
**Information technology — Security
techniques — Application security —
Part 5:
Protocols and application security
controls data structure**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
*Technologies de l'information — Techniques de sécurité — Sécurité
des applications —
Partie 5: Protocoles et structure de données de contrôles de sécurité
d'application*

[ISO/IEC 27034-5:2017](https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68f073db268f/iso-iec-27034-5-2017)

[https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-
8522-68f073db268f/iso-iec-27034-5-2017](https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68f073db268f/iso-iec-27034-5-2017)



iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27034-5:2017](https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68f073db268f/iso-iec-27034-5-2017)

<https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68f073db268f/iso-iec-27034-5-2017>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Application Security Control Structure	2
5.1 General	2
5.2 ASC information requirements	2
5.2.1 Overview	2
5.2.2 Integrity assurance	4
5.2.3 Multilingual/multiregional data representation	4
5.2.4 ASC information requirements	5
5.3 ASC data structure recommendations	14
5.3.1 General	14
5.3.2 Exchange	14
5.3.3 Self-containedness	14
6 Application Security Life Cycle Reference Model	14
6.1 General	14
6.2 Application Management Layer	16
6.2.1 General	16
6.2.2 Initiating	16
6.2.3 Planning	16
6.2.4 Executing	17
6.2.5 Monitoring and controlling	17
6.2.6 Closing	18
6.3 Application provisioning and operation layer	18
6.3.1 General	18
6.3.2 Preparation: Initiating	18
6.3.3 Preparation: Plan	19
6.3.4 Outsourcing: Realization	19
6.3.5 Outsourcing: Transition	19
6.3.6 Development: Inception	20
6.3.7 Development: Elaboration	20
6.3.8 Development: Construction	20
6.3.9 Acquisition: Plan	21
6.3.10 Acquisition: Close	21
6.3.11 Transition: Plan	21
6.3.12 Transition: Development	21
6.3.13 Transition: Test	22
6.3.14 Utilization: Utilization	22
6.3.15 Utilization: Maintenance	23
6.3.16 Archival: Archival	23
6.3.17 Destruction: Destruction	24
6.4 Infrastructure management	25
6.4.1 General	25
6.4.2 Establishment of the infrastructure	25
6.4.3 Maintenance of the infrastructure	25
6.5 Application audit	26
6.5.1 General	26
6.5.2 Initiating the audit	26
6.5.3 Prepare the audit	27

6.5.4	Conduct the audit.....	27
6.5.5	Report.....	28
6.5.6	Complete the audit.....	28
6.5.7	Follow-up.....	28
6.6	Roles.....	29
7	ASC Package.....	31
	Bibliography	33

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27034-5:2017](https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68f073db268f/iso-iec-27034-5-2017)

<https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68f073db268f/iso-iec-27034-5-2017>

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 27034 series can be found on the ISO website.

Introduction

General

There is an increasing need for organizations to focus on protecting their information at the application level. A systematic approach towards increasing the level of application security provides an organization with evidence that information being used or stored by its applications is being adequately protected.

ISO/IEC 27034 (all parts) provides concepts, principles, frameworks, components and processes to assist organizations in integrating security seamlessly throughout the life cycle of their applications.

The Application Security Control (ASC) is one of the key components of this document.

To facilitate the implementation of ISO/IEC 27034 (all parts) application security framework and the communication and exchange of ASCs, a minimal set of essential attributes should be documented and explained for realizing ASCs and certain other components of the framework.

This document explains the minimal set of essential attributes of ASCs and further details the Application Security Life Cycle Reference Model (ASLCRM).

Purpose

The purpose of this document is to document and explain the essential information and data structure requirements for ASCs. The advantages of a standardized set of essential information attributes and data structure of ASCs include the following:

- a) normalized ASC creation, communication, protection and verification in compliance with the requirements of this document; and
- b) minimized cost of security in application projects by facilitating the reuse of approved controls and acquisition of ASCs from different sources.

In addition, this document defines and details the processes, activities and roles involved in the Application Security Life Cycle Reference Model.

Targeted audiences

General

The following audiences will find values and benefits when carrying their designated organizational roles:

- a) managers;
- b) ONF committee;
- c) domain experts;
- d) suppliers; and
- e) acquirers.

