SVENSK STANDARD
SS-ISO/IEC 27002:2014

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 – Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2013, IDT)

Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013, 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 27002:2013 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO/IEC 27002:2013 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-ISO/IEC 27002:2005 utgåva 1.

The International Standard ISO/IEC 27002:2013 has the status of a Swedish Standard. This document contains the Swedish language version of ISO/IEC 27002:2013 followed by the official English version.

This standard supersedes the Swedish Standard SS-ISO/IEC 27002:2005, 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

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 Directives, Part 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 procent 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.

ISO/IEC 27002 togs fram av den gemensamma tekniska kommittén ISO/IEC JTC 1, Informationsteknologi, underkommitté SC 27, IT-säkerhetstekniker.

Denna andra utgåva upphäver och ersätter den första utgåvan (SS-ISO/IEC 27002:2005), som har reviderats med avseende på tekniskt innehåll och struktur.

0 Orientering

0.1 Allmänt

Denna standard är avsedd för organisationer att användas som referens för val av säkerhetsåtgärder inom ramen för att införa ett ledningssystem för informationssäkerhet (LIS) baserat på SS-ISO/IEC 27001:2013[10]. Den kan även användas som vägledning för organisationer i införandet av allmänt accepterade informationssäkerhetsåtgärder. Denna standard är också avsedd att användas i utvecklingen av bransch- och organisationsspecifika riktlinjer gällande hantering av informationssäkerhet, med hänsyn tagen till deras områdesspecifika informationssäkerhetsrisker.

Organisationer av alla slag och storlekar (inklusive offentliga och privata, kommersiella och ideella) samlar in, bearbetar, lagrar och överför information i många former, inklusive elektroniskt, fysiskt och verbalt (t.ex. samtal och presentationer).

Värdet av informationen går längre än skrivna ord, siffror och bilder: kunskap, koncept, idéer och varumärken är exempel på immateriella former av information. I en sammanlänkad värld är information och relaterade processer, system, nätverk och personal inom driften, hantering och skydd av tillgångar, lika värdefulla för en organisations verksamhet som andra viktiga tillgångar. De förtjänar eller behöver därför skydd mot olika riskbilder.

Tillgångar är utsatta för både avsiktliga och oavsiktliga hot medan relaterade processer, system, nätverk och människor har inneboende svagheter. Ändringar av verksamhetsprocesser och system eller andra yttre förändringar (som nya författningar) kan skapa nya informationssäkerhetsrisker. Därför, med tanke på de många sätt som hot kan utnyttja sårbarheter för att skada en organisation är informationssäkerhetsrisker alltid närvarande. Verkningsfull hantering av informationssäkerhet minskar dessa risker genom att skydda en organisation mot hot och sårbarheter och minskar därmed dess påverkan på organisationens tillgångar.

Informationssäkerhet uppnås genom att införa en lämplig uppsättning av säkerhetsåtgärder, inklusive policy och tillhörande regelverk, processer, rutiner, organisatoriska strukturer samt funktioner i program och hårdvara. Dessa säkerhetsåtgärder behöver vid behov upprättas, införas, övervakas, granskas och förbättras, för att uppfylla varje organisations specifika säkerhets- och verksamhetsmål. Ett LIS så som det definieras i SS-ISO/IEC 27001 har en holistisk och samordnad syn på organisationens informationssäkerhetsrisker, i syfte att införa en uppsättning informationssäkerhetsåtgärder inom ramen för ett sammanhållet ledningssystem.

Många informationssystem har inte utformats för att vara säkra i den mening som avses i SS-ISO/IEC 27001 och denna standard. Den säkerhet som kan uppnås enbart genom tekniska hjälpmedel är begränsad och bör stödjas av lämplig hantering och rutiner. Att identifiera vilka säkerhetsåtgärder som bör införas kräver noggrann planering och detaljfokus. Ett framgångsrikt LIS kräver stöd av alla medarbetare i organisationen. Det kan också krävas deltagande från intressenter, leverantörer eller andra externa parter. Specialistråd från externa parter kan också behövas.

I en mer allmän bemärkelse ger verkningsfull informationssäkerhet ledningen, och andra intressenter, möjlighet att kunna förlita sig på att organisationens tillgångar är rimligt säkra och skyddade mot skador och den utgör en förutsättning för verksamheten.

0.2 Informationssäkerhetskrav

Det är väsentligt att en organisation identifierar sina säkerhetskrav. Det finns tre huvudsakliga källor för säkerhetskrav:

a) bedömning av organisationens risker, med hänsyn tagen till organisationens övergripande verksamhetsstrategi och mål, vilket sker genom en riskbedömning där hot mot tillgångar identifieras, sårbarheter och sannolikheten för deras förekomst utvärderas och den potentiella konsekvensen beräknas

b) författningsenliga och avtalsmässiga krav som en organisation, dess handelspartners, leverantörer och tjänsteleverantörer måste uppfylla, samt deras sociokulturella miljö

c) den uppsättning principer, mål och verksamhetskrav för informationshantering, bearbetning, lagring, kommunikation och arkivering som en organisation har utvecklat för att stödja sin verksamhet.

