SVENSK STANDARD
SS-ISO/IEC 27001:2014

Fastställd/Approved: 2014-02-26
Publicerad/Published: 2014-02-27
Utgåva/Edition: 2
Språk/Language: svenska/Swedish; engelska/English
ICS: 01.140.30; 04.050; 33.040.40; 35.020; 35.040; 35.080

Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav
(ISO/IEC 27001:2013, IDT)

Information technology – Security techniques – Information security management systems – Requirements
(ISO/IEC 27001:2013, IDT)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Den internationella standarden ISO/IEC 27001:2013 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO/IEC 27001:2013 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-ISO/IEC 27001:2006 utgåva 1.

The International Standard ISO/IEC 27001:2013 has the status of a Swedish Standard. This document contains the Swedish language version of ISO/IEC 27001:2013 followed by the official English version.

This standard supersedes the Swedish Standard SS-ISO/IEC 27001:2006, edition 1.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Standarden är framtagen av kommittén för Informationssäkerhet, SIS/TK 318.

Innehåll

Sida

Förord ... **iii**
0 Orientering ... **iv**
0.1 Allmänt ... **iv**
0.2 Kompatibilitet med andra ledningssystemstandarder ... **iv**
1 Omfattning ... **1**
2 Normativa hänvisningar ... **1**
3 Termer och definitioner ... **1**
4 Organisationens förutsättningar ... **1**
4.1 Att förstå organisationen och dess förutsättningar ... **1**
4.2 Att förstå intressenters behov och förväntningar ... **1**
4.3 Att bestämma ledningssystemets omfattning ... **1**
4.4 Ledningssystem för informationssäkerhet ... **2**
5 Ledarskap ... **2**
5.1 Ledarskap och engagemang ... **2**
5.2 Policy ... **2**
5.3 Befattningar, ansvar och befogenheter inom organisationen ... **3**
6 Planering ... **3**
6.1 Åtgärder för att hantera risker och möjligheter ... **3**
6.2 Informationssäkerhetsmål och planering för att uppnå dem ... **5**
7 Stöd ... **5**
7.1 Resurser ... **5**
7.2 Kompetens ... **5**
7.3 Medvetenhet ... **5**
7.4 Kommunikation ... **6**
7.5 Dokumenterad information ... **6**
8 Verksamhet ... **7**
8.1 Planering och styrning av verksamheten ... **7**
8.2 Bedömning av informationssäkerhetsrisker ... **7**
8.3 Behandling av informationssäkerhetsrisker ... **7**
9 Utvärdering av prestanda ... **7**
9.1 Övervakning, mätning, analys och utvärdering ... **7**
9.2 Internrevision ... **8**
9.3 Ledningens genomgång ... **8**
10 Förbättringar ... **9**
10.1 Avvikelse och korrigerande åtgärd ... **9**
10.2 Ständig förbättring ... **9**
Bilaga A (normativ) Åtgärdsmål och säkerhetsåtgärder ... **10**
Litteraturförteckning ... **23**

Förord

ISO (Internationella Standardiseringsorganisationen) är en världsomspännande sammanslutning av nationella standardiseringsorgan (ISO-medlemmar). Utarbetandet av internationella standarder sker normalt i ISOs tekniska kommittéer. Varje medlemsland som är intresserat av arbetet i en teknisk kommitté har rätt att bli medlem i den. Internationella organisationer, statliga såväl som icke-statliga, som samarbetar med ISO deltar också i arbetet. ISO har nära samarbete med International Electrotechnical Commission (IEC) i alla frågor rörande elektroteknisk standardisering.

Internationella standarder utarbetas i enlighet med ISO/IEC direktiven, del 2.

Huvuduppgiften för de tekniska kommittéerna är att utarbeta internationella standarder. Förslag till internationella standarder som godkänts av de tekniska kommittéerna sänds till medlemsländerna för röstning. För publicering av en internationell standard krävs att minst 75 % av de röstande medlemsländerna godkänner förslaget.

Det bör uppmärksammas att vissa beståndsdelar i denna internationella standard möjligen kan vara föremål för patenträtter. ISO ska inte hållas ansvarig för att identifiera någon eller alla sådana patenträtter.

SS-ISO/IEC 27001 har tagits fram av den gemensamma tekniska kommittén ISO/IEC JTC 1, Informationsteknologi, underkommitté SC 27, IT-säkerhetstekniker.

Denna andra upplaga utgåvan och ersätter den första utgåvan (SS-ISO/IEC 27001:2006), efter teknisk revidering.

