INFOTEHNOLOOGIA
Infoturvaintsidentide haldus
Osa 1: Põhimõtted ja protsess

Information technology
Information security incident management
Part 1: Principles and process
(ISO/IEC 27035-1:2023, identical)

EVS • EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-ISO/IEC 27035-1:2024 sisaldab rahvusvahelise standardi ISO/IEC 27035-1:2023 „Information technology. Information security incident management. Part 1: Principles and process“ identset ingliskeelset teksti.	This Estonian Standard EVS-ISO/IEC 27035-1:2024 consists of the identical English text of the International Standard ISO/IEC 27035-1:2023 „Information technology. Information security incident management. Part 1: Principles and process“.
Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 04, standardi avaldamist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus.	Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 04, the Estonian Standard has been published by the Estonian Centre for Standardisation and Accreditation.
Standard EVS-ISO/IEC 27035-1:2024 on jõustunud sellekohase teate avaldamisega EVS Teatajas.	Standard EVS-ISO/IEC 27035-1:2024 has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	This standard is available from the Estonian Centre for Standardisation and Accreditation.

Käsitlusala

See dokument on ISO/IEC 27035 sarja standardite alusdokument. Selles esitatakse infoturvaintsidentide haldamise põhitegevuste kontseptsioonid, põhimõtted ja protsessid, mis pakuvad struktureeritud lähenemisviisi, kuidas valmistuda intsidentide avastamiseks, aruandluseks, hindamiseks ja neile reageerimiseks ning saadud kogemuste rakendamiseks.

Selles dokumendis antud infoturvaintsidentide haldusprotsessi ja selle põhitegevuste juhendid on üldised ja mõeldud kohaldamiseks kõikidele organisatsioonidele, olenemata nende tüübist, suurusest või olemusest. Organisatsioonid saavad kohandada juhiseid vastavalt oma tüübile, suurusele ja äritegevuse iseloomule seoses infoturvariskidega. See dokument kehtib ka infoturvaintsidentide haldusteenuseid pakkuvate väliste organisatsioonide kohta.

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

ICS 35.030

[Blank page]

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27035-1:2016), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— new terms “incident management team” and “incident coordinator” are defined in Clause 3;

— new subclauses 4.5, 4.6 and 4.7 are added in Clause 4;

— the title of Clause 5 has been changed to “Process”;

— Annex C has been updated;

— a new Annex D has been added;

— the text has been editorially revised.

A list of all parts in the ISO/IEC 27035 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 27035 series provides additional guidance to the controls on incident management in ISO/IEC 27002. These controls should be implemented based upon the information security risks that the organization is facing.

Information security policies or controls alone do not guarantee total protection of information, information systems, services or networks. After controls have been implemented, residual vulnerabilities are likely to remain that can reduce the effectiveness of information security and facilitate the occurrence of information security incidents. This can potentially have direct and indirect adverse consequences on an organization's business operations. Furthermore, it is inevitable that new instances of previously unidentified threats cause incidents to occur. Insufficient preparation by an organization to deal with such incidents makes any response less effective, and increases the degree of potential adverse business consequence. Therefore, it is essential for any organization desiring a strong information security programme to have a structured and planned approach to:

— plan and prepare information security incident management, including policy, organization, plan, technical support, awareness and skills training, etc.;

— detect, report and assess information security incidents and vulnerabilities involved with the incident;

— respond to information security incidents, including the activation of appropriate controls to prevent, reduce, and recover from impact;

— deal with reported information security vulnerabilities involved with the incident appropriately;

— learn from information security incidents and vulnerabilities involved with the incident, implement and verify preventive controls, and make improvements to the overall approach to information security incident management.

The ISO/IEC 27035 series is intended to complement other standards and documents that give guidance on the investigation of, and preparation to investigate, information security incidents. The ISO/IEC 27035 series is not a comprehensive guide, but a reference for certain fundamental principles and a defined process that are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise.

While the ISO/IEC 27035 series encompasses the management of information security incidents, it also covers some aspects of information security vulnerabilities. Guidance on vulnerability disclosure and vulnerability handling by vendors is also provided in ISO/IEC 29147 and ISO/IEC 30111, respectively.

The ISO/IEC 27035 series also intends to inform decision-makers when determining the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyse and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

Further information about investigative standards is available in Annex A.

Information technology — Information security incident management —

Part 1: Principles and process

1 Scope

This document is the foundation of the ISO/IEC 27035 series. It presents basic concepts, principles and process with key activities of information security incident management, which provide a structured approach to preparing for, detecting, reporting, assessing, and responding to incidents, and applying lessons learned.

The guidance on the information security incident management process and its key activities given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance according to their type, size and nature of business in relation to the information security risk situation. This document is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

3.1.1
incident management team
IMT
team consisting of appropriately skilled and trusted members of an organization responsible for leading all information security incident management activities, in coordination with other parties both internal and external, throughout the incident lifecycle

Note 1 to entry: The head of this team can be called the incident manager who has been appointed by top management to adequately respond to all types of incidents.