybersecurity — IoT security and privacy — Guidelines



AS/NZS ISO/IEC 27400:2024

This Joint Australian/New Zealand Standard™ was prepared by Joint Technical Committee IT-012, Information security, cybersecurity and privacy protection. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 03 August 2024 and by the New Zealand Standards Approval Board on 05 June 2024.

This Standard was published on 23 August 2024.

The following are represented on Committee IT-012:

- Australasian Society for Computers and Law
- Australian Industry Group
- Australian Information Industry Association
- Australian Information Security Association
- Australian Security Industry Association
- Business Continuity Institute Australasia
- Consumers Federation of Australia
- CSIRO Data 61
- Cyber Security Cooperative Research Centre
- Department of Defence (Australian Government)
- Department of Internal Affairs, NZ
- Energy Networks Australia
- Engineers Australia
- ISACA Melbourne
- Joint Accreditation System of Australia & New Zealand
- Monash University
- NZ Ministry of Business, Innovation and Employment (MBIE)
- Office of the Victorian Information Commissioner
- University of Waikato
- University of Wollongong

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 27400:2024.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

ISBN 978 1 76139 771 4

Australian/New Zealand Standard™

Cybersecurity — IoT security and privacy — Guidelines

First published as AS/NZS ISO/IEC 27400:2024.

COPYRIGHT

© ISO/IEC 2024 — All rights reserved

© Standards Australia Limited/the Crown in right of New Zealand, administered by the New Zealand Standards Executive 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information security, cybersecurity and privacy protection.

The objective of this document is to provide guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

This document is identical with, and has been reproduced from, ISO/IEC 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*.

As this document has been reproduced from an International document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
National Foreword	iv
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 IoT concepts	2
5.1 General	2
5.2 Characteristics of IoT systems	3
5.3 Stakeholders of IoT systems	4
5.3.1 General	4
5.3.2 IoT service provider	4
5.3.3 IoT service developer	4
5.3.4 IoT user	5
5.4 IoT ecosystem	5
5.5 IoT service life cycles	5
5.6 Domain based reference model	7
6 Risk sources for IoT systems	8
6.1 General	8
6.2 Risk sources	9
6.2.1 General	9
6.2.2 Sample risk sources related to IoT domains	10
6.2.3 Risk sources from outside the IoT domains	12
6.2.4 Privacy related risk sources	12
7 Security and privacy controls	13
7.1 Security controls	13
7.1.1 General	13
7.1.2 Security controls for IoT service developer and IoT service provider	13
7.1.3 Security controls for IoT user	31
7.2 Privacy controls	32
7.2.1 General	32
7.2.2 Privacy controls for IoT service developer and IoT service provider	32
7.2.3 Privacy controls for IoT user	38
Annex A (informative) IoT monitoring camera sample risk scenario	40
Bibliography	42

National Foreword

Australia

Internet of Things (IoT) systems are widely deployed in Australia. They are increasingly deployed within critical infrastructure such as transport, energy and water networks. They introduce new challenges for information security across a wide range of technologies and entities.

This document is of high relevance and interest to services of critical infrastructure in light of new security legislation in Australia. It provides guidelines on the responsibilities of all entities.

This document provides useful security and privacy guidelines for three important IoT stakeholder groups: users, developers and service providers.

A comprehensive list of identified risk sources is documented. A practical example is used to illustrate these risk sources.

This document includes a list of suggested controls. These controls provide practical considerations for responding to these multiple risk sources.

This document only contains guidelines, with no requirements. For practical Standards-based implementation and use, it should be read with associated and identified companion Standards.

Where “personally identifiable information” is used in this document, interchange with “personal information” to suit the Australian context.

New Zealand

Internet of Things (IoT) systems are widely deployed in New Zealand. There is a clear understanding of IoT benefits including the value of data that can be collected from IoT devices, including in the primary industry sectors. There is increasing deployment of IoT systems in supply chain, logistics and retail infrastructure and to support research and environmental monitoring.

IoT systems introduce new challenges for information security across a wide range of technologies and entities.

This document provides useful security and privacy guidelines for three important IoT stakeholder groups: users, developers and service providers.

A comprehensive list of identified risk sources is documented. A practical example is used to illustrate these risk sources.

