SVENSK STANDARD
SS-ISO/IEC 27001:2006

Fastställd/Approved: 2006-01-19
Rättad och omtryckt/Corrected and reprinted: september 2007
Utgåva/Edition: 1
Språk/Language: engelska/English; svenska/Swedish
ICS: 01.140.30; 04.050; 03.120.10; 33.040.40 ; 35.020; 35.040; 35.080

Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2005, IDT)

Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2005, IDT)

SWEDISH STANDARDS INSTITUTE

Hitta rätt produkt och ett leveranssätt som passar dig

Standarder
Genom att följa gällande standard både effektiviserar och säkrar du ditt arbete. Många standarder ingår dessutom ofta i paket.

Tjänster
Abonnemang är tjänsten där vi uppdaterar dig med aktuella standarder när förändringar sker på dem du valt att abonnera på. På så sätt är du säker på att du alltid arbetar efter rätt utgåva.
e-nav är vår online-tjänst som ger dig och dina kollegor tillgång till standarder ni valt att abonnera på dygnet runt. Med e-nav kan samma standard användas av flera personer samtidigt.

Leveranssätt
Du väljer hur du vill ha dina standarder levererade. Vi kan erbjuda dig dem på papper och som pdf.

Andra produkter
Vi har böcker som underlättar arbetet att följa en standard. Med våra böcker får du ökad förståelse för hur standarder ska följas och vilka fördelar den ger dig i ditt arbete. Vi tar fram många egna publikationer och fungerar även som återförsäljare. Det gör att du hos oss kan hitta över 500 unika titlar. **Vi har även tekniska rapporter, specifikationer och "workshop agreement".**
Matriser är en översikt på standarder och handböcker som bör läsas tillsammans. De finns på sis.se och ger dig en bra bild över hur olika produkter hör ihop.

Standardiseringsprojekt
Du kan påverka innehållet i framtida standarder genom att delta i någon av SIS ca 400 Tekniska Kommittéer.

Find the right product and the type of delivery that suits you

Standards
By complying with current standards, you can make your work more efficient and ensure reliability. Also, several of the standards are often supplied in packages.

Services
Subscription is the service that keeps you up to date with current standards when changes occur in the ones you have chosen to subscribe to. This ensures that you are always working with the right edition.
e-nav is our online service that gives you and your colleagues access to the standards you subscribe to 24 hours a day. With e-nav, the same standards can be used by several people at once.

Type of delivery
You choose how you want your standards delivered. We can supply them both on paper and as PDF files.

Other products
We have books that facilitate standards compliance. They make it easier to understand how compliance works and how this benefits you in your operation. We produce many publications of our own, and also act as retailers. This means that we have more than 500 unique titles for you to choose from. We also have technical reports, specifications and workshop agreements.
Matrices, listed at sis.se, provide an overview of which publications belong together.

Standardisation project
You can influence the content of future standards by taking part in one or other of SIS's 400 or so Technical Committees.

Den internationella standarden ISO/IEC 27001:2005 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO/IEC 27001:2005 med svensk översättning.

Denna standard ersätter SS 62 77 99-2, utgåva 2.

Standarden är rättad och omtryckt 2007 med avseende på den svenska översättningen.

Vid tolkning av kraven i standarden har den engelska texten tolkningsföreträde.

The International Standard ISO/IEC 27001:2005 has the status of a Swedish Standard. This document contains the official English version of ISO/IEC 27001:2005 with a Swedish translation.

This standard supersedes the Swedish Standard SS 62 77 99-2, edition 2.

The standard was corrected and reprinted in 2007 with respect to the Swedish translation.

The English text has priority for interpretation of the requirements in the standard.

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), tel +46 8 555 520 00.
Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

SIS Förlag AB, SE 118 80 Stockholm, Sweden. Tel: +46 8 555 523 10. Fax: +46 8 555 523 11.
E-mail: sis.sales@sis.se Internet: www.sis.se

Contents

Page

Innehåll

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*.

Förord

ISO (International Organization for Standardization) och IEC (International Electrotechnical Commission) utgör det specialiserade systemet för internationell standardisering. Nationella organ som är medlemmar i ISO eller IEC deltar i utvecklingen av internationella standarder genom medverkan i tekniska kommittéer inom respektive organisationer med uppgift att behandla avgränsade tekniska områden. De tekniska kommittéerna inom ISO och IEC samarbetar inom områden av gemensamt intresse. Andra internationella organisationer, statliga eller privata, som samarbetar med ISO och IEC, deltar också i arbetet. Inom området informationsteknik har ISO och IEC bildat en gemensam teknisk kommitté, ISO/IEC JTC 1.

Internationella standarder utformas i enlighet med de regler som anges i ISO/IEC Directives, Part 2.

