ÍST EN ISO/IEC 27002:2017

ÍSLENSKUR STAÐALL

STAÐLARÁÐ ÍSLANDS

Gildistaka 2017-04-20
ICS 29.240.01

Upplýsingatækni
– Öryggisaðferðir
– Starfsvenjur fyrir upplýsingaöryggisstýringar

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 27002:2017

Formáli íslensku þýðingarinnar

Þessi íslenski staðall, ÍST EN ISO/IEC 27002:2013, 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 ÍST ISO/IEC 27002:2005.
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 27002

Febrúar 2017

ICS 03.100.70;35.030

Íslensk útgáfa

Upplýsingatækni – Öryggisaðferðir – Starfsvenjur fyrir upplýsingaöryggisstýringar (ISO/IEC 27002:2013 með Leiðréttingu 1:2014 og Leiðréttingu 2:2015)

Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstecnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Þessi staðall er hin íslenska útgáfa evrópska staðalsins EN ISO/IEC 27002:2017. 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 27002:2017

Formáli evrópska staðalsins

Texti ISO/IEC 27001:2013 að meðtöldum Leiðréttingu 1:2014 og Leiðréttingu 2:2015 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 27002:2017.

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 27002:2013 að meðtöldum Leiðréttingu 1:2014 og Leiðréttingu 2:2015 var samþykktur óbreyttur af CEN sem EN ISO/IEC 27002:2017.

European foreword

The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 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 27002:2017.

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 27002:2013 including Cor 1:2014 and Cor 2:2015 has been approved by CEN as EN ISO/IEC 27002:2017 without any modification.

ÍST EN ISO/IEC 27002:2017

Efnisyfirlit

Contents

ÍST EN ISO/IEC 27002:2017

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.

Alþjóðastaðlar eru samdir í samræmi við Vinnureglur ISO/IEC, 2. hluta.

Alþjóðastaðallinn ISO/IEC 27002 var saminn af sameiginlegu tækninefndinni ISO/IEC JTC 1, *Information technology*, undirnefnd SC 27, *IT Security techniques*.

Athygli er vakin á því að sum atriði í þessu skjali gætu fallið undir einkaleyfi. ISO ber ekki ábyrgð á að tilgreina einstök eða öll slík einkaleyfi.

Þessi önnur útgáfa fellir úr gildi og kemur í stað fyrstu útgáfu (ÍST ISO/IEC 27002:2005), sem hefur verið tæknilega endurskoðuð auk endurskoðunar á uppbyggingu.

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 liasion with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical commitee, ISO/IEC JTC 1.

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

ISO/IEC 27002 was prepared by Joint Technical Commitee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques.*

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

This second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structually revised.

0 Inngangur

0.1 Bakgrunnur og samhengi

Þessi alþjóðastaðall er hannaður svo skipulagsheildir geti notað hann til tilvísunar við val á stýringum þegar verið er að innleiða stjórnunarkerfi um upplýsingaöryggi byggt á ÍST EN ISO/IEC 27001[10] eða sem leiðbeiningarskjal handa skipulagsheildum við innleiðingu á almennt viðurkenndum upplýsingaöryggisstýringum. Staðallinn er einnig ætlaður til notkunar við þróun á leiðbeiningum um stjórnun upplýsingaöryggis sem tekur mið af viðkomandi atvinnugrein eða skipulagsheild með hliðsjón af öryggisáhættuumhverfi þeirra.

Skipulagsheildir af öllum stærðum og gerðum (þ.m.t. opinber fyrirtæki, einkafyrirtæki, fyrirtæki rekin í hagnaðarskyni og fyrirtæki sem ekki eru rekin í hagnaðarskyni) safna, vinna, geyma og senda upplýsingar á margs konar formi, þar með talið rafrænt, raunlægt og munnlega (t.d. samtöl og kynningar).

Upplýsingar hafa ekki bara gildi þegar þær eru skriflegar, tölulegar eða í formi mynda; þekking, hugtök, hugmyndir og vörumerki eru dæmi um óefnislegar upplýsingar. Í samtengdum heimi eru upplýsingar og ferli sem tengjast þeim; kerfi, net og starfsfólk sem kemur að rekstri, meðhöndlun og verndun þeirra, verðmæti sem eins og aðrar mikilvægar rekstrareignir hafa virði fyrir rekstur skipulagsheildarinnar og verðskulda því eða þarfnast verndunar gegn háska af ýmsu tagi.