It includes a list of suggested controls. These controls provide practical considerations for responding to these multiple risk sources.

This document only contains guidelines, with no requirements. For practical Standards-based implementation and use, it should be read with associated and identified companion Standards.

Where “personally identifiable information” is used in this document, exchange with “personal information” to suit the New Zealand context.

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

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.

Introduction

Information security is a major concern of any information and communication technology (ICT) system and Internet of Things (IoT) systems are no exception. IoT systems present particular challenges for information security in that they are highly distributed and involve a large number of diverse entities. This implies that there are a very large attack surface and a significant challenge for the information security management system (ISMS) to apply and maintain appropriate security controls across the whole system.

Privacy or personally identifiable information (PII) protection is a significant concern for some types of IoT systems. Where an IoT system acquires or uses PII, it is usually the case that there are laws and regulations that apply to the acquisition, storage and processing of PII. Even where regulations are not a concern, the handling of PII by an IoT system remains a reputational and trust concern for the organizations involved, for example, if the PII is stolen or is misused, potentially causing some form of harm to the people identified by the information.

Security and privacy controls in this document are developed for stakeholders in an IoT system environment, so as to be utilized by each IoT stakeholder, throughout the IoT system life cycle.

Australian/New Zealand Standard

Cybersecurity — IoT security and privacy — Guidelines

1 Scope

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20924, ISO/IEC 27000, ISO/IEC 29100, ISO 31000 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

cloud computing

paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.5]

3.2

cloud service

one or more capabilities offered via *cloud computing* (3.1) invoked using a defined interface

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.8]

3.3

IoT device

entity of an IoT system that interacts and communicates with the physical world through sensing or actuating

3.4

IoT device developer

entity that creates an assembled final IoT device

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

3.5

IoT platform

infrastructure that enables the deployment, management and operation of IoT devices

3.6

IoT system

system providing functionalities of Internet of Things

Note 1 to entry: IoT system is inclusive of IoT devices, IoT gateways, sensors, and actuators.



Documents

Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2024

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

3.7

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 none IoT solutions

3.8

ecosystem

infrastructure and services based on a network of organizations and stakeholders

Note 1 to entry: Organizations can include public bodies.

[SOURCE: ISO/IEC TS 27570:2021, 3.8]

4 Abbreviated terms

ASD	Application and Service Domain
CRM	Customer Relationship Management
DoS	Denial of Service
IC	Integrated Circuit
ICT	Information and Communications Technology
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ITS	Intelligent Traffic System
OMD	Operations and Management Domain
OTA	Over The Air
PED	Physical Entity Domain
PII	Personally Identifiable Information
RAID	Resource Access and Interchange Domain
SCD	Sensing and Controlling Domain
UD	User Domain
Wi-Fi	Wireless Fidelity

5 IoT concepts

5.1 General

This clause provides a brief introduction to IoT concepts and reference models which are useful in the context of security and privacy. Detailed information on these topics is provided in ISO/IEC 30141.

5.2 Characteristics of IoT systems

The applications of IoT systems are diverse, making it impractical to define a generally applicable set of characteristics for every IoT system. As a practical way to describing characteristics of IoT systems, “common characteristics” and “specific characteristics for application areas” can be identified.

IoT systems share following common characteristics.

- IoT systems include IoT devices, which is specific hardware and software equipment which is used in conjunction with or attached to physical things or materials.
- IoT devices are connected to networks and have the ability to transmit and receive data. Wired as well as wireless networks can be used.
- IoT devices usually have sensing capabilities, e.g. for detecting environment states or movements.
- IoT devices can have actuating capabilities, e.g. receiving controlling data in order to initiate physical actions.
- IoT systems include IoT applications in order to process data from IoT devices, to generate and send controlling data, and to enable integration with other systems.
- IoT systems include operational components which allows the setup and operation of IoT devices and applications.
- IoT systems support human or digital users (for further information refer to ISO/IEC 30141).

Depending in which area or for which purpose IoT systems are used there are specific requirements. See the following list of examples.

