ÍST EN ISO/IEC 27000:2017

ÍSLENSKUR STAÐALL

STAÐLARÁÐ ÍSLANDS

Gildistaka 2017-04-20
ICS 29.240.01

Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Yfirlit og orðaforði

Information technology – Security techniques – Information security management systems – Overview and vocabulary

Staðfestur af Staðlaráði Íslands

1. prentun.

Eftirtaldir aðilar styrktu útgáfu þessa staðals á íslensku:

Advania

Borgun

Capacent

Fjármálaeftirlitið

Íslandsbanki

Landhelgisgæsla Íslands

Landsbankinn

Landslög

Landsspítali

Nasdaq verðbréfamiðstöð hf

Netorka hf

Nova

Opin kerfi hf

Orkufjarskipti

Orkuveita Reykjavíkur

Persónuvernd

Reykjavíkurborg

Ríkisskattstjóri

Síminn

Sjóvá

Tollstjóri

Tryggingamiðstöðin

Veritas Capital

Vodafone

Þekking hf

Þjóðskrá Íslands

ÍST EN ISO/IEC 27000:2017

Formáli íslensku þýðingarinnar

Þessi íslenski staðall, ÍST EN ISO/IEC 27000:2016, sem einnig er evrópskur og alþjóðlegur staðall, var staðfestur af Staðlaráði Íslands, sem er samstarfsvettvangur íslenskra hagsmunaaðila til að vinna að stöðlun og beitingu staðla. Íslenska þýðingin var gerð að tilhlutan Staðlaráðs Íslands og Fagstaðlaráðs í upplýsingatækni (FUT).

Vinnuhópinn skipuðu:
- Þorvarður Kári Ólafsson formaður
- Elísabet Árnadóttir
- Grímur Kjartansson
- Guðbjörn Sverrir Hreinsson
- Jón Kristinn Ragnarsson
- Ólafur Róbert Rafnsson
- Pétur S. Hilmarsson

Þessi staðall kemur í stað kafla 3 í ÍST ISO/IEC 27001:2005

Þýðingin er gerð til hagræðis fyrir íslenska notendur. Kappkostað hefur verið að hafa íslenska textann eins nákvæman eins og framast er unnt. Engu að síður getur Staðlaráð Íslands ekki ábyrgst að þýðingin endurspegli nákvæmlega merkingu frumtextans, orð fyrir orð.

Af þessum sökum er enski textinn birtur við hlið hins íslenska og til hans ber að leita komi til deilumála um túlkun ákvæða í staðlinum. Staðlarnir eru í stöðugri endurskoðun og þar með þýðingin. Notendur staðlanna eru eindregið hvattir til að koma athugasemdum og ábendingum til Staðlaráðs Íslands.

EVRÓPSKUR STAÐALL
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27000

Febrúar 2017

ICS 01.040.35; 03.100.70;35.030

Íslensk útgáfa

Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Yfirlit og orðaforði (ISO/IEC 27000:2016)

Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2016)

Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire (ISO/IEC 27000:2016)

Informationstecnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2016)

Þessi staðall er hin íslenska útgáfa evrópska staðalsins EN ISO/IEC 27000:2017. Hann var þýddur af Staðlaráði Íslands. Hann hefur sama gildi og opinberu útgáfurnar.

Þessi evrópski staðall var samþykktur af CEN 26. janúar 2017.

Meðlimir CEN og CENELEC eru skyldugir til að uppfylla þær kröfur starfsreglna CEN/CENELEC sem greina frá skilyrðum þess að þessi evrópski staðall sé gerður að landsstaðli án nokkurra breytinga. Hægt er að fá nýjustu lista og skráningartilvísanir sem varða slíka landsstaðla með því að biðja um slíkt hjá aðalskrifstofunni eða hjá hvaða CEN eða CENELEC meðlim sem er.

Þessi evrópski staðall er til í þremur opinberum útgáfum (ensku, frönsku og þýsku). Útgáfa á öðru tungumáli, þar sem meðlimur CEN eða CENELEC þýðir yfir á sitt tungumál á eigin ábyrgð og tilkynnir um útgáfuna til aðalskrifstofunnar, hefur sama gildi og opinberu útgáfurnar.

