SVENSK STANDARD
SS-ISO/IEC 27002:2022

Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2022, IDT)

Information security – cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022, IDT)

Svenska Institutet för Standarder

Språk: svenska/Swedish; engelska/English
Utgåva: 3

Denna standard är såld av
SEK Svensk Elstandard som även lämnar
allmänna upplysningar om svensk och utländsk standard.
Postadress: SEK, Box 1284, 164 29 Kista
Telefon: 08-444 14 00.
E-post: sek@elstandard.se Internet: www.elstandard.se

Svenska Institutet för Standarder

Den här standarden kan hjälpa dig att effektivisera och kvalitetssäkra ditt arbete. SIS har fler tjänster att erbjuda dig för att underlätta tillämpningen av standarder i din verksamhet.

SIS Abonnemang
Snabb och enkel åtkomst till gällande standard med SIS Abonnemang, en prenumerationstjänst genom vilken din organisation får tillgång till all världens standarder, senaste uppdateringarna och där hela din organisation kan ta del av innehållet i prenumerationen.

Utbildning, event och publikationer
Vi erbjuder även utbildningar, rådgivning och event kring våra mest sålda standarder och frågor kopplade till utveckling av standarder. Vi ger också ut handböcker som underlättar ditt arbete med att använda en specifik standard.

Vill du delta i ett standardiseringsprojekt?
Genom att delta som expert i någon av SIS 300 tekniska kommittéer inom CEN (europeisk standardisering) och/eller ISO (internationell standardisering) har du möjlighet att påverka standardiseringsarbetet i frågor som är viktiga för din organisation. Välkommen att kontakta SIS för att få veta mer!

Kontakt
Skriv till kundservice@sis.se, besök sis.se eller ring 08 - 555 523 10

Upplysningar om sakinnehållet i standarden lämnas av Svenska institutet för standarder, telefon 08 - 555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Standarden är framtagen av kommittén för LIS, SIS/TK 318/AG 11.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Fastställd: 2022-09-22
ICS: 01.140.30; 03.100.70; 04.050; 33.040.40; 35.020; 35.030; 35.040; 35.080

Svenska Institutet för Standarder

Den internationella standarden ISO/IEC 27002:2022 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO/IEC 27002:2022 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-ISO/IEC 27002:2014, utgåva 2, SS-EN ISO/IEC 27002:2017, utgåva 1.

The International Standard ISO/IEC 27002:2022 has the status of a Swedish Standard. This document contains the Swedish language version of ISO/IEC 27002:2022 followed by the official English version.

This standard supersedes the Swedish Standard SS-ISO/IEC 27002:2014, edition 2, SS-EN ISO/IEC 27002:2017, edition 1.

Svenska Institutet för Standarder

LÄSANVISNINGAR FÖR STANDARDER

I dessa anvisningar behandlas huvudprinciperna för hur regler och yttre begränsningar anges i standardiseringsprodukter.

Krav
Ett krav är ett uttryck i ett dokuments innehåll som anger objektivt verifierbara kriterier som ska uppfyllas och från vilka ingen avvikelse tillåts om efterlevnad av dokumentet ska kunna åberopas.Krav uttrycks med hjälpverbet **ska** (eller **ska inte** för förbud).

Rekommendation
En rekommendation är ett uttryck i ett dokuments innehåll som anger en valmöjlighet eller ett tillvägagångssätt som bedöms vara särskilt lämpligt utan att nödvändigtvis nämna eller utesluta andra. Rekommendationer uttrycks med hjälpverbet **bör** (eller **bör inte** för avrådanden).

Instruktion
Instruktioner anges i imperativ form och används för att ange hur något görs eller utförs. De kan underordnas en annan regel, såsom ett krav eller en rekommendation. De kan även användas självständigt, och är då att betrakta som krav.

