Avaldatud eesti keeles: veebruar 2008
Jõustunud Eesti standardina: veebruar 2008

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse tegevusjuhis
(ISO/IEC 27002:2005)

Information technology
Security techniques
Code of practice for information security management
(ISO/IEC 27002:2005)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard:

– on rahvusvahelise standardi ISO/IEC 17799:2005 “Information technology – Security techniques – Code of practice for information security management” ingliskeelse teksti identne tõlge eesti keelde ning tõlgendamise erimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest,

– on kinnitatud Eesti Standardikeskuse 29.01.2008 käskkirjaga nr 12,

– jõustub sellekohase teate avaldamisel EVS Teataja 2008. aasta veebruarikuu numbris.

Standardi tõlkis Vello Hanson, tehnilise korrektuuri tegi Taavi Valdlo, käesoleva standardi on heaks kiitnud tehniline komitee EVS/TK 4 “Infotehnoloogia”.

Standardi väljaandmist rahastas osaliselt Majandus- ja Kommunikatsiooniministeerium.

Käesolev standard arvestab juulis 2007 avaldatud tehnilist parandust (Technical Corrigendum 1 (2007-07)), millega muudeti standardi tähiseks ISO/IEC 27002:2005.

Standard asendab Eesti standardi EVS-ISO/IEC 17799:2003.

This standard is the Estonian [et] version of the International Standard ISO/IEC 27002:2005. It was translated by Estonian Centre for Standardisation. This standard also consists the English text.

ICS 35.080
Võtmesõnad: infoturve, haldus, tegevusjuhis
Hinnagrupp TC

SISUKORD

Lk

CONTENTS

Page

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IECga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele.

Ühise tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse rahvuslikele kogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75 % hääletanud rahvuslikelt kogudelt.

Tuleb pöörata tähelepanu võimalusele, et mõned selle rahvusvahelise standardi elemendid võivad olla patendiõiguse objektiks. ISO ega IEC ei ole kohustatud mingeid või kõiki selliseid patendiõigusi välja selgitama.

Rahvusvahelise standardi ISO/IEC 17799 koostas ISO/IEC ühendatud tehniline komitee JTC 1 "Infotehnoloogia" alamkomitee SC 27, "Infoturbemeetodid".

Käesolev teine redaktsioon tühistab ja asendab esimese redaktsiooni (ISO/IEC 17799:2000), mis on tehniliselt läbi vaadatud.

Alamkomitees ISO/IEC JTC 1/SC 27 on väljatöötamisel infoturbe halduse süsteemi (ISMS) rahvusvaheliste standardite sari. Sellesse sarja kuuluvad turbehaldussüsteemi nõuete, riskihalduse, -mõõdustiku ja -mõõtmise ning teostussuuniste rahvusvahelised standardid. See sari saab nummerduse, milles kasutatakse numbrisarja 27000 jj.

Alates aastast 2007 on ISO/IEC 17799 käesolev uus redaktsioon esitatud ühildatuna uue nummerdusega kujul ISO/IEC 27002.

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 17799 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

This second edition cancels and replaces the first edition (ISO/IEC 17799:2000), which has been technically revised.

A family of Information Security Management System (ISMS) International Standards is being developed within ISO/IEC JTC 1/SC 27. The family includes International Standards on information security management system requirements, risk management, metrics and measurement, and implementation guidance. This family will adopt a numbering scheme using the series of numbers 27000 et seq.

From 2007, it is proposed to incorporate the new edition of ISO/IEC 17799 into this new numbering scheme as ISO/IEC 27002.

0 SISSEJUHATUS

0.1 Mis on infoturve?

Teave on vara, mis nagu muudki tähtsad talitlusvarad on organisatsiooni tegevusele oluline ja seega vajab asjakohast kaitset. See on eriti tähtis üha enam kokkuühendatud tegevuskeskkonnas. Sellise üha kasvava ühendatavuse tulemusena on teave praegu avatud üha arvukamatele ja mitmekesisematele ohtudele ja nõrkustele (vt ka OECD "Suunised infosüsteemide ja võrkude turbe kohta").

Teave võib eksisteerida paljudes vormides. Teda võib paberile trükkida või kirjutada, elektrooniliselt salvestada, edastada posti teel või elektrooniliste vahenditega, näidata filmides või kõnelda vestluses. Teave, millise kuju ta ka ei võtaks või milliste vahenditega teda ka ei jagataks või talletataks, peaks alati olema asjakohaselt kaitstud.