Að verðmætum geta bæði steðjað ógnir af ásetningi og fyrir slysni þar sem ferli sem tengjast þeim, kerfi, net og fólk býr yfir eðlislægum veilum. Breytingar á rekstrarferlum og -kerfum og aðrar ytri breytingar (s.s. ný lög og reglugerðir) geta skapað nýja upplýsingaöryggisáhættu. Í ljósi þess með hve margvíslegum hætti ógnir gætu nýtt veikleika til þess að skaða skipulagsheildina er upplýsingaöryggisáhætta ávallt fyrir hendi. Markvirkt upplýsingaöryggi dregur úr þessari áhættu með því að vernda skipulagsheildina gegn ógnum og veilum og dregur einnig úr áhrifum sem verðmæti þess gætu orðið fyrir.

Upplýsingaöryggi næst með því að innleiða viðeigandi stýringar, þ. á m. stefnur, ferli, verklagsreglur, skipurit og hugbúnaðar- og vélbúnaðaraðgerðir. Þessum stýringum þarf að koma upp og innleiða þær, vakta, rýna og bæta eftir þörfum til þess að tryggja að öryggis- og rekstrarmarkmið skipulagsheildarinnar séu uppfyllt. Upplýsingaöryggisstefna eins og sú stefna sem sett er fram í ÍST EN ISO/IEC 27001[10] gefur heildræna og samræmda sýn á upplýsingaöryggisáhættu skipulagsheildarinnar svo innleiða megi heildstæða röð upplýsingaöryggisstýringa innan heildarramma samfellds stjórnunarkerfis.

Mörg upplýsingakerfi hafa ekki verið hönnuð til þess að vera örugg í sama skilningi og er að finna í ÍST EN ISO/IEC 27001[10] og þessum staðli. Öryggið sem hægt er að ná fram með tæknilegum aðferðum er takmarkað og ætti því að styðja við það með viðeigandi stjórnun og verklagsreglum. Vandlegrar skipulagningar og nákvæmni er þörf til þess að skera úr um það hvaða stýringar ættu að vera fyrir hendi. Vel heppnað stjórnunarkerfi um upplýsingaöryggi krefst stuðnings allra starfsmanna skipulagsheildarinnar. Einnig kann að vera þörf á þátttöku hluthafa, birgja eða annarra utanaðkomandi aðila. Enn fremur kann að vera þörf á sérfræðiráðgjöf frá utanaðkomandi aðilum.

Almennt séð veitir markvirkt upplýsingaöryggi stjórnendum og öðrum hagsmunaaðilum einnig vissu fyrir því að verðmæti skipulagsheildarinnar séu nokkuð örugg og vernduð gegn skaða sem gerir reksturinn greiðari.

0.2 Upplýsingaöryggiskröfur

Nauðsynlegt er að skipulagsheild beri kennsl á öryggiskröfur sínar. Öryggiskröfur eru flokkaðar í þrjá meginflokka eftir uppruna:

a) mat á áhættu sem steðjað getur að skipulagsheildinni, að teknu tilliti til markmiða hennar og heildaráætlunar um rekstur. Með áhættumati eru greindar þær ógnir sem steðja að verðmætum, mat lagt á veilur og líkurnar á því að þær eigi sér stað og hugsanleg áhrif þeirra metin;
b) kröfur laga, stjórnvaldsreglna og samninga sem skipulagsheild, viðskiptaaðilar hennar, verktakar og þjónustuveitendur verða að uppfylla sem og félagsmenningarlegt umhverfi þeirra;
c) meginreglur, markmið og rekstrarkröfur sem gilda um meðhöndlun, vinnslu, geymslu, miðlun og safnvistun upplýsinga sem skipulagsheild hefur þróað til þess að styðja við starfsemi sína.