Meðlimir CEN og CENELEC eru landsstaðlaráð Austurríkis, Belgíu, Búlgaríu, Danmerkur, Eistlands, Finnlands, Frakklands, Grikklands, Hollands, Írlands, Íslands, Ítalíu, Króatíu, Kýpur, Lettlands, Litháen, Lúxemborgar, Makedóníu, Möltu, Noregs, Póllands, Portúgals, Rúmeníu, Serbíu, Slóvakíu, Slóveníu, Spánar, Stóra-Bretlands, Sviss, Svíþjóðar, Tékklands, Tyrklands, Ungverjalands og Þýskalands.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Aðalskrifstofa: Avenue Marnix 17
B - 1000 Brussels

ÍST EN ISO/IEC 27000:2017

Formáli evrópska staðalsins

Texti ISO/IEC 27000:2016 var saminn af tækninefndinni ISO/IEC/JTC 1 “Information technology“ (Upplýsingatækni) sem heyrir undir Alþjóða staðlasamtökin (ISO) og Alþjóða raftækniráðið (IEC), og hefur verið tekinn upp sem EN ISO/IEC 27000:2017.

Þessi evrópski staðall skal fá gildi landsstaðals, annaðhvort með útgáfu alsams texta eða með staðfestingu upprunalegu útgáfunnar, í síðasta lagi fyrir lok ágúst 2017, og landsstaðlar sem innihalda kröfur sem stangast á við kröfur þessa staðals skulu jafnframt felldir úr gildi í síðasta lagi fyrir lok ágúst 2017.

Athygli er vakin á því að sum atriði í þessum alþjóðastaðli gætu fallið undir einkaleyfi. CEN og/eða CENELEC bera ekki ábyrgð á að greina einhver eða öll slík einkaleyfi.

Samkvæmt starfsreglum CEN/CENELEC eru landsstaðlastofnanir eftirtalinna landa skyldug til að innleiða þennan evrópska staðal: Austurríki, Belgía, Búlgaría, Danmörk, Eistland, Finnland, Frakkland, Grikkland, Holland, Írland, Ísland, Ítalía, Króatía, Kýpur, Lettland, Litháen, Lúxemborg, Makedónía, Malta, Noregur, Pólland, Portúgal, Rúmenía, Serbía, Slóvakía, Slóvenía, Spánn, Stóra-Bretland, Sviss, Svíþjóð, Tékkland, Tyrkland, Ungverjaland og Þýskaland.

Yfirlýsing um samþykkt:

Texti ISO/IEC 27000:2016 var samþykktur óbreyttur af CEN sem EN ISO/IEC 27000:2017.

European foreword

The text of ISO/IEC 27000:2016 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27000:2017.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27000:2016 has been approved by CEN as EN ISO/IEC 27000:2017 without any modification.

ÍST EN ISO/IEC 27000:2017

Efnisyfirlit

Formáli íslensku þýðingarinnar ____ 4

Formáli evrópska staðalsins ____ 6

Formáli ____ 10

0 Inngangur ____ 12

1 Umfang ____ 14

2 Hugtök og skilgreiningar ____ 14

3 Stjórnunarkerfi um upplýsingaöryggi ____ 34
- 3.1 Almennt ____ 34
- 3.2 Hvað er stjórnunarkerfi um upplýsingaöryggi? ____ 36
- 3.3 Ferlisnálgun ____ 38
- 3.4 Hvers vegna stjórnunarkerfi um upplýsingaöryggi er mikilvægt ____ 38
- 3.5 Að koma á, vakta, viðhalda og endurbæta stjórnunarkerfi um upplýsingaöryggi ____ 40
- 3.6 Þættir sem ráða úrslitum um árangur stjórnunarkerfis um upplýsingaöryggi ____ 46
- 3.7 Ávinningur af staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi ____ 46

4 Staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi ____ 46
- 4.1 Almennar upplýsingar ____ 46
- 4.2 Staðlar sem lýsa yfirliti og hugtakanotkun ____ 48
- 4.3 Staðlar sem tilgreina kröfur ____ 48
- 4.4 Staðlar sem lýsa almennum leiðbeiningum ____ 50
- 4.5 Staðlar sem lýsa leiðbeiningum fyrir tiltekna geira ____ 54