Managers

Managers should read this document because they are responsible for:

- a) ensuring the ASCs are reusable within the organization, and
- b) ensuring the ASCs are available, communicated and used in application projects with proper tools and procedures all across the organization.

Organization Normative Framework (ONF) Committee

The ONF Committee is responsible for managing the implementation and maintenance of the application-security-related components and processes in the Organization Normative Framework. The ONF Committee:

- a) implements the ASC Library,
- b) approves ASCs that correctly mitigate application security risks, and
- c) manages the cost of implementing and maintaining the ASCs.

Domain experts

Domain experts contribute knowledge in application provisioning, operating or auditing, who:

- a) participate in ASC development, validation and verification,
- b) participate in ASC implementation and maintenance, by proposing strategies, components and implementation processes for adapting ASCs to the organization's context, and
- c) validate that ASCs are useable and useful in application projects.

Security tools and ASC supplier

Suppliers contribute to develop, maintain and distribute tools and/or ASCs. They

- a) create, validate, enforce integrity (through a recognized method, such as signing), distribute and apply ASCs, and
- b) align with a common and standardized exchange protocol (structure and format) for ASCs.

Security tools and ASC acquirer

Acquires are individuals or organizations who want to acquire ASCs. They

- a) integrate ASCs into their organization and ensure the interoperability of any internal and third-party ASCs,
- b) adapt ASCs and enforce their integrity, and
- c) ensure that the activities and tasks of acquired ASCs can be mapped to the organization's application lifecycle.

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO/IEC 27034-5:2017

<https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68f073db268f/iso-iec-27034-5-2017>

Information technology — Security techniques — Application security —

Part 5:

Protocols and application security controls data structure

1 Scope

This document outlines and explains the minimal set of essential attributes of ASCs and details the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM).

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 27034-1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1 and the following apply.

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

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

3.1 activity

set of actions or tasks carried out by an actor during the application's life cycle

3.2 information group record

list of information elements to which an organization can assign labels, such as names, description and categorization values

Note 1 to entry: To avoid confusion, information group name should be unique within the organization.

3.3 information element

piece of information that should be categorized and identified by a name, description, and domain values (e.g. a field in a database)

Note 1 to entry: An information group can be seen as an information element.

4 Abbreviated terms

ASC	Application Security Control
ASLC	Application Security Life Cycle
ASLCRM	Application Security Life Cycle Reference Model
ICT	Information and Communication Technology
ONF	Organization Normative Framework

5 Application Security Control Structure

5.1 General

Each Application Security Control (ASC) defines a security-related activity performed at a specific point in an application's life cycle to mitigate a risk or to satisfy a requirement. The security activity is supplemented by a verification measurement (activity) that specifies the necessary steps to verify its successful application. For both the security activity and verification measurement, an ASC specifies how, where, when and by whom the activity should be implemented. Information about the required effort is also captured.

The purpose of this clause is to provide a specification of the ASC information requirements and data structure recommendations. Organizations may choose to implement the information requirements and data structure requirements using either a narrative approach or other suitable data structure, which best suits organizational needs and requirements.

NOTE 1 To identify the minimum set of attributes needed to define a valid ASC, the name of each ASC attribute defined in this document includes the mention “(M)” when the attribute is **mandatory**, or the mention “(O)” when the attribute is **optional**.

NOTE 2 The inclusion of an optional attribute could require the implementation of subsequent mandatory attributes. Mandatory attributes under an optional attribute are mandatory only when the optional attribute is implemented [e.g. see 5.2.4.2, e)].

The purpose of this clause is also to provide a list of possible activities enabling the ONF Committee to attach ASCs into the Application Security Life Cycle Reference Model (ASLCRM).

ASC developers should align their vocabulary with ISO/IEC 27034 (all parts) when they need to describe assets.

5.2 ASC information requirements

5.2.1 Overview

This subclause defines the recommended information requirements for individual application security controls. For a concrete implementation in form of an XML Schema of this document, please refer to ISO/IEC 27034-5-1.

Note that this document does not define how the various ASC information items are identified or managed. For details about the latter, consult the management and audit process defined in ISO/IEC 27034-2, ISO/IEC 27034-3 and ISO/IEC 27034-4.

NOTE Explicit indication of an inheritance hierarchy is not implemented in the ASC structure, but could be implemented in future versions.