Infoturve on teabe kaitsmine mitmesuguste ohtude eest, eesmärgiga tagada jätkusuutlikkus, minimeerida äririski ning maksimeerida investeeringute tasuvust ja soodsaid ärilisi võimalusi.

Teabe turvalisus saavutatakse rakendades sobivat meetmestikku, sealhulgas poliitikaid, protsesse, protseduure, organisatsioonilisi struktuure ning tarkvara- ja riistvarafunktsioone. Organisatsiooni konkreetsete turva- ja tegevuseesmärkide saavutamise tagamiseks tuleb neid meetmeid kehtestada, evitada, seirata, läbi vaadata ja vajaduse korral täiustada. Seda tuleks teha kooskõlas muude talitluse halduse protsessidega.

0.2 Miks vajatakse infoturvet

Teave ning selle tugiprotsessid, süsteemid ja võrgud on olulised ärilised varad. Teabe turvalisuse määratlemine, saavutamine, säilitamine ja täiustamine võib olla oluline konkurentsivõime, rahavoo, rentaabluse, õigusaktidele vastavuse ja ärilise kuvandi säilitamiseks.

Üha enam ähvardavad organisatsioone ja nende infosüsteeme turvaohud väga mitmesugustest allikatest, sealhulgas arvutipõhine pettus, spionaaž, sabotaaž, vandalism, kahjutuli,

0 INTRODUCTION

0.1 What is information security?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

0.2 Why information security is needed?

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism,

üleujutus. Sellised kahjustuste allikad nagu kahjurkood, arvutite häkkimine ja teenusetõkestuslikud ründed on muutunud tavalisemaks, ambitsioonikamaks ja üha rafineeritumaks.

Infoturve on tähtis nii avaliku kui ka erasektori ettevõtetele ja elutähtsate infrastruktuuride kaitsmisele. Mõlemas sektoris toimib infoturve võimaldajana, näiteks e-riigi või e-tegevuse saavutamisel ning kaasnevate riskide vältimisel või vähendamisel. Avalike ja privaatvõrkude kokkuühendamine ja inforessursside ühiskasutus raskendavad pääsu reguleerimise saavutamist. Suund hajustöötlusele on nõrgendanud keskse spetsialistide sooritatava reguleerimise toimivust.

Paljud infosüsteemid pole kavandatud turvalisteks. Tehniliste vahenditega võib saavutada piiratud turvet ning seda tuleks toetada sobiva halduse ja protseduuridega. Vajalike meetmete väljaselgitamine nõuab hoolikat plaanimist ja üksikasjadele tähelepanu pööramist. Infoturbe haldus nõuab vähemalt organisatsiooni kõigi töötajate osalust. Ta võib nõuda ka aktsionäride, tarnijate, kolmandate poolte, klientide või muude väliste poolte osalust. Vajalikuks võivad osutuda ka asjatundjate nõuanded välistest organisatsioonidest.

0.3 Kuidas selgitada välja turvanõuded

On oluline, et organisatsioon selgitaks välja oma turvanõuded. Selleks on kolm peamist allikat.

1. Üks allikas tuleneb organisatsiooni riskide kaalutlemisest, mis arvestab organisatsiooni üldist tegutsemise strateegiat ja eesmärke. Riskide kaalutlemise teel tuvastatakse ohud varadele, hinnatakse nõrkused ohtude suhtes ja ohtude teostumise tõenäosus ning hinnatakse nende võimalik toime.

2. Teine allikas on õigusaktide, statuudi, eeskirjade ja lepingute nõuded, mida peavad täitma organisatsioon, ta äripartnerid, allettevõtjad ja teenuseandjad, ning nende sotsiaalne ja kultuuriline keskkond.

3. Veel üks allikas on see konkreetne infotöötluse printsiipide, eesmärkide ja talitlusnõuete kogum, mille on organisatsioon välja töötanud oma tegevuse toetuseks.

fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.

0.3 How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements.

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.

3. A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations.

0.4 Turvariskide kaalutlemine

Turvanõuded selgitatakse välja turvariskide metoodilise kaalutlemisega. Kulutused turvameetmetele tuleb tasakaalustada äriliste kahjudega, mis võivad tuleneda turvariketest.

Riski kaalutlemise tulemused aitavad suunata ja määrata sobivaid haldustoiminguid ja prioriteete teabe turvariskide halduseks ja nende riskide eest kaitsma valitud turvameetmete rakendamiseks.