Nauðsynlegt er að vega og meta auðlindir sem beitt er við innleiðingu stýringa á móti rekstrarskaða vegna öryggismála sem líklegur væri ef stýringarnar væru ekki fyrir hendi. Niðurstöður áhættumats munu hjálpa til við að leiða og ákvarða viðeigandi aðgerðir og forgangsröðun stjórnenda við stjórnun á áhættu vegna upplýsingaöryggis og innleiðingu á stýringum sem hafa verið valdar til þess að verjast slíkri áhættu.

0 Introduction

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

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. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. 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. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

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

a) the assessment of 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;
b) 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;
c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005[11] veitir leiðsögn um stjórnun upplýsingaöryggisáhættu, þ.m.t. ráðgjöf um áhættumat, áhættumeðferð, áhættusamþykki, upplýsingamiðlun um áhættu, áhættuvöktun og áhætturýni.

0.3 Val á stýringum

Stýringar er hægt að velja úr þessum staðli eða öðrum stýringasöfnum eða hanna nýjar stýringar til að mæta sérþörfum ef það á við.

Val á stýringum er háð ákvörðunum í skipulagsheildinni, byggðum á viðmiðum fyrir áhættusamþykki, valkostum um áhættumeðferð og almennri nálgun við áhættustjórnun sem skipulagsheildin beitir og ætti einnig að falla undir öll viðeigandi innlend og alþjóðleg lög og reglugerðir. Val á stýringum veltur einnig á því hvernig samspil stýringa er þegar ítrasta vörn er veitt.

Líta má á sumar stýringarnar í þessum staðli sem leiðbeinandi meginreglur um stjórnun upplýsingaöryggis sem eigi því við um flestar skipulagsheildir. Stýringarnar eru útskýrðar nánar hér á eftir ásamt leiðbeiningum um innleiðingu. Frekari upplýsingar um val á stýringum og aðra valkosti um áhættumeðferð er að finna í ISO/IEC 27005.[11]

0.4 Þróun eigin leiðbeininga

Líta má á þennan alþjóðastaðal sem upphafsreit fyrir þróun sértækra leiðbeininga fyrir skipulagsheild. Ekki er víst að allar stýringar og leiðsögn í þessum starfsvenjum eigi við. Enn fremur kann að vera þörf fyrir viðbótarstýringar og -leiðbeiningar sem ekki er getið um í þessum staðli. Við þróun skjala með viðbótarleiðbeiningum og -stýringum getur verið gagnlegt, þar sem við á, að fella inn í þau tilvísanir í greinar í þessum staðli, til þess að auðvelda úttektarmönnum og viðskiptaaðilum að kanna hlítingu.

0.5 Athugunarefni varðandi lífsferil

Upplýsingar eiga sér náttúrulegan lífsferil, allt frá því þær eru skapaðar og myndast, í gegnum geymslu, vinnslu, notkun og sendingu og þar til þær eru að endingu eyðilagðar eða eyðast. Virði verðmæta eða aðsteðjandi hættur kunna að taka breytingum á meðan á lífsferli þeirra stendur (t.d. hefur óheimil uppljóstrun eða þjófnaður á fjárhagsreikningum fyrirtækis mun minni þýðingu eftir að þær hafa verið birtar formlega) en upplýsingaöryggi er þó jafnan mikilvægt í tilteknum mæli á öllum stigum.

Upplýsingakerfi eiga sér lífsferla sem spanna tímann allt frá því þau eru hugsuð upp, sett fram, hönnuð, þróuð, prófuð, innleidd, notuð og þeim viðhaldið og þar til þau eru loks tekin úr notkun og þeim fargað. Taka ætti mið af upplýsingaöryggi á sérhverju þessara stiga. Nýjungar í kerfisþróun og breytingar á fyrirliggjandi kerfum skapa tækifæri fyrir skipulagsheildir til þess að uppfæra og bæta öryggisstýringar með hliðsjón af raunverulegum atvikum og núverandi og fyrirséðum upplýsingaöryggisáhættum.

0.6 Tengdir staðlar

Þessi staðall veitir leiðbeiningar um breitt svið upplýsingaöryggisstýringa sem algengt er að beita í margvíslegum skipulagsheildum, en hinir staðlarnir í ISO/IEC 27000 staðlasamstæðunni láta í té viðbótarráðgjöf eða kröfur til fyllingar fyrir aðra þætti heildarferlisins fyrir stjórnun upplýsingaöryggis.