- For consumer IoT systems pricing is very sensitive, which makes low cost for manufacturing and operating IoT devices important. Depending on the data processed, data privacy can also be very important.
- Industrial IoT systems can replace or be used in conjunction with an industrial plant and control systems and therefore, be subject to similar requirements such as high availability or safety. Safety of process utilizing IoT systems may depend on the security characteristics of an IoT device.
- IoT systems used in vehicles are used in the context of reliability or safety relevant functionalities. Whereas in the reliability related use case privacy requirements can be important to consider, a safety use case can impose high integrity and availability requirements.

For further information and discussion of specific use cases for IoT systems, refer to ISO/IEC TR 22417:2017.

IoT service providers often use cloud infrastructure to implement their services. Especially when using public cloud services, this allows low initial cost and great scalability.

An IoT service provider should ensure as a consumer of a cloud service that the cloud service has adequate security controls in place. These controls, often also in combination with additional controls at the IoT service provider’s side, should fully address the security and privacy requirements of the IoT users (e.g. regarding protection of PII), for which the IoT service provider is in a supplier role.

For further guidance on supplier relationships in cloud services refer to ISO/IEC 27036-4, for guidance on security controls for cloud services based on ISO/IEC 27002 refer to ISO/IEC 27017, and further guidance on PII protection in public cloud is provided in ISO/IEC 27018.

5.3 Stakeholders of IoT systems

5.3.1 General

In order to be able to implement security and privacy for an IoT system, it is important to know the stakeholders of the system. Depending on their role, they are either setting the level of security and privacy required for the system based on their risk appetite, or they contribute to effective controls for achieving these requirements.

ISO/IEC 30141 defines three types of roles: IoT service provider, IoT service developer and IoT users. It also defines a number of subroles and activities, some of them relate to security and privacy.

In [5.3](#), the common stakeholders relevant for most IoT systems are introduced.

5.3.2 IoT service provider

An IoT service provider manages and operates the services of an IoT system which are offered to the IoT users.

Common services provided by IoT service providers include connectivity services, data collection and management services as well as management service for IoT-related assets such as IoT devices.

The IoT service needs to match the IoT user's needs and is dependent on a specific use case or a relevant IoT ecosystem.

IoT service providers need to understand the functional and non-functional requirements of IoT users for services provided, and to satisfy IoT users with the services, particularly in terms of security and privacy.

In order to achieve this, IoT service providers also need to fully understand any relevant threat vectors in order to be able to perform a risk assessment and to select effective risk treatment options.

For specific controls which have to be considered by an IoT service provider, refer to the controls given in [Clause 7](#) which have "IoT service provider" as the indicated audience.

5.3.3 IoT service developer

IoT service developers are responsible for the design, implementation and integration of IoT services.

IoT service developers can be further specialized, e.g. by taking on the role as architect for IoT solutions or platforms, as designer and or implementer for IoT applications, as designer or implementer for IoT devices.

In each role, IoT service developers should follow best practices for design and development, e.g. adhering to security and privacy by design principles or using secure software development life cycles.

One of the subroles of IoT service developers is IoT device developer. It does engineer and produce specific hardware equipment to be used in IoT systems, in particular IoT devices.

IoT devices can either be operated and used directly by an IoT user or by an IoT service provider, and the technically same device can be used in various different IoT use cases. It is important for an IoT device developer to consider the security and privacy requirements of potential usage scenarios for the device in the design phase, in order to be able to offer devices which have the right set of functionality and features to fulfil their customers' need.

IoT service developers need to understand and consider the security and privacy expectations and requirements of the IoT service providers as well as of IoT users, so that necessary controls are selected to ensure adequate treatment of risks of the IoT system.

For more information regarding controls which have to be considered by IoT service developers, refer to the controls given in [Clause 7](#) which have "IoT service developer" as an indicated audience.

5.3.4 IoT user

An IoT user is the end user of an IoT service and can be categorized into human user and digital user. Human user is an individual who uses the IoT service. Digital user is a non-human user of the IoT service; it can be an automated service acting on behalf of a human user.

In the case of human user, he/she can be either represented by an individual, for example, in the case of consumer level IoT systems, or by an organization, e.g. in the case of industrial IoT systems.

In any case, the IoT user does directly set or at least does influence the functional and non-functional requirements for an IoT system or an IoT service.