Den gemensamma tekniska kommitténs främsta uppgift är att utarbeta internationella standarder. Förslag till internationell standard som antagits av den gemensamma tekniska kommittén sänds till medlemmarna för omröstning. Publicering som internationell standard kräver godkännande av minst 75 % av röstande medlemmar.

Det bör framhållas att vissa delar av detta dokument kan omfattas av patenträtter. ISO och IEC frånsäger sig ansvaret för att identifiera några eller alla sådana patenträtter.

ISO/IEC 27001 utformades av Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Sub-Committee SC 27, *IT Security techniques*.

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.

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.

---

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

0 Orientering

0.1 Allmänt

Denna standard har utformats för att tillhandahålla en modell för att upprätta, införa, driva, övervaka, granska, underhålla och förbättra ett ledningssystem för informationssäkerhet (LIS). Att införa ett LIS bör vara ett strategiskt beslut för en organisation. Utformningen och införandet av en organisations LIS påverkas av organisationens behov och mål, av säkerhetskrav, av de processer som tillämpas samt av organisationens storlek och struktur. Dessa faktorer och de stödsystem som finns kan förväntas ändras med tiden. Det förväntas att omfattningen av en LIS-tillämpning anpassas till organisationens behov, dvs. en enkel situation kräver en enkel lösning.

Denna standard kan tillämpas av interna och externa intressenter för att bedöma efterlevnaden.

0.2 Processinriktning

I denna standard tillämpas processinriktning för att upprätta, införa, driva, övervaka, granska, underhålla och förbättra en organisations LIS.

För att en organisation ska fungera verkningsfullt behöver den identifiera och styra många aktiviteter. En aktivitet som använder resurser och som styrs för att göra det möjligt att omforma insatser till utfall kan anses vara en process. Ofta utgör utfallet från en process direkt insatsen till nästa process.

Tillämpningen av ett system av processer inom en organisation tillsammans med identifieringen av och samspelet mellan dessa processer, samt styrningen av dem, kan betecknas som "processinriktning".

Processinriktningen gällande styrning av informationssäkerhet, som beskrivs i denna standard, uppmanar dess användare att betona betydelsen av:

a) förståelse för organisationens krav på informationssäkerhet samt behovet av att upprätta policy och mål för informationssäkerhet

b) införande och drift av säkerhetsåtgärder för att hantera en organisations informationssäkerhetsrisker inom ramen för organisationens övergripande verksamhetsrisker

c) övervakning och granskning av LIS prestanda och verkan

d) ständig förbättring baserad på objektiv mätning.

I denna standard används PDCA-modellen (”Plan-Do-Check-Act”) för att strukturera alla processer för LIS. Figur 1 visar hur ett LIS tar intressenternas informationssäkerhetskrav och förväntningar som insats och genom de nödvändiga åtgärderna och processerna skapar utfall i form av informationssäkerhet som uppfyller kraven och förväntningarna. Figur 1 visar även sambanden mellan processerna så som de anges i avsnitten 4, 5, 6, 7 och 8.

Tillämpningen av PDCA-modellen speglar också de principer som anges i OECD Guidelines (2002) [1)] gällande styrning av säkerheten i informationssystem och nätverk. Denna standard erbjuder en hållbar modell för att införa principerna i riktlinjerna som gäller riskbedömning, utformning och införande av säkerhet, styrning av säkerhet samt förnyad bedömning av säkerhet.

---

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

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.

