ÍST ISO/IEC 27001:2005

ÍSLENSKUR STAÐALL

STAÐLARÁÐ ÍSLANDS

Gildistaka: 2006-07-15
ICS: 35.040

Upplýsingatækni - Öryggistækni - Stjórnkerfi upplýsingaöryggis - Kröfur

IInformation technology - Security techniques - Information security management systems - Requirements

Staðfestur af Staðlaráði Íslands

Sýnishorn

2. prentun.

Formáli íslensku þýðingarinnar

Þessi íslenski staðall, ÍST ISO/IEC 27001:2005, sem einnig er 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 FUT.

Vinnuhópur á vegum Fagstaðlaráðs í upplýsingatækni (FUT), sem starfar á vegum Staðlaráðs Íslands, vann að þýðingu staðalsins og fá meðlimir vinnuhópsins þakkir fyrir vinnu við yfirlestur og ráðgjöf.

Vinnuhópinn skipuðu:

Marinó G. Njálsson
Jónas Sturla Sverrisson
Elías Atlason
Kristín Þórsdóttir
Sigurjón Þór Árnason
Þorvarður Kári Ólafsson
Guðbjörg Björnsdóttir (Staðlaráði/FUT)
Stefán Briem (þýðandi)

Þessi staðall kemur í stað staðalsins ÍST BS 7799-2:2002.

Þýðingin er einungis gerð til hagræðis fyrir íslenska notendur. Kappkostað hefur verið að hafa íslenska textann eins nákvæman 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 íslenska þýðingin. Notendur staðlanna eru eindregið hvattir til að koma athugasemdum og ábendingum til Staðlaráðs Íslands.

Vinnuhópurinn taldi rétt að gefa skýringu á notkun hugtaksins „organization" sem þýtt er með orðinu „fyrirtæki".

Þessi notkun orðsins er viðtekin í öðrum stöðlum (t.d. ÍST EN ISO 9000:2005) og hefur hlotið góðan hljómgrunn. Með „fyrirtæki" er átt við t.d. félag, hlutafélag, firma, atvinnufyrirtæki, stofnun, góðgerðastofnun, einyrkja, samtök eða hluta eða samsetningu af þessu. Fyrirtæki getur verið opinbert eða í einkaeign.

ÍST ISO/IEC 27001:2005

Efnisyfirlit

Contents

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.

Meginverkefni sameiginlegu tækninefndarinnar er að semja alþjóðastaðla. Frumvörp að alþjóðastöðlum, sem sameiginlega tækninefndin hefur komið sér saman um, eru send aðilum samtakanna til atkvæðagreiðslu. Alþjóðastaðall er ekki gefinn út nema að minnsta kosti 75 % þeirra aðila sem greiða atkvæði hafi samþykkt staðalinn.

Athygli er vakin á því að sum atriði í þessu skjali gætu fallið undir einkaleyfi. ISO og IEC bera ekki ábyrgð á að tilgreina einhver eða öll slík einkaleyfi.

Alþjóðastaðallinn ISO/IEC 27001 var saminn af sameiginlegu tækninefndinni ISO/IEC JTC 1, Information technology, undirnefnd SC 27, IT Security techniques.

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 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

0 Inngangur

0.1 Almennt

Þessi alþjóðastaðall var saminn til þess að láta í té líkan til að koma upp, innleiða, starfrækja, vakta, rýna, viðhalda og endurbæta stjórnkerfi upplýsingaöryggis. Það ætti að vera stefnumarkandi ákvörðun fyrir fyrirtæki að taka upp upplýsingaöryggisstjórnkerfi. Þarfir og markmið, öryggiskröfur, þau ferli sem beitt er, sem og stærð fyrirtækis og formgerð hafa áhrif á hönnun og innleiðingu upplýsingaöryggisstjórnkerfis í fyrirtækinu. Búist er við að þessi atriði og stuðningskerfi þeirra taki breytingum með tímanum. Gert er ráð fyrir að við innleiðingu á upplýsingaöryggisstjórnkerfi verði umfang þess í samræmi við þarfir fyrirtækisins, t.d. að einföld staða kalli á einfalda upplýsingaöryggisstjórnkerfislausn.

Þennan alþjóðastaðal geta hagsmunaaðilar innan og utan fyrirtækisins notað til þess að meta samræmi.

0.2 Ferlisnálgun

Í þessum alþjóðastaðli er tekin upp ferlisnálgun við stofnun, innleiðingu, rekstur, vöktun, rýni, viðhald og umbætur á upplýsingaöryggisstjórnkerfi í fyrirtæki.

Til þess að fyrirtæki geti starfað með virkum hætti þarf að bera kennsl á og stjórna fjölmörgum athöfnum. Alla starfsemi sem nýtir auðlindir og er stjórnað til að auðvelda breytingu ílags í frálag má líta á sem ferli. Oft myndar frálag eins ferlis með beinum hætti ílag hins næsta.

Þá aðferð að beita kerfi ferla innan fyrirtækis ásamt því að bera kennsl á ferlin og samspil þeirra og stjórna þeim má nefna „ferlisnálgun“.

