ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA Jún 2021

STN	**Informačné technológie Bezpečnostné metódy Aplikačná bezpečnosť Časť 6: Prípadové štúdie**	**STN ISO/IEC 27034-6 97 4102**

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

Informationstechnologie
Sicherheitstechniken
Sicherheit von Anwendungen
Teil 6: Fallstudien

Táto norma obsahuje anglickú verziu ISO/IEC 27034-6: 2016.

This standard includes the English version of ISO/IEC 27034-6: 2016.

132825

Anotácia

Účelom tohto dokumentu je poskytnúť príklady opatrení bezpečnosti aplikácií v organizácii, aby mohli počas svojho životného cyklu obstarávať, vyvíjať, zadávať a spravovať zabezpečenie svojich špecifických aplikácií.

Národný predhovor

Normatívne referenčné dokumenty

V tomto dokumente nie sú uvedené žiadne normatívne referenčné dokumenty.

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

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.

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.

INTERNATIONAL STANDARD ISO/IEC 27034-6:2016(E)

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.