Viðauki A (til upplýsingar)
Orðalag við lýsingu á ákvæðum ____ 60

Viðauki B (til upplýsingar)
Hugtak og eignarhald á hugtaki ____ 62

Ritaskrá ____ 70

Contents

European foreword ____ 7

Foreword ____ 11

0 Introduction ____ 13

1 Scope ____ 15

2 Terms and definitions ____ 15

3 Information security management systems ____ 35
- 3.1 General ____ 35
- 3.2 What is an ISMS? ____ 37
- 3.3 Process approach ____ 39
- 3.4 Why an ISMS is important ____ 39
- 3.5 Establishing, monitoring, maintaining and improving an ISMS ____ 41
- 3.6 ISMS critical success factors ____ 47
- 3.7 Benefits of the ISMS family of standards ____ 47

4 ISMS family of standards ____ 47
- 4.1 General information ____ 47
- 4.2 Standards describing an overview and terminology ____ 49
- 4.3 Standards specifying requirements ____ 49
- 4.4 Standards describing general guidelines ____ 51
- 4.5 Standards describing sector-specific guidelines ____ 55

Annex A (informative)
Verbal forms for the expression of provisions ____ 61

Annex B (informative)
Term and term ownership ____ 63

Bibliography ____ 71

Formáli

ISO (International Organization for Standardization – Alþjóðlegu staðlasamtökin) og IEC (International Electrotechnical Commission – Alþjóða raftækniráðið) mynda sérhæft kerfi fyrir alþjóðlega stöðlun. Staðlastofnanir einstakra landa sem eiga aðild að ISO eða IEC taka þátt í þróun alþjóðastaðla með starfrækslu tækninefnda sem hvor staðlasamtökin um sig setja á fót til að fást við afmörkuð tæknisvið. Tækninefndir ISO og IEC hafa samvinnu um efnissvið sem hagsmunir þeirra beggja tengjast. Aðrar alþjóðlegar stofnanir, bæði þær sem starfa á vegum ríkisstjórna og aðrar, taka einnig þátt, í samvinnu við ISO og IEC. Á sviði upplýsingatækni hafa ISO og IEC komið á fót sameiginlegri tækninefnd, ISO/IEC JTC 1.

Verklagsreglunum sem notaðar voru við samningu þessa skjals og þeim sem ætlað er að fylgja við frekara viðhald þess er lýst í Vinnureglum ISO/IEC, 1. hluta. Vakin er sérstök athygli á mismunandi samþykktarreglum fyrir mismunandi tegundir skjala. Þetta skjal var samið í samræmi við ritreglur Vinnureglna ISO/IEC, 2. hluta (sjá www.iso.org/directives) .

Athygli er vakin á því að sum atriði í þessu skjali gætu fallið undir einkaleyfi. ISO og IEC bera ekki ábyrgð á að tilgreina einstök eða öll slík einkaleyfi. Ef við á er nánari upplýsingar um einkaleyfi sem borin hafa verið kennsl á við samningu skjalsins að finna í Inngangi og/eða á lista ISO yfir mótteknar yfirlýsingar um einkaleyfi (sjá www.iso.org/patents).

Sé eitthvert vöruheiti nefnt í þessu skjali eru það upplýsingar til hægðarauka fyrir notendur en ber ekki að skilja sem meðmæli.

Varðandi útskýringar á merkingu tiltekinna heita og hugtaka sem tengjast samræmismati, og upplýsingar um hvernig ISO fer eftir grundvallarreglum WTO í Tæknilegum viðskiptahindrunum (TBT) vísast til eftirfarandi slóðar: Foreword – Supplementary information

Nefndin sem ber ábyrgð á þessu skjali er ISO/IEC JTC 1, *Information technology, undirnefnd* SC 27*, IT Security techniques.*

Þessi fjórða útgáfa fellir úr gildi og kemur í stað þriðju útgáfu (ISO/IEC 27000:2014), sem hefur verið tæknilega endurskoðuð.

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword – Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This fourth edition cancels and replaces the third edition (ISO/IEC 27000:2014), which has been technically revised.