Riski kaalutlemist tuleks korrata perioodiliselt, et võtta arvesse kõiki muutusi, mis võivad mõjutada riski kaalutlemise tulemusi.

Lisateavet turvariskide kaalutlemise kohta on jaotises 4.1 "Turvariskide kaalutlemine".

0.4 Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

More information about the assessment of security risks can be found in clause 4.1 “Assessing security risks”.

0.5 Turvameetmete valimine

Kui turvanõuded ja -riskid on välja selgitatud ja on tehtud otsused riskide käsitluse kohta, tuleks valida ja evitada sobivad turvameetmed, millega tagada riskide vähendamine vastuvõetava tasemeni. Sõltuvalt olukorrast võib turvameetmeid valida käesolevast standardist või muudest meetmestikest või töötada erivajaduste rahuldamiseks välja uusi. Turvameetmete valimine sõltub organisatsiooni otsustest, mis põhinevad riski aktsepteerimise kriteeriumidel, riski käsitluse võimalustel ja üldisest organisatsioonis rakendatavast riskihalduse metoodikast, ning peaksid järgima ka kõiki asjassepuutuvaid kodumaiseid ja rahvusvahelisi õigusakte ja eeskirju.

Mõningaid selles standardis leiduvaid turvameetmeid võib lugeda infoturbe haldust suunavateks põhimõteteks ja nad on kohaldatavad enamikule organisatsioonidele. Detailsemalt seletatakse neid allpool alajaotises "Infoturbe lähtepunkt".

Lisateavet meetmete valimise ja muude riski käsitlemise võimaluste kohta on jaotises 4.2 "Turvariskide käsitlus".

0.5 Selecting controls

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate. The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading “Information security starting point”.

More information about selecting controls and other risk treatment options can be found in clause 4.2 "Treating security risks".

0.6 Infoturbe lähtepunkt

Mitmeid turvameetmeid võib lugeda heaks lähtepunktiks infoturbe teokstegemisele. Nad kas põhinevad olulistel õiguslikel nõuetel või siis peetakse neid infoturbe levinud menetlustavaks.

0.6 Information security starting point

A number of controls can be considered as a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common practice for information security.

Organisatsioonile õiguslikust vaatepunktist olulisteks peetavate turvameetmete hulka kuuluvad sõltuvalt kohaldatavaist õigusaktidest

a) andmekaitse ja isikuteabe privaatsus (vt 15.1.4),

b) organisatsiooni dokumentide kaitse (vt 15.1.3),

c) intellektuaalse omandi õigused (vt 15.1.2).

Infoturbe levinud menetlustavaks peetavate meetmete hulka kuuluvad

a) infoturbepoliitika dokument (vt 5.1.1),

b) infoturbe alaste kohustuste jaotamine (vt 6.1.3);

c) infoturbe alane teadlikkus, haridus ja koolitus (vt 8.2.2),

d) õige töötlus rakendustes (vt 12.2),

e) tehniliste nõrkuste haldus (vt 12.6),

f) jätkusuutlikkuse haldus (vt 14),

g) infoturbeintsidentide ja -täiustuste haldus (vt 13.2).

Need meetmed on rakendatavad enamikus organisatsioonides ja keskkondades.

Tuleks silmas pidada, et ehkki kõik meetmed selles standardis on olulised ja neid tuleks arvestada, tuleks iga meetme asjakohasus määrata konkreetsete organisatsiooni ähvardavate riskide valguses. Seega, kuigi ülalkirjeldatud lähenemisviisi peetakse heaks lähtepunktiks, ei asenda ta riskide kaalutlemisel põhinevat turvameetmete valimist.

Controls considered to be essential to an organization from a legislative point of view include, depending on applicable legislation:

a) data protection and privacy of personal information (see 15.1.4);

b) protection of organizational records (see 15.1.3);

c) intellectual property rights (see 15.1.2).

Controls considered to be common practice for information security include:

a) information security policy document (see 5.1.1);

b) allocation of information security responsibilities (see 6.1.3);

c) information security awareness, education, and training (see 8.2.2);

d) correct processing in applications (see 12.2);

e) technical vulnerability management (see 12.6);

f) business continuity management (see 14);

g) management of information security incidents and improvements (see 13.2).

These controls apply to most organizations and in most environments.