It is in the core interest of the IoT user that an IoT system or IoT service can be used without introducing unacceptable risks in the area of security and privacy.

The level of security and privacy required to be provided in a IoT system or service is mainly driven by expectations or risk considerations done by IoT users. However, IoT users may often be unaware of the security implications of the technologies.

For any use case a profound understanding of the IoT users and of their needs and requirements is crucial.

In order to be able to treat IoT related risks adequately, there are also controls an IoT user should consider and implement. For more information regarding these controls, refer to the controls given in [Clause 7](#) which has “IoT User” as an indicated audience.

5.4 IoT ecosystem

Dependencies among IoT service providers, IoT service developers and IoT users in the context of security and privacy in an IoT system can be described as an ecosystem, an analogy to the concept in ecology. The dependencies in security and privacy in IoT include:

- a) products and services supplier relationships;
- b) provision of measures by other entities within the ecosystem necessary in implementing security and privacy controls (see [Clause 7](#)); and
- c) potential externality of consequences in conceivable risk scenarios not contained within an entity (see [Clause 6](#)), e.g. failure in implementing a control by an IoT service provider or an IoT service developer giving rise to security and privacy risk of IoT users.

Furthermore, there are concerns about adverse effects on other organizations beyond the impact between stakeholders assumed in a single IoT system, such as cyber attacks against external organizations and countries that exploit vulnerable IoT systems and devices. These adverse effects need to be addressed in an expanded ecosystem that includes the entities potentially affected, and responsible organizations should implement controls ([Clause 7](#)) addressing them.

5.5 IoT service life cycles

An IoT service introduces various life cycles, which can be mapped to the stakeholders of an IoT system.

More specifically, an IoT service is:

- a) developed by an IoT service developer and IoT device developer(s);
- b) provided by an IoT service provider; and
- c) used by IoT users.

Processes of these stakeholders form a set of interdependent life cycles of device development, service development, service provision and use of the service. [Figure 1](#) shows these life cycles of IoT service and the relationships among them.