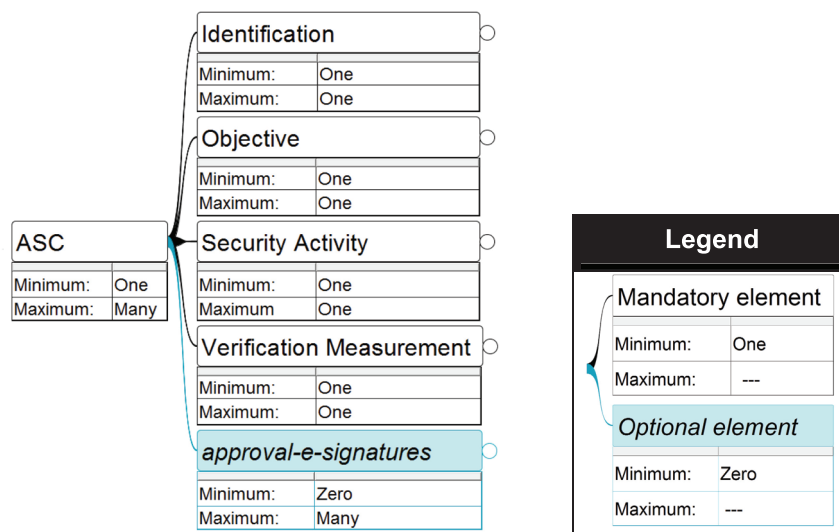


Figure 1 — Main sections of ASC information

As specified in ISO/IEC 27034-1:2011, 8.1.2.6.5, and shown in [Figure 1](#), each ASC should contain the following sections:

- a) **ASC Identification (M)**: This section should contain the following information:
 - 1) identification information about the ASC (id, name, etc.);
 - 2) a high-level description of the scope and intent of the ASC;
 - 3) information about the current version including the creation date, current lifecycle stage, revision notes and identification information about its author and owner; and
 - 4) references to super-ordinate and sub-ordinate ASCs.
- b) **ASC Objective (M)**: This section should contain the following information:
 - 1) a detailed description of the ASC's intent and security objective;
 - 2) one or more security requirements that justify 'why' the ASC is needed as well as information about the context and the application functionality from which the security requirements originated;
 - 3) one or more levels of trust for which the ASC is mandatory along with a description of the level of trust range;
 - 4) preconditions and assumptions for applying the ASC. In particular:
 - i) a list of preconditions;
 - ii) a list of (informal) threat assumptions; and
 - iii) a description of the operating environment (context of use).
- c) **ASC Security Activity (M)**: This section should contain the following information pertinent to the security activity defined by the ASC:
 - 1) a high-level description of the security activity (what);
 - 2) a description of the asset that is protected (targeted) by carrying out the security activity (where);

- 3) a definition of the roles (and required qualifications) involved in the execution of the tasks and actions involved in the security activity (who);
 - 4) an indication of the complexity and costs of the security activity (how much);
 - 5) a detailed specification of the tasks and actions to be performed by the security activity, the expected outcomes and preconditions (how); and
 - 6) an indication as to when (relative to Application Security Life Cycle Reference Model) the tasks and actions of the security activity should be performed (when).
- d) **ASC Verification Measurement (M):** This section should contain the following information pertinent to the verification measurements defined by the ASC:
- 1) a high-level description of the verification measurement (what);
 - 2) a description of the asset that is verified (audited) by the verification measurement (where);
 - 3) a definition of the roles (and required qualifications) involved in the execution of the tasks and actions involved in the verification activity (who);
 - 4) an indication of the complexity and costs of the verification measurement (how much);
 - 5) a detailed specification of the tasks and actions to be performed by the verification activity, the expected outcomes and preconditions (how); and
 - 6) an indication as to when (relative to Application Security Life Cycle Reference Model) the tasks and actions of the verification activity should be performed (when).

Further details for each information requirement are provided in [5.2.4](#).

5.2.2 Integrity assurance

[ISO/IEC 27034-5:2017](https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68873d2688/iso-iec-27034-5-2017)

[https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-](https://standards.iteh.ai/catalog/standards/sist/19474081-571d-4d5c-8522-68873d2688/iso-iec-27034-5-2017)

In order to ensure the integrity of contents of ASCs, an ASC should be 'signable' (or similar recognized method). It should support cascading and multiple e-signatures as well as timestamps.

