

# American National Standard

INCITS/ISO/IEC 27034-5:2017 (2019)

(ISO/IEC 27034-5:2017, IDT)

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

**Developed by**



*Where IT all begins*



## INCITS/ISO/IEC 27034-5:2017 (2019)

### PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.**

Date of ANSI Approval: 10/24/2019

Published by American National Standards Institute,  
25 West 43rd Street, New York, New York 10036

Copyright 2019 by Information Technology Industry Council  
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

First edition  
2017-10

---

---

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

*Technologies de l'information — Techniques de sécurité — Sécurité des applications —*

*Partie 5: Protocoles et structure de données de contrôles de sécurité d'application*



Reference number  
ISO/IEC 27034-5:2017(E)

© ISO/IEC 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

This is a preview of "INCITS/ISO/IEC 27034...". Click here to purchase the full version from the ANSI store.

## Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviated terms</b> .....	<b>2</b>
<b>5 Application Security Control Structure</b> .....	<b>2</b>
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
<b>6 Application Security Life Cycle Reference Model</b> .....	<b>14</b>
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

This is a preview of "INCITS/ISO/IEC 27034...". [Click here to purchase the full version from the ANSI store.](#)

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
<b>7</b>	<b>ASC Package.....</b>	<b>31</b>
	<b>Bibliography.....</b>	<b>33</b>

This is a preview of "INCITS/ISO/IEC 27034...". Click here to purchase the full version from the ANSI store.

## 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](http://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](http://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](http://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.