

INFOTEHNOLOOGIA
Turbemeetodid
Infoturvaintsidentide haldus

Information technology
Security techniques
Information security incident management
(ISO/IEC 27035:2011)

EESTI STANDARDI EESSÕNA**NATIONAL FOREWORD**

<p>See Eesti standard EVS-ISO/IEC 27035:2012 „Infotehnoloogia. Turbemeetodid. Infoturvaintsidentide haldus“ sisaldab rahvusvahelise standardi ISO/IEC 27035:2011 „Information technology – Security techniques – Information security incident management“ identset ingliskeelset teksti.</p>	<p>This Estonian Standard EVS-ISO/IEC 27035:2012 consists of the identical English text of the International Standard ISO/IEC 27035:2011 “Information technology – Security techniques – Information security incident management”.</p>
<p>Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.</p>	<p>Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian standard has been published by the Estonian Centre for Standardisation.</p>
<p>Standard EVS-ISO/IEC 27035:2012 on jõustunud sellekohase teate avalamisega EVS Teataja 2012. aasta septembrikuu numbris.</p>	<p>This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.</p>
<p>Standard on kättesaadav Eesti Standardikeskusest.</p>	<p>The standard is available from the Estonian Centre for Standardisation.</p>

Käsitlusala

See standard annab struktureeritud ja plaanitud metoodika, millega

- avastada infoturvaintsidente, neist teatada ja neid hinnata;
- reageerida infoturvaintsidentidele ja hallata neid;
- avastada, hinnata ja hallata infoturvanõrkusi;
- infoturvaintsidentide ja -nõrkuste haldamise tulemusena täiustada pidevalt infoturvaintsidentide ja -nõrkuste haldust.

See standard annab juhiseid suurtele ja keskmistele organisatsioonidele infoturvaintsidentide halduse kohta. Väiksemad organisatsioonid võivad kasutada selles standardis kirjeldatud dokumentide, protsesside ja rutiinide põhikomplekti vastavalt oma suurusele ja tegevusala tüübile sõltuvalt infoturvariskilisest olukorrast. Standard annab juhiseid ka välistele organisatsioonidele, kes osutavad infoturvaintsidentide halduse teenuseid.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja aadressile standardiosakond@evs.ee.

ICS 35.040

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact the Estonian Centre for Standardisation:
Aru 10, 10317 Tallinn, Estonia; www.evs.ee; phone 605 5050; e-mail info@evs.ee

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	2
4.1 Basic concepts	2
4.2 Objectives	3
4.3 Benefits of a structured approach	4
4.4 Adaptability	5
4.5 Phases	6
4.6 Examples of information security incidents	7
5 Plan and prepare phase	8
5.1 Overview of key activities	8
5.2 Information security incident management policy	10
5.3 Information security incident management integration in other policies	12
5.4 Information security incident management scheme	13
5.5 Establishment of the ISIRT	18
5.6 Technical and other support (including operational support)	19
5.7 Awareness and training	20
5.8 Scheme testing	22
6 Detection and reporting phase	22
6.1 Overview of key activities	22
6.2 Event detection	25
6.3 Event reporting	25
7 Assessment and decision phase	26
7.1 Overview of key activities	26
7.2 Assessment and initial decision by the PoC	28
7.3 Assessment and incident confirmation by the ISIRT	30
8 Responses phase	31
8.1 Overview of key activities	31
8.2 Responses	32
9 Lessons learnt phase	40
9.1 Overview of key activities	40
9.2 Further information security forensic analysis	40
9.3 Identifying the lessons learnt	41
9.4 Identifying and making improvements to information security control implementation	42
9.5 Identifying and making improvements to information security risk assessment and management review results	42
9.6 Identifying and making improvements to the information security incident management scheme	42
9.7 Other improvements	43
Annex A (informative) Cross reference table of ISO/IEC 27001 vs ISO/IEC 27035	44
Annex B (informative) Examples of information security incidents and their causes	47
Annex C (informative) Example approaches to the categorization and classification of information security events and incidents	50

Annex D (informative) Example information security event, incident and vulnerability reports and forms.....	62
Annex E (informative) Legal and regulatory aspects	74
Bibliography.....	76

This document is a preview generated by EVS

Introduction

In general, information security policies or controls alone will not guarantee total protection of information, information systems, services or networks. After controls have been implemented, residual vulnerabilities are likely to remain that can make information security ineffective and thus information security incidents possible. This can potentially have both direct and indirect adverse impacts on an organization's business operations. Further, it is inevitable that new instances of previously unidentified threats will occur. Insufficient preparation by an organization to deal with such incidents will make any response less effective, and increase the degree of potential adverse business impact. Therefore, it is essential for any organization serious about information security to have a structured and planned approach to:

- detect, report and assess information security incidents;
- respond to information security incidents, including the activation of appropriate controls for the prevention and reduction of, and recovery from, impacts (for example in the support of crisis management areas);
- report information security vulnerabilities that have not yet been exploited to cause information security events and possibly information security incidents, and assess and deal with them appropriately;
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

This International Standard provides guidance on information security incident management in Clause 4 to Clause 9. These clauses consist of several subclauses, which include a detailed description of each phase.

The term 'information security incident management' is used in this International Standard to encompass the management of not just information security incidents but also information security vulnerabilities.

Information technology — Security techniques — Information security incident management

1 Scope

This International Standard provides a structured and planned approach to:

- a) detect, report and assess information security incidents;
- b) respond to and manage information security incidents;
- c) detect, assess and manage information security vulnerabilities; and
- d) continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

This International Standard provides guidance on information security incident management for large and medium-sized organizations. Smaller organizations can use a basic set of documents, processes and routines described in this International Standard, depending on their size and type of business in relation to the information security risk situation. It also provides guidance for external organizations providing information security incident management services.

2 Normative references

The following referenced documents are indispensable for the application 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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1

information security forensics

application of investigation and analysis techniques to capture, record and analyse information security incidents

3.2

information security incident response team

ISIRT

team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle