INFOTEHNOLOOGIA
Turbemeetodid
Infoturvaintsidentide haldus

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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

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.

Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.

Standard EVS-ISO/IEC 27035:2012 on jõustunud sellekohase teate avaldamisega EVS Teataja 2012. aasta septembrikuu numbris.

Standard on kättesaadav Eesti Standardikeskusest.

NATIONAL FOREWORD

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”.

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.

This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.

The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

See standard annab struktureeritud ja plaanitud metoodika, millega

a) avastada infoturvaintsidente, neist teatada ja neid hinnata;

b) reageerida infoturvaintsidentidele ja hallata neid;

c) avastada, hinnata ja hallata infoturvanõrkusi;

d) 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

Contents

Page

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