INTERNATIONAL STANDARD

ISO/IEC 27034-6

First edition
2016-10-01

Information technology — Security techniques — Application security —

Part 6: Case studies

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

Partie 6: Études de cas

Reference number
ISO/IEC 27034-6:2016(E)

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, 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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **1**
5 Security guidance for specific applications ... **1**
5.1 General ... 1
5.2 ASC example: Java code revision for mobile applications ... 2
5.2.1 General ... 2
5.2.2 Purpose ... 2
5.2.3 Context ... 2
5.2.4 ORGANIsation Information classification guidelines ... 2
5.2.5 Levels of trust included in the ORGANIsation ASC Library ... 2
5.2.6 Outcome ... 3
5.2.7 ORGANIsation stakeholders involved in these ASCs ... 4
5.2.8 Descriptions of sample ASCs ... 6
5.3 Case study: Developing ASCs to address the issue of privacy for two countries ... 19
5.3.1 General ... 19
5.3.2 Purpose ... 19
5.3.3 Context ... 19
5.4 Case study: Integration of third-party ASCs ... 21
5.4.1 General ... 21
5.4.2 Purpose ... 21
5.4.3 Context ... 21
5.5 Case study: Using the ASLCRM to facilitate implementation of ASCs by different development groups inside an organization ... 24
5.5.1 General ... 24
5.5.2 Purpose ... 24
5.5.3 Context ... 24
5.6 Case study: Implementation of third-party ASCs in a secure development life cycle process ... 26
5.6.1 General ... 26
5.6.2 Purpose ... 26
5.6.3 Context ... 26
5.6.4 Preparation phase (1.00) ... 27
5.6.5 Requirements phase (2.00) ... 30
5.6.6 Design phase (3.00) ... 31
5.6.7 Implementation phase (4.00) ... 34
5.6.8 Verification phase (5.00) ... 36
5.6.9 Release phase (6.00) ... 37
5.6.10 Sustainment, support and servicing phase (7.00) ... 38
Annex A (informative) **XML examples for case studies in 5.2** ... **41**
Bibliography ... **70**

© ISO/IEC 2016 – All rights reserved

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 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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 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.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

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

© ISO/IEC 2016 – All rights reserved

Introduction

0.1 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 formal structure should be defined for representing ASCs and certain other components of the framework.

0.2 Purpose

The purpose of this document is to provide examples of security guidance for organizations to acquire, develop, outsource and manage security for their specific applications through their life cycle.

0.3 Targeted Audiences

0.3.1 General

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

a) domain experts.

0.3.2 Domain experts

Domain experts contributing knowledge in application provisioning, operating or auditing, who need to

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.

© ISO/IEC 2016 – All rights reserved

Information technology — Security techniques — Application security —

Part 6: Case studies

1 Scope

This document provides usage examples of ASCs for specific applications.

NOTE Herein specified ASCs are provided for explanation purposes only and the audience is encouraged to create their own ASCs to assure the application security.

2 Normative references

There are no normative references cited in this document.

3 Terms and definitions

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

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

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

4 Abbreviated terms

ASC application security control

ASLC application security life cycle

ASLCRM application security life cycle reference model

ONF organization normative framework

5 Security guidance for specific applications

5.1 General

Guidelines play an important role for companies trying to implement any best practice or ISO standard because they instruct how to institutionalize the practices or rules and, sometimes, the guidance is based on common examples.

Companies benefit from this guidance as it demonstrates, as a practical example, how to structure ASCs for specific applications using the recommended XML data structure defined in ISO/IEC 27034-5-1 and for the implementation of the Organizational Normative Framework.

© ISO/IEC 2016 – All rights reserved