5.2.3 Multilingual/multiregional data representation

In order to ensure global communication of ASCs, the ASC data structure should support localized text and the specification of information items, processes or ICT in multiple languages.

5.2.4 ASC information requirements

5.2.4.1 Identification (M)

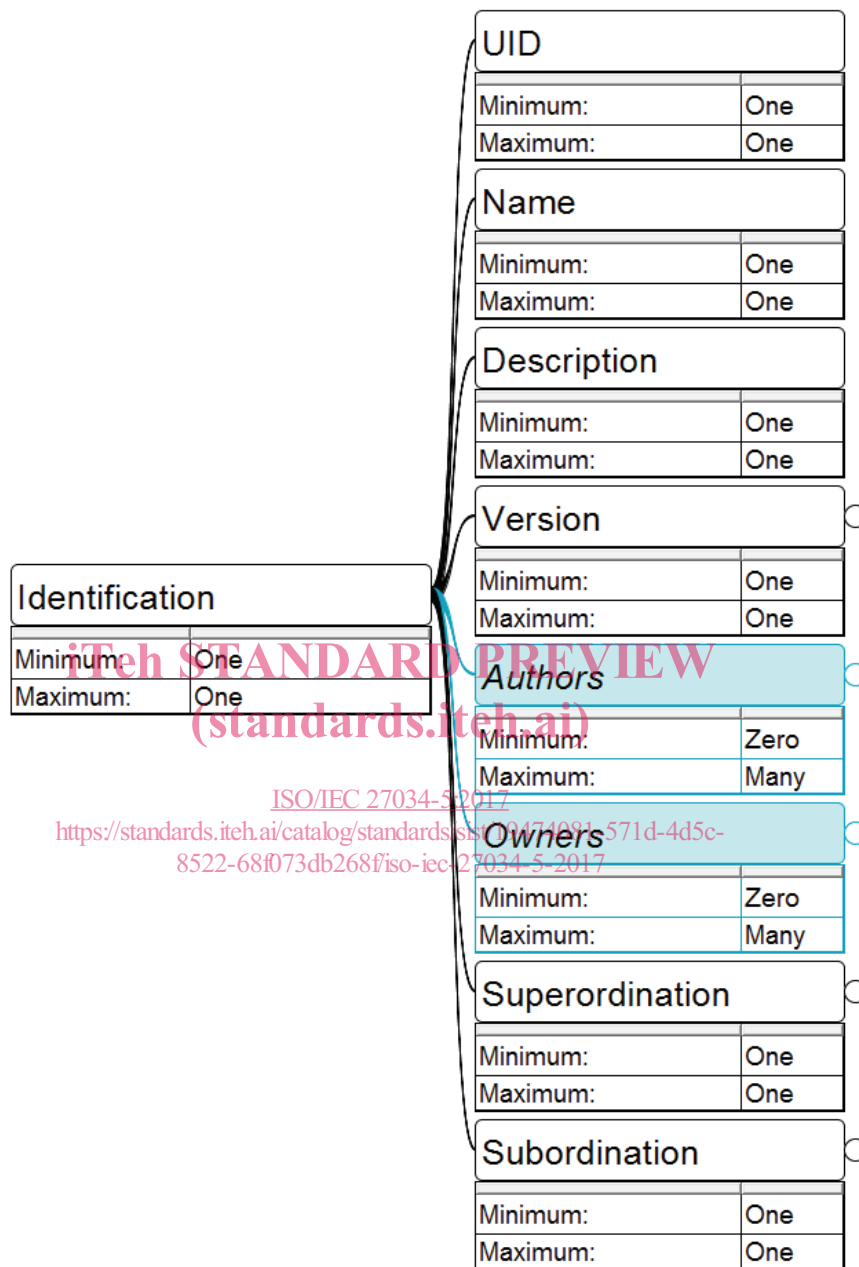


Figure 2 — Identification section of an ASC

As shown in [Figure 2](#), an ASC should contain the following information pertinent to its identity:

- a) Identification information about the ASC including:
 - 1) **UID (M)**: A unique identifier inside the schema;
 - 2) **Name (M)**: A representative name;
- b) **Description (M)**: High-level description of the ASCs intent and scope;