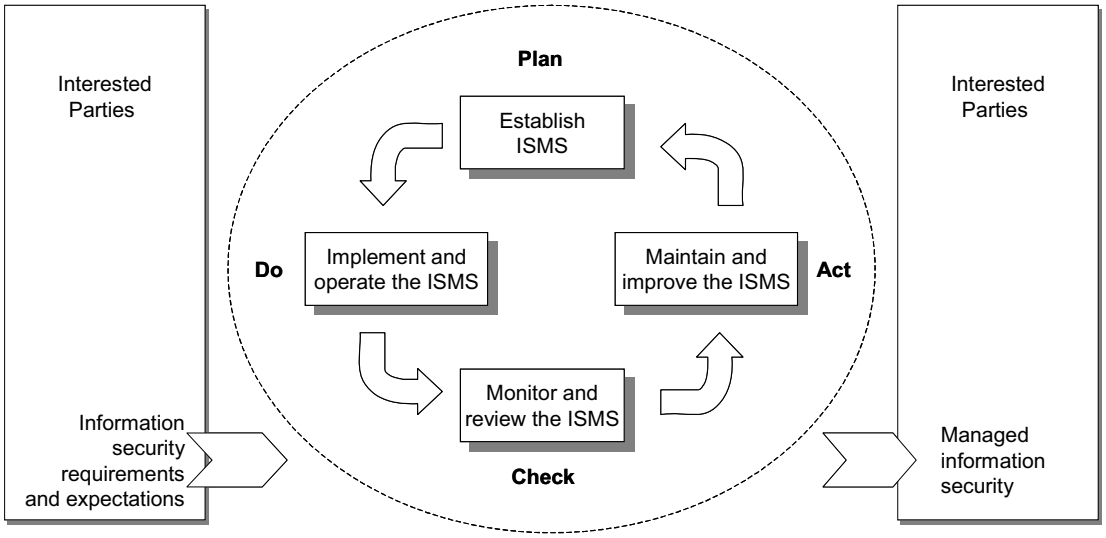


Figure 1 — PDCA model applied to ISMS processes

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

0.3 Compatibility with other management systems

This International Standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards. Table C.1 illustrates the relationship between the clauses of this International Standard, ISO 9001:2000 and ISO 14001:2004.

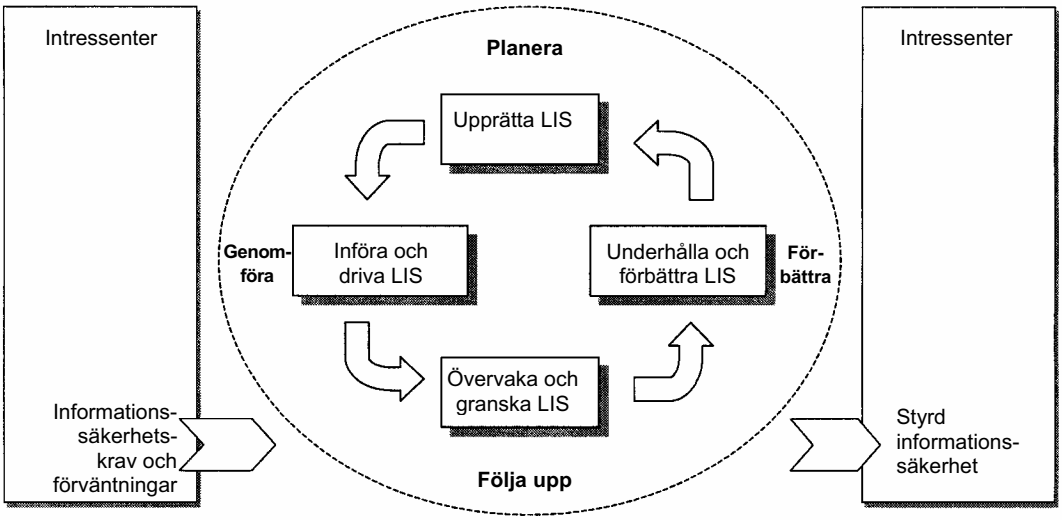
This International Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

EXEMPEL 1

Ett krav kan vara att överträdelser av informationssäkerhet inte får orsaka allvarlig ekonomisk skada för en organisation och/eller olägenhet för organisationen.

EXEMPEL 2

En förväntning kan vara att om en allvarlig incident inträffar – kanske attack på en organisations webbplats för e-handel – bör det finnas personal som har fått tillräcklig praktisk utbildning i tillämpliga rutiner för att minimera skadeverkan.



Figur 1 – PDCA-modellen tillämpad på LIS-processen

Planera (upprätta LIS)	Upprätta policy för LIS, mål, processer och rutiner som är relevanta för riskhantering och förbättring av informationssäkerhet och som ger resultat i linje med organisationens övergripande policy och mål.
Genomföra (införa och driva LIS)	Införa och driva policyn för LIS, säkerhetsåtgärder, processer och rutiner.
Följa upp (övervaka och granska LIS)	Bedöma och, där det är tillämpligt, mäta processers prestanda i förhållande till LIS-policyn, mål och praktisk erfarenhet samt rapportera resultaten till ledningen för granskning.
Förbättra (underhålla och förbättra LIS)	Vidta korrigerande och förebyggande åtgärder, baserade på resultaten av interna revisioner av LIS och ledningens genomgång eller annan relevant information, för att ständigt förbättra LIS.

0.3 Förenlighet med andra ledningssystem

Denna standard är samordnad med SS-EN ISO 9001:2000 och SS-EN ISO 14001:2004 för att stödja enhetligt och integrerat införande och drift med besläktade ledningssystemstandarder. Ett lämpligt utformat ledningssystem kan alltså uppfylla kraven i alla dessa standarder. Tabell C.1 visar sambanden mellan avsnitten i denna standard, i SS-EN ISO 9001:2000 och i SS-EN ISO 14001:2004.

Denna standard är utformad så att en organisation kan samordna eller integrera sitt LIS med krav i besläktade ledningssystem.