It should be noted that although all controls in this standard are important and should be considered, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

0.7 Kriitilised edutegurid

Kogemused on näidanud, et infoturbe edukaks evituseks organisatsioonis on sageli otsustavalt olulised järgmised tegurid:

a) turvapoliitika, -eesmärgid ja -tegevused, mis kajastavad ärieesmärke;

b) organisatsiooni kultuuriga kooskõlas olev infoturbe evituse, käigushoiu, seire ja täiustamise metoodika ja raamstruktuur;

c) juhtkonna kõigi tasemete nähtav toetus ja pühendumus;

0.7 Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

a) information security policy, objectives, and activities that reflect business objectives;

b) an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;

c) visible support and commitment from all levels of management;

d) hea turvanõuete, riski kaalutlemise ja riskihalduse tundmine;

e) infoturbe tõhus propageerimine kõigile juhtidele, töötajatele ja muudele osapooltele nende teadlikkuse saavutamiseks;

f) suuniste andmine infoturbepoliitika ja -standardite kohta kõigile juhtidele, töötajaile ja muudele pooltele;

g) hoolitsemine infoturbe halduse tegevuste finantseerimise eest;

h) asjakohase teadlikkuse, koolituse ja hariduse tagamine;

i) toimiva infoturbeintsidentide halduse protsessi rajamine;

j) infoturbe halduse soorituse hindamiseks ja täiustusettepanekute näol tagasiside saamiseks kasutatava mõõtesüsteemi[1] evitamine.

[1] Tuleb silmas pidada, et infoturbe mõõtmised ei kuulu käesoleva standardi käsitlusalasse.

d) a good understanding of the information security requirements, risk assessment, and risk management;

e) effective marketing of information security to all managers, employees, and other parties to achieve awareness;

f) distribution of guidance on information security policy and standards to all managers, employees and other parties;

g) provision to fund information security management activities;

h) providing appropriate awareness, training, and education;

i) establishing an effective information security incident management process;

j) implementation of a measurement[1] system that is used to evaluate performance in information security management and feedback suggestions for improvement.

[1] Note that information security measurements are outside of the scope of this standard.

0.8 Omaenda suuniste väljatöötamine

Käesolevat tegevusjuhist võib lugeda lähtepunktiks, millest alustada organisatsioonispetsiifiliste suuniste väljatöötamist. Kõik selles tegevusjuhises leiduvad suunised ja meetmed ei ole võib-olla rakendatavad. Peale selle võivad osutuda vajalikeks lisameetmed, mida see standard ei sisalda. Kui koostatakse dokumente, mis sisaldavad lisasuuniseid või -meetmeid, on ehk kasulik kohaldatavail juhtudel lisada viited selle standardi jaotistele, et hõlbustada auditoritel ja äripartneritel vastavuse kontrollimist.

0.8 Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

INFOTEHNOLOOGIA. TURBEMEETODID
Infoturbe halduse tegevusjuhis

Information technology. Security techniques
Code of practice for information security management

1 KÄSITLUSALA

See standard rajab suunised ja üldpõhimõtted infoturbe halduse algatamiseks, evitamiseks, käigushoiuks ja täiustamiseks organisatsioonis. Standardis visandatud eesmärgid annavad üldisi suuniseid infoturbe halduse üldtunnustatud sihtide kohta.

Selle standardi juhtimiseesmärgid ja meetmed on mõeldud evitamiseks eesmärgiga täita riski kaalutlemise teel tuvastatud nõudeid. See standard võib olla praktiliseks juhiseks organisatsiooni turvastandardite ja toimiva turbehalduse tavade väljakujundamisel ning ta võib aidata luua usaldust organisatsioonidevahelistes ettevõtmistes.

1 SCOPE

This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

2 TERMINID JA MÄÄRATLUSED

Selle dokumendi otstarbeks kehtivad alljärgnevad määratlused.

2.1
vara
miski, millel on organisatsiooni jaoks väärtus.
[ISO/IEC 13335-1:2004]

2.2
meede
riskihalduse vahend, sealhulgas poliitika, protseduur, suunis, tava või organisatsiooniline struktuur, võib olla loomult administratiivne, tehniline, halduslik või juriidiline

MÄRKUS. Meedet kasutatakse ka turvameetme või vastumeetme tähenduses.

2 TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply.

2.1
asset
anything that has value to the organization
[ISO/IEC 13335-1:2004]

2.2
control
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature

NOTE Control is also used as a synonym for safeguard or countermeasure.