0 Inngangur

0.1 Yfirlit

Í alþjóðastöðlum um stjórnunarkerfi er sett fram líkan sem fylgt er við uppsetningu og starfrækslu stjórnunarkerfis. Líkan þetta felur í sér tilhögun sem sérfræðingar á þessu sviði hafa sammælst um að sé sú nýjasta og háþróaðasta á alþjóðlegan mælikvarða. ISO/IEC JTC 1/SC 27 starfrækir sérfræðinganefnd sem annast þróun alþjóðlegra stjórnunarkerfisstaðla um upplýsingaöryggi, sem einnig eru nefndir staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi.

Með því að nota staðla í staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi geta skipulagsheildir þróað og innleitt ramma fyrir stjórnun öryggis upplýsingaverðmæta, þ. á m. fjármálaupplýsinga, hugverka og starfsmannaupplýsinga, eða upplýsinga sem viðskiptavinir eða þriðju aðilar hafa falið þeim. Einnig má nota þessa staðla við undirbúning fyrir sjálfstætt mat á stjórnunarkerfi þeirra um upplýsingaöryggi sem beitt er við verndun upplýsinga.

0.2 Staðlaröð á sviði stjórnunarkerfa um upplýsingaöryggi

Staðlaröð á sviði stjórnunarkerfa um upplýsingaöryggi (sjá grein 4) er ætlað að hjálpa skipulagsheildum af öllum stærðum og gerðum að innleiða og starfrækja stjórnunarkerfi um upplýsingaöryggi og er sett saman úr eftirfarandi alþjóðastöðlum sem bera almennu yfirskriftina *Upplýsingatækni – Öryggisaðferðir* (hér á eftir í númeraröð):

- ÍST EN ISO/IEC 27000, *Stjórnunarkerfi um upplýsingaöryggi – Yfirlit og orðaforði*
- ÍST EN ISO/IEC 27001, *Stjórnunarkerfi um upplýsingaöryggi – Kröfur*
- ÍST EN ISO/IEC 27002, *Starfsvenjur fyrir upplýsingaöryggisstýringar*
- ISO/IEC 27003, *Information security management system implementation guidance*
- ISO/IEC 27004, *Information security management – Measurement*
- ISO/IEC 27005, *Information security risk management*
- ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007, *Guidelines for information security management systems auditing*
- ISO/IEC TR 27008, *Guidelines for auditors on information security controls*
- ISO/IEC 27010, *Information security management for inter-sector and inter-organizational communications*
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*
- ISO/IEC 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
- ISO/IEC 27014, *Governance of information security*
- ISO/IEC TR 27015, *Information security management guidelines for financial services*
- ISO/IEC TR 27016, *Information security management – Organizational economics*
- ISO/IEC 27017, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- ISO/IEC 27018, *Code of practice for PII protection in public clouds acting as PII processors*
- ISO/IEC 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

ATHUGASEMD Hin almenna yfirskrift „Upplýsingatækni – Öryggisaðferðir“ sýnir að þessir staðlar voru samdir af sameiginlegu tækninefndinni ISO/IEC JTC 1, Information technology, undirnefnd SC 27, IT Security techniques.

Alþjóðastaðlar sem ekki bera þetta sama almenna heiti en eru einnig hluti af staðlaröð á sviði stjórnunarkerfa um upplýsingaöryggi eru sem hér segir:

- ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002*

0.3 Tilgangur þessa alþjóðastaðals

Þessi alþjóðastaðall gefur yfirlit yfir stjórnunarkerfi um upplýsingaöryggi og skilgreinir hugtök sem tengjast þeim.

ATHUGASEMD Í viðauka A er skýrt hvaða orðalagi er beitt til þess að lýsa kröfum og/eða leiðsögn í staðlaröð á sviði stjórnunarkerfa um upplýsingaöryggi.

0 Introduction

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1/SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

0.2 ISMS family of standards

The ISMS family of standards (see Clause 4) is intended to assist organizations of all types and sizes to implement and operate an ISMS and consists of the following International Standards, under the general title *Information technology – Security techniques* (given below in numerical order):

- ISO/IEC 27000, *Information security management systems – Overview and vocabulary*
- ISO/IEC 27001, *Information security management systems – Requirements*
- ISO/IEC 27002, *Code of practice for information security controls*
- ISO/IEC 27003, *Information security management system implementation guidance*
- ISO/IEC 27004, *Information security management – Measurement*
- ISO/IEC 27005, *Information security risk management*
- ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007, *Guidelines for information security management systems auditing*
- ISO/IEC TR 27008, *Guidelines for auditors on information security controls*
- ISO/IEC 27009, *Sector-specific application* of *ISO/IEC 27001 – Requirements*
- ISO/IEC 27010, *Information security management for inter-sector and inter-organizational communications*
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on* ISO/IEC 27002
- ISO/IEC 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
- ISO/IEC 27014, *Governance of information security*
- ISO/IEC TR 27015, *Information security management guidelines for financial services*
- ISO/IEC TR 27016, *Information security management – Organizational economics*
- ISO/IEC 27017, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- ISO/IEC 27018, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- ISO/IEC 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

NOTE The general title "*Information technology – Security techniques*" indicates that these International Standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:
– ISO 27799, *Health informatics – Information security management in health using ISO/IEC 27002*

0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems and defines related terms.

NOTE Annex A provides clarification on how verbal forms are used to express requirements and/or guidance in the ISMS family of standards.

Staðlaröð á sviði stjórnunarkerfa um upplýsingaöryggi felur í sér staðla sem:
a) skilgreina kröfur sem gilda um stjórnunarkerfi um upplýsingaöryggi og þá sem votta slík kerfi;
b) veita beinan stuðning, ítarlega leiðsögn og/eða túlkun á heildarferlinu við að koma á, innleiða, viðhalda og bæta stjórnunarkerfi um upplýsingaöryggi;
c) fjalla um leiðbeiningar fyrir stjórnunarkerfi um upplýsingaöryggi sem beinast að tilteknum geirum; og
d) fjalla um samræmismat fyrir stjórnunarkerfi um upplýsingaöryggi.

Hugtök og skilgreiningar sem kveðið er á um í þessum alþjóðastaðli:
– gera skil algengum hugtökum og skilgreiningum í staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi;
– gera ekki skil öllum hugtökum og skilgreiningum sem notaðar eru í staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi; og
– takmarka ekki að ný hugtök séu skilgreind í staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi.

1 Umfang

Þessi alþjóðastaðall gefur yfirlit yfir stjórnunarkerfi um upplýsingaöryggi og hugtök og skilgreiningar sem oft koma fyrir í staðlaröð á sviði stjórnunarkerfis um upplýsingaöryggi. Þessum alþjóðastaðli má beita á skipulagsheildir af öllum stærðum og gerðum (t.d. viðskiptafyrirtæki, ríkisstofnanir, skipulagsheildir sem ekki eru reknar í hagnaðarskyni).

2 Hugtök og skilgreiningar

Í þessu skjali gilda eftirfarandi hugtök og skilgreiningar.

2.1
aðgangsstýring
leið til þess að tryggja að aðgangur að verðmætum sé heimill og takmarkaður í samræmi við *kröfur* (2.63) vegna rekstrar og öryggis.

2.2
greiningarlíkan
algrím eða útreikningur sem tengir eina eða fleiri *grunnmælibreytur* (2.10) og/eða *afleiddar mælibreytur* (2.22) við tilheyrandi *ákvörðunarviðmið* (2.21)

2.3
árás
tilraun til þess að eyðileggja, gera berskjaldaða, breyta, gera óvirkt, stela eða öðlast óheimilan aðgang að verðmæti eða nota verðmæti án heimildar

2.4
eigind
eiginleiki eða sérkenni *viðfangs* (2.55) sem hægt er að aðgreina megindlega eða eigindlega með mennskum eða sjálfvirkum aðferðum
[HEIMILD: ISO/IEC 15939:2007, með breytingum – „viðfang“ hefur komið í stað „einindis“ í skilgreiningunni.]

2.5
úttekt
kerfisbundið, óháð og skjalfest *ferli* (2.61) til þess að afla úttektargagna og meta þau hlutlægt í því skyni að ákvarða að hve miklu leyti úttektarviðmið eru uppfyllt

Athugasemd 1 við færslu: Úttekt getur verið innri úttekt (fyrsta aðila) eða ytri úttekt (annars aðila eða þriðji aðila) og hún getur verið sameinuð úttekt (þar semsameinuð eru tvö eða fleiri svið).

Athugasemd 2 við færslu: „Úttektargögn“ og „úttektarviðmið“ eru skilgreind í ISO 19011.