Vísað er til ÍST EN ISO/IEC 27000 fyrir almenna kynningu á bæði stjórnunarkerfi um upplýsingaöryggi og staðlasamstæðunni. ÍST EN ISO/IEC 27000 lætur í té orðalista með formlegum skilgreiningum á flestum hugtökum sem notuð eru í ISO/IEC 27000 staðlasamstæðunni og lýsir umfangi og markmiðum hvers staðals innan samstæðunnar.

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

0.3 Selecting controls

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 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. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.[11]

0.4 Developing your own guidelines

This International Standard 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.

0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

Upplýsingatækni – Öryggisaðferðir – Starfsvenjur fyrir stjórnun upplýsingaöryggis

1 Umfang

Þessi alþjóðastaðall veitir leiðbeiningar um upplýsingaöryggisstaðla skipulagsheilda og starfsvenjur í stjórnun upplýsingaöryggis, þ.m.t. val, innleiðingu og stjórnun stýringa, og tekur mið af upplýsingaöryggisáhættuumhverfi skipulagsheildarinnar.

Þessi alþjóðastaðall er hannaður til notkunar af skipulagsheildum sem ætla að:
a) velja stýringar í innleiðingarferli á stjórnunarkerfi um upplýsingaöryggi sem byggt er á ÍST EN ISO/IEC 27001;[10]
b) innleiða almennt viðurkenndar upplýsingaöryggisstýringar;
c) þróa eigin leiðbeiningar um upplýsingaöryggisstjórnun.

2 Tilvísanir í staðla

Vísað er til eftirfarandi skjala, í heild eða að hluta, í þessu skjali og eru þau ómissandi við notkun þess. Að því er varðar dagsettar tilvísanir á aðeins sú útgáfa sem vísað er í við. Ef tilvísanir eru ódagsettar vísa þær til nýjustu útgáfu viðkomandi skjals (ásamt öllum breytingum).

ÍST EN ISO/IEC 27000, Upplýsingatækni – Öryggistækni – Stjórnunarkerfi um upplýsingaöryggi – Yfirlit og orðaforði

3 Hugtök og skilgreiningar

Í þessu skjali gilda hugtök og skilgreiningar ÍST EN ISO/IEC 27000.

4 Skipulag þessa staðals

Í þessum staðli eru 14 greinar um öryggisstýringu sem sameiginlega innihalda samtals 35 meginflokka öryggis og 114 stýringar.

4.1 Greinar

Í hverri grein sem skilgreinir öryggisstýringu er að finna einn eða fleiri meginöryggisflokka.

Röð greinanna í þessum staðli endurspeglar ekki mikilvægi þeirra. Öryggisstýringar í einni eða öllum greinanna geta verið mikilvægar, allt eftir aðstæðum, og því ætti hver sú skipulagsheild sem notar þennan staðal að tilgreina hvaða stýringar koma að notum, hversu mikilvægar þær eru, sem og notkun þeirra í einstökum rekstrarferlum. Enn fremur er atriðum ekki raðað í forgangsröð í listum í þessum staðli.

4.2 Flokkar stýringa

Í hverjum meginöryggisstýringarflokki eru:
a) stýringarmarkmið þar sem fram kemur að hverju er stefnt;
b) ein eða fleiri stýringar sem unnt er að beita til þess að ná stýringarmarkmiðinu.

Lýsingar á stýringum eru byggðar upp sem hér segir:

Stýring
Skilgreind er tiltekin stýringaryfirlýsing, til þess að uppfylla stýringarmarkmiðið.

Leiðsögn um innleiðingu
Veittar eru nákvæmari upplýsingar til þess að styðja innleiðingu stýringarinnar og ná stýringarmarkmiðinu. Verið getur að hluti þessarar leiðsagnar eigi ekki við eða sé ekki fullnægjandi í öllum tilvikum og mögulegt að hún uppfylli ekki sértækar stýringarkröfur skipulagsheildarinnar.