Sú ferlisnálgun fyrir stjórnun upplýsingaöryggis sem kynnt er í þessum alþjóðastaðli hvetur beitendur hennar til að leggja áherslu á mikilvægi eftirfarandi atriða:

a) að skilja kröfur fyrirtækis um upplýsingaöryggi og þörfina á að setja fram stefnu og markmið fyrir upplýsingaöryggi;

b) að innleiða stýringar og beita þeim til þess að stjórna upplýsingaöryggisáhættu fyrirtækis þegar um er að ræða rekstraráhættu í fyrirtækinu öllu;

c) að vakta og rýna frammistöðu og skilvirkni upplýsingaöryggisstjórnkerfisins; og

d) stöðugra umbóta á grundvelli hlutlægra mælinga.

0 Introduction

0.1 General

This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

This International Standard can be used in order to assess conformance by interested internal and external parties.

0.2 Process approach

This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a) understanding an organization's information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;

c) monitoring and reviewing the performance and effectiveness of the ISMS; and

d) continual improvement based on objective measurement.

Í þessum alþjóðastaðli er tekið upp ferlislíkan, sem þekkt er undir enska heitinu „Plan-Do-Check-Act" (PDCA). Það er notað til að byggja upp öll upplýsingaöryggisstjórnkerfisferli. Á mynd 1 er sýnt hvernig upplýsingaöryggisstjórnkerfi tekur sem ilag kröfur um upplýsingaöryggi og væntingar hagsmunaaðila og að loknum nauðsynlegum aðgerðum og ferlum skilar af sér upplýsingaöryggi sem frálagi (þ.e. stjórnuðu upplýsingaöryggi) sem uppfyllir þessar kröfur og væntingar. Á mynd 1 eru einnig sýnd tengsl ferlanna sem eru kynnt í greinum 4, 5, 6, 7 og 8.

Með því að taka upp PDCA-líkanið endurspeglast einnig þær meginreglur eins og þær eru settar fram í OECD Guidelines (2002)[1)] sem kveða á um öryggi í upplýsingakerfum og -netum. Þessi alþjóðastaðall veitir traust líkan fyrir innleiðingu á þeim meginreglum þessara OECD-leiðbeininga sem kveða á um áhættumat, hönnun og innleiðingu öryggis, öryggisstjórnun og endurmat öryggis.

DÆMI 1
Krafa gæti verið um að brot á upplýsingaöryggi valdi fyrirtæki ekki alvarlegum fjárhagsskaða og/eða hneisu.

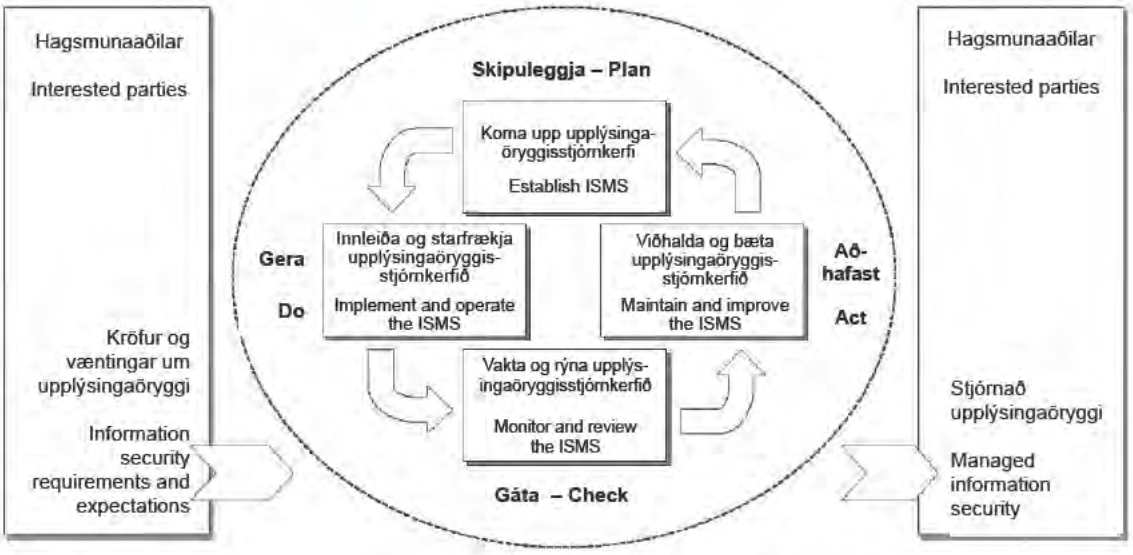
DÆMI 2
Þær væntingar gætu verið gerðar að ef alvarlegt atvik kemur upp – svo sem innbrot á rafrænan viðskiptavef fyrirtækis – þá sé tiltækt fólk með nægilega þjálfun í viðeigandi verklagsreglum til að lágmarka áhrifin.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6, 7 and 8.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002)[1)] governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

EXAMPLE 1
A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2
An expectation might be that if a serious incident occurs – perhaps hacking of an organization's eBusiness web site – there should be people with sufficient training in appropriate procedures to minimize the impact.



Mynd 1 – PDCA-líkani beitt á upplýsingaöryggisstjórnkerfisferli – Figure 1 – PDCA model applied to ISMS processes

[1)] OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[1)] OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org