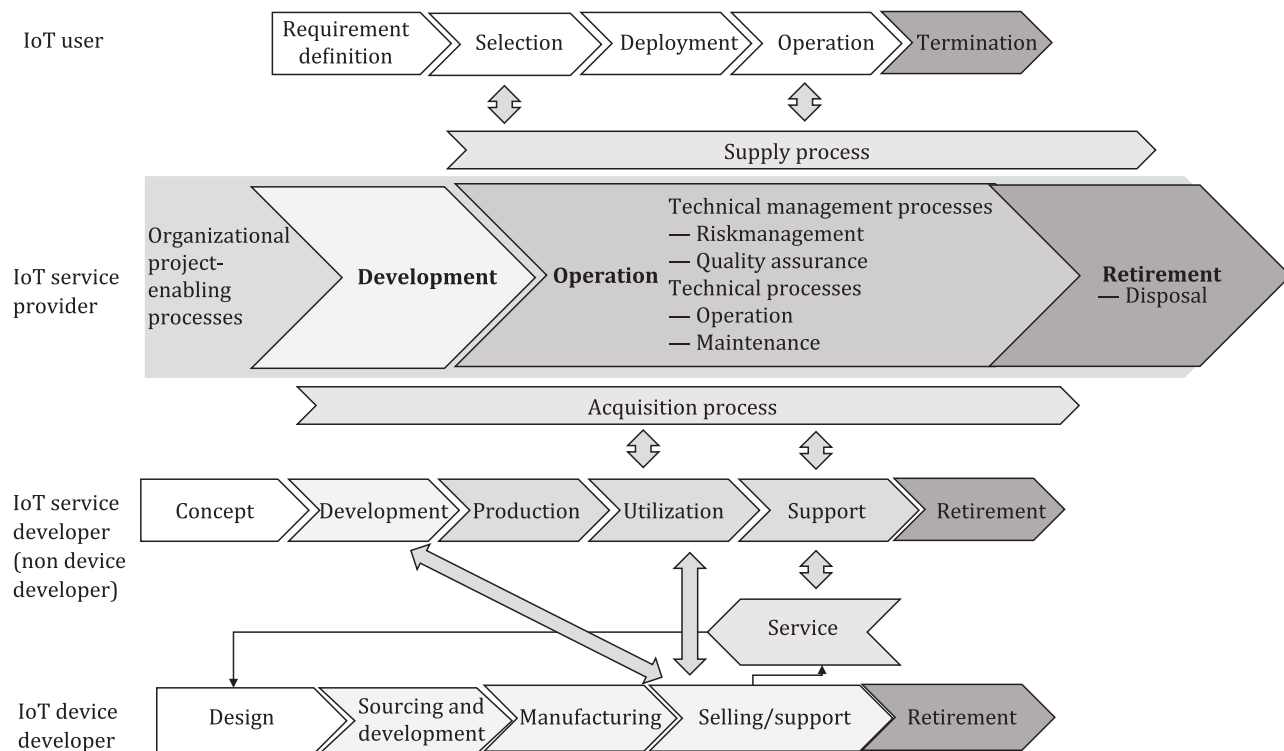


Figure 1 — IoT service life cycles

In the life cycle of the IoT device, the IoT device developer designs, develops, manufactures, sells to and supports the IoT service developers, the IoT service providers or the IoT users. At retirement of the device, the IoT device developer terminates supporting the IoT device. Security and privacy requirements are considered in design and development of the IoT device, and implemented as features of the IoT device, e.g.

- d) user authentication and access control mechanisms of the device;
- e) physical security feature such as secure case; and
- f) device software and firmware updating mechanism and operation.

During supplier relationships, information of these features is provided to and used by the IoT service developers and the IoT service providers at relevant stages of their life cycles. An IoT device developer should ensure that adequate and updated device information including security related information is available to all relevant stakeholders.

The IoT service developer designs, develops, produces, and supports the IoT system that enables the IoT service. At retirement, the IoT service developer terminates supporting the IoT system. Based on requirements for an IoT service driven by the needs of the assumed users of the service, security and privacy requirements are considered in design and development of the IoT system, and implemented as features of the IoT system, e.g.

- g) user authentication and access control mechanisms of the service;
- h) protection against malware;
- i) redundancy of components and network;
- j) software updating mechanism and operation; and

- k) functions and procedures for system operations.

Information of these features is provided to and used by the IoT service providers at relevant stages of its life cycle and they need to be aligned with the security features of the used IoT devices.

The IoT service provider develops the operation and operates the IoT service acquired from the IoT service developer. At retirement, the IoT service provider terminates provision of the service. The activities of these phases of the life cycle, i.e. development, operation and retirement, are implementation of system life cycle processes given in ISO/IEC 15288 including but not limited to:

- l) acquisition process;
- m) supply process;
- n) organizational project enabling processes;
- o) technical management processes;
 - 1) risk management process;
 - 2) quality assurance process;
- p) technical processes;
 - 3) operation process;
 - 4) maintenance process; and
 - 5) disposal process.

Among these processes, the risk management process and the quality assurance process are key to security and privacy in the IoT service. In the risk management process, security and privacy risks are assessed and treated by applying the features of the IoT devices and the IoT system and implementing secure operations. Through the quality assurance process, the IoT system and software are ensured to be excluding vulnerabilities and malicious components, and to have necessary safety functions that ensure availability of the IoT system along with other safety aspects.

Through the supply process, information related to security and privacy in the use of the IoT service and software updates are provided to the IoT user.

The IoT user chooses an IoT service that meets its service and functional requirements along with security and privacy requirements. Information related to security and privacy is provided by the IoT service provider and the IoT device developer, and are examined by the IoT user at this stage. After purchasing the IoT service, the IoT user applies software and firmware updates and uses other information provided by the IoT service provider and the IoT device developer to keep the level of security and privacy during the operation till the decommissioning of the IoT device.

It should be noted that security and privacy issues can occur due to lack of consistency among life cycles of the stakeholders. As an example, the IoT service providers should be aware of the possibility that support period of a specific IoT device terminates during the operation of the IoT service, or the IoT device developer or other IoT service developer cease to exist in the market, while the IoT users continue to use the IoT device whether aware or not of the termination.