0 Orientering

0.1 Allmänt

Denna standard har tagits fram för att tillhandahålla krav för att upprätta, införa, underhålla och ständigt förbättra ett ledningssystem för informationssäkerhet. Antagandet av ett ledningssystem för informationssäkerhet är ett strategiskt beslut för en organisation. Upprättandet och införandet av en organisations ledningssystem för informationssäkerhet påverkas av organisationens behov och mål, säkerhetskrav, de organisatoriska processer som används och organisationens storlek och struktur. Alla dessa påverkande faktorer kan komma att förändras över tiden.

Ledningssystemet för informationssäkerhet bevarar informationens konfidentialitet, riktighet och tillgänglighet genom att tillämpa en riskhanteringsprocess och ger förtroende för berörda parter att risker hanteras på ett adekvat sätt.

Det är viktigt att ledningssystemet för informationssäkerhet är en integrerad del av organisationens processer och övergripande ledningsstruktur och att informationssäkerhet beaktas i utformningen av processer, informationssystem och säkerhetsåtgärder. Det förväntas att ett införande av ett ledningssystem för informationssäkerhet sker i en omfattning som anpassas till organisationens behov.

Denna standard kan användas internt och av externa parter för att bedöma organisationens förmåga att uppfylla organisationens egna informationssäkerhetskrav.

Den ordning i vilken kraven presenteras i denna standard syftar inte till att återspegla deras betydelse och antyder heller inte den ordning i vilken de ska genomföras. De redovisade kraven numreras enbart i hänvisningssyfte.

SS-ISO/IEC 27000 beskriver en översikt av och vokabulär för ledningssystem för informationssäkerhet, med referens till standardserien som relaterar till ledningssystem för informationssäkerhet (inklusive SS-ISO/IEC 27003 [2], SS-ISO/IEC 27004 [3] och SS-ISO/IEC 27005 [4]), med relaterade termer och definitioner.

0.2 Kompatibilitet med andra ledningssystemstandarder

Denna standard tillämpar högnivåstruktur, identiska titlar på underavsnitt, identisk text, vanliga termer och grundbegrepp som de definierats i bilaga SL av del 1 av ISO/IEC direktiven, konsoliderade ISO-tillägg, och är därför kompatibel med andra ledningssystemstandarder som har antagit bilaga SL.

Detta gemensamma angreppssätt, som definierats i bilaga SL, kommer att vara användbart för de organisationer som väljer att använda ett enda ledningssystem som uppfyller kraven i två eller flera ledningssystemstandarder.

Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav

1 Omfattning

Denna standard specificerar kraven för upprättande, införande, underhåll och ständig förbättring av ett ledningssystem för informationssäkerhet inom ramarna för organisationen. Denna standard innehåller också krav på bedömning och behandling av informationssäkerhetsrisker, anpassat till organisationens behov. Kraven som anges i denna standard är generiska och är avsedda att vara tillämpliga i alla organisationer, oavsett typ, storlek och slag. Att undanta något av kraven specificerade i avsnitt 4 till 10 är inte acceptabelt när en organisation avser efterleva denna standard.

2 Normativa hänvisningar

Detta dokument hänvisar till följande dokument som är nödvändiga när detta dokument ska tillämpas. För daterade hänvisningar gäller endast den utgåva som anges. För odaterade hänvisningar gäller senaste utgåvan av dokumentet (inklusive alla tillägg).

SS-ISO/IEC 27000, *Informationsteknologi — Säkerhetstekniker — Ledningssystem för informationssäkerhet — Översikt och terminologi*

Contents

Page

Foreword ... **iv**

0 Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Context of the organization ... **1**
4.1 Understanding the organization and its context ... 1
4.2 Understanding the needs and expectations of interested parties ... 1
4.3 Determining the scope of the information security management system ... 1
4.4 Information security management system ... 2

5 Leadership ... **2**
5.1 Leadership and commitment ... 2
5.2 Policy ... 2
5.3 Organizational roles, responsibilities and authorities ... 3

6 Planning ... **3**
6.1 Actions to address risks and opportunities ... 3
6.2 Information security objectives and planning to achieve them ... 5

7 Support ... **5**
7.1 Resources ... 5
7.2 Competence ... 5
7.3 Awareness ... 5
7.4 Communication ... 6
7.5 Documented information ... 6

8 Operation ... **7**
8.1 Operational planning and control ... 7
8.2 Information security risk assessment ... 7
8.3 Information security risk treatment ... 7

9 Performance evaluation ... **7**
9.1 Monitoring, measurement, analysis and evaluation ... 7
9.2 Internal audit ... 8
9.3 Management review ... 8

10 Improvement ... **9**
10.1 Nonconformity and corrective action ... 9
10.2 Continual improvement ... 9

Annex A (normative) **Reference control objectives and controls** ... **10**

Bibliography ... **23**

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*.

This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been technically revised.

0 Introduction

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Information technology — Security techniques — Information security management systems — Requirements

1 Scope

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*