De resurser som behövs i införandet av säkerhetsåtgärder måste balanseras mot vad som kan bli resultatet av en säkerhetsrelaterad skada för verksamheten vid avsaknad av dessa säkerhetsåtgärder. Resultatet från en riskanalys hjälper till att styra och besluta om lämpliga åtgärder och prioriteringar för att hantera informationssäkerhetsrisker, och för att införa valda säkerhetsåtgärder för att skydda verksamheten mot dessa risker.

SS-ISO/IEC 27005[11] ger vägledning om hantering av informationssäkerhetsrisker, inklusive vägledning om riskbedömning, riskbehandling, riskacceptans, riskkommunikation, riskövervakning och granskning av risker.

0.3 Val av säkerhetsåtgärder

Säkerhetsåtgärder kan väljas från denna standard eller andra uppsättningar av säkerhetsåtgärder. Alternativt kan nya säkerhetsåtgärder utformas för att möta särskilda behov i den omfattning som krävs.

Valet av säkerhetsåtgärder är beroende av organisatoriska beslut som grundas på kriterierna för riskacceptans, alternativen för riskbehandling samt allmän tillämpad riskhanteringsstrategi för organisationen, och bör också omfattas av nationella och internationella lagar och förordningar. Val av säkerhetsåtgärder beror också på det sätt som de samverkar för att ge ett skydd på flera nivåer.

Vissa av säkerhetsåtgärderna i denna standard kan betraktas som vägledande principer för hantering av informationssäkerhet och är tillämpliga för de flesta organisationer. Säkerhetsåtgärderna förklaras mer i detalj nedan tillsammans med en vägledning för införande. Mer information om att välja säkerhetsåtgärder och andra riskbehandlingsalternativ kan hittas i SS-ISO/IEC 27005[11].

0.4 Utveckla egna riktlinjer

Denna standard kan betraktas som en utgångspunkt för att utveckla organisationsspecifika riktlinjer. Alla säkerhetsåtgärder och vägledningar i denna standard är kanske inte tillämpliga. Dessutom kan ytterligare säkerhetsåtgärder och riktlinjer som inte ingår i denna standard krävas. När dokument som innehåller ytterligare riktlinjer eller säkerhetsåtgärder utvecklas, kan det i förekommande fall vara relevant att inkludera korsreferenser till avsnitt i denna standard. Detta för att underlätta för revisorer och verksamhetspartners att genomföra granskningar av efterlevnad.

0.5 Livscykelsöverväganden

Information har en naturlig livscykel, från skapande och uppkomst genom lagring, bearbetning, användning och överföring till dess slutliga förstörelse eller upplösning. Tillgångars värde och risker kopplade till dem kan variera över tid (t.ex. obehörigt röjande eller stöld av ett företags räkenskap är avsevärt mindre betydelsefullt efter att de har publicerats formellt) men informationssäkerhet förblir viktigt under alla stadier.

Informationssystem har livscykler där de utformas, specificeras, designas, utvecklas, testas, införs, används, underhålls, utrangeras och kasseras. Informationssäkerhet bör beaktas i alla skeden. Ny systemutveckling och förändringar av befintliga system innebär möjligheter för organisationer att uppdatera och förbättra säkerhetsåtgärderna genom att beakta verkliga incidenter, samt nuvarande och möjliga framtida informationssäkerhetsrisker.

0.6 Relaterade standarder

Medan denna standard ger vägledning avseende ett brett spektrum av informationssäkerhetsåtgärder som vanligen tillämpas i många olika organisationer, ger de återstående standarderna i ISO 27000-serien kompletterande råd eller krav på andra aspekter av den övergripande processen för hantering av informationssäkerhet.

SS-ISO/IEC 27000 innehåller en allmän introduktion till LIS och den resterande familjen av standarder. SS-ISO/IEC 27000 tillhandahåller en ordlista där de flesta av de termer som används i hela ISO 27000-seriens standarder är formellt definierade, samt beskriver omfattning och mål för varje del av serien.

Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder

1 Omfattning

Denna standard ger vägledning för organisationens interna normer för informationssäkerhet och praktisk hantering av informationssäkerhet. Det innefattar val av, införande och förvaltning av säkerhetsåtgärder med hänsyn tagen till organisationens riskmiljö gällande informationssäkerhet.

Denna standard är utformad för att användas av organisationer som avser att:

a) välja säkerhetsåtgärder för införande av ett ledningssystem för informationssäkerhet baserat på SS-ISO/IEC 27001[10];

b) införa allmänt accepterade informationssäkerhetsåtgärder;

c) utveckla sina egna riktlinjer för hantering av informationssäkerhet.

2 Normativa hänvisningar

Följande dokument, hela eller delar av, är nödvändiga när det här dokumentet 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, *Informationsteknik — Säkerhetstekniker — Ledningssystem för informationssäkerhet — Översikt och terminologi*

Contents

Page

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.

ISO/IEC 27002 was prepared by Joint Technical Committee 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 structurally revised.

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] 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.

Information technology — Security techniques — Code of practice for information security controls

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;[10]

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

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*