5.6 Domain based reference model

IoT reference models presented in ISO/IEC 30141 provide views of the IoT systems. One of the reference models is the domain based reference model which is a framework of functions constituting the IoT system and its operations. [Figure 2](#) is derived from ISO/IEC 30141:2018, Figure 13. The IoT user, the IoT service provider and the IoT service developer are added in this figure to show relevance of these stakeholders to the IoT domains.

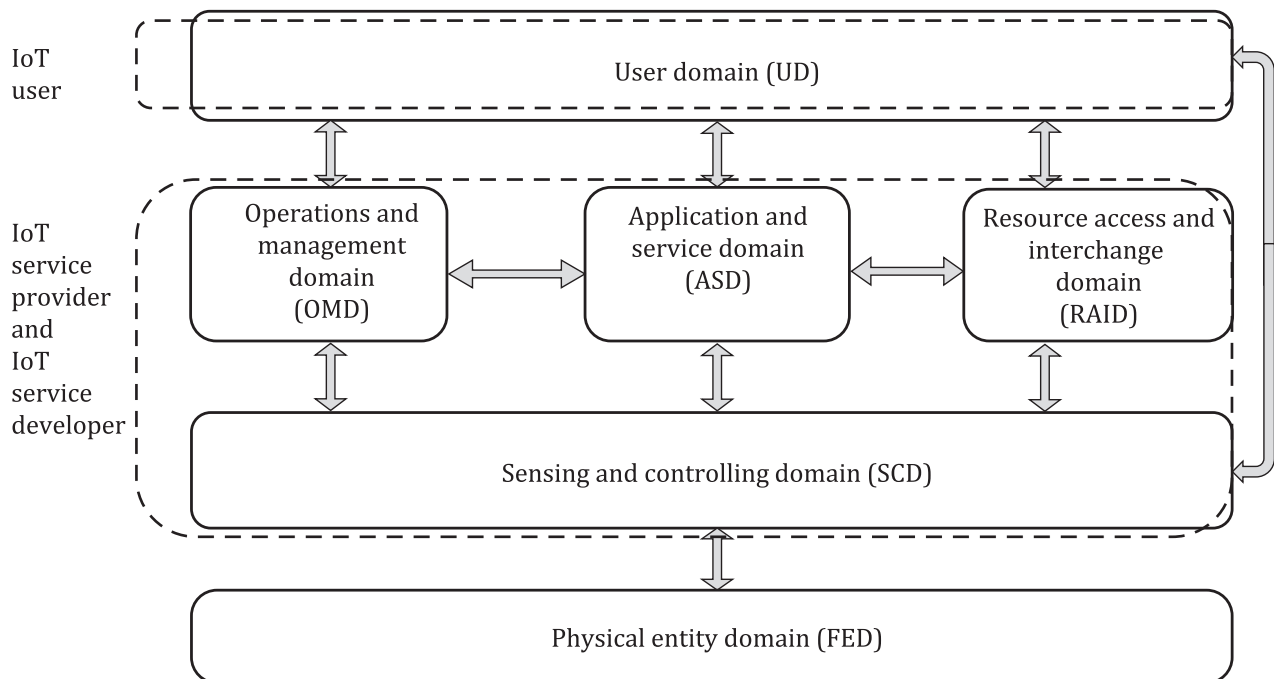


Figure 2 — Domain based reference model

Figure 2 shows the following IoT domains:

- the User Domain (UD) includes human and digital users;
- the Physical Entity Domain (PED) includes the physical entities in an IoT system;
- the Sensing and Controlling Domain (SCD) includes IoT devices and IoT gateways;
- the Operations and Management Domain (OMD) includes the operation support system and the business support system;
- the Resource Access and Interchange Domain (RAID) provides mechanisms by which external entities can access the capabilities of the IoT systems; and
- Application and Service Domain (ASD) includes the applications and services offered by the IoT service providers.

The domain-based reference model provides the overall structure of the elements of an IoT system for considering IoT security and privacy. The risk sources can be identified in relation to the IoT domains (see 6.2). Each of the security and privacy controls can be related to one or more IoT domains (see Clause 7).

6 Risk sources for IoT systems

6.1 General

This clause provides guidance and information on IoT specific factors and inputs which need to be considered when identifying risk sources for IoT systems.

Based on identified risk sources, risk management for IoT systems should be done by using the approaches and methods which have been standardised.