Förklaring
En förklaring är ett uttryck i ett dokuments innehåll som förmedlar information. En förklaring kan uttrycka tillåtelse, möjlighet eller förmåga. Tillåtelse uttrycks med hjälpverbet **får**. Inom standardiseringen saknas rekommenderad nekande motsats till hjälpverbet får, förbud uttrycks med **ska inte** enligt reglerna för krav. Möjlighet och förmåga uttrycks med hjälpverbet **kan** (eller motsatsen **kan inte**).

READING INSTRUCTIONS FOR STANDARDS

These instructions cover the main principles for the use of provisions and external constraints in standardization deliverables.

Requirement
A requirement is an expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled, and from which no deviation is permitted if conformance with the document is to be claimed. Requirements are expressed by the auxiliary **shall** (or **shall not** for prohibition).

Recommendation
A recommendation is an expression, in the content of a document, that conveys a suggested possible choice or course of action deemed to be particularly suitable, without necessarily mentioning or excluding others. Recommendations are expressed by the auxiliary **should** (or **should not** for dissuasion).

Instruction
An instruction is expressed in the imperative mood and is used in order to convey an action to be performed. It can be subordinated to another provision, such as a requirement or a recommendation. It can also be used independently and is then to be regarded as a requirement.

Statement
A statement is an expression, in the content of a document, that conveys information. A statement can express permission, possibility or capability. Permission is expressed by the auxiliary **may**. There is no recommended opposite expression for the auxiliary may in standardization, prohibition is expressed by the use of **shall not** in accordance with the rules for requirements. Possibility and capability are expressed by the auxiliary **can** (its opposite being **cannot**).

Innehållsförteckning

Förord

ISO (Internationella standardiseringsorganisationen) och IEC (Internationella elektrotekniska kommissionen) bildar ett speciellt system för internationell standardisering. Nationella organ som är medlemmar i ISO eller IEC deltar i utarbetandet av internationella standarder i tekniska kommittéer som har inrättats av respektive organisation för specifika tekniska verksamhetsområden. ISO:s och IEC:s tekniska kommittéer samarbetar inom områden av ömsesidigt intresse. Andra internationella organisationer, statliga såväl som icke-statliga, som samarbetar med ISO och IEC deltar också i arbetet.

De förfaranden som använts vid utarbetandet av det här dokumentet samt de som är avsedda att tillämpas vid uppdatering därav beskrivs i ISO/IEC-direktiven, del 1. Det bör särskilt noteras att det krävs olika godkännandekriterier för olika typer av dokument. Det här dokumentet har utarbetats i enlighet med de redaktionella reglerna i ISO/IEC-direktiven, del 2 (se www.iso.org/directives eller www.iec.ch/members_experts/refdocs).

Observera att vissa delar i detta dokument kan omfattas av patenträtter. ISO och IEC ansvarar inte i någon del för identifiering av sådana patenträttigheter. Information om eventuella patenträttigheter som identifierats under dokumentets utarbetande återges i avsnittet Inledning och/eller ISO:s förteckning över mottagna patentdeklarationer (se www.iso.org/patents) eller i IEC:s förteckning över mottagna patentdeklarationer (se patents.iec.ch).

Eventuella handelsnamn som förekommer i dokumentet anges som i informationssyfte för att underlätta för användarna och innebär inte något godkännande.

För förklarande information om standarders frivilliga karaktär, innebörden i ISO-specifika termer och uttryck som rör bedömning av överensstämmelse samt information om ISO:s efterlevnad av Världshandelsorganisationens (WTO:s) principer i avtalet om tekniska handelshinder (TBT) se www.iso.org/iso/foreword.html. För IEC, se www.iec.ch/understanding-standards.

Detta dokument har utarbetats av den gemensamma tekniska kommittén ISO/IEC JTC 1, *Information technology*, underkommitté SC 27, *Information security, cybersecurity and privacy protection*.

Denna tredje utgåva upphäver och ersätter den andra utgåvan (ISO/IEC 27002:2013), som har genomgått teknisk översyn. Den inbegriper även de tekniska rättelserna ISO/IEC 27002:2013/Cor 1:2014 och ISO/IEC 27002:2013/Cor 2:2015.

De huvudsakliga förändringarna i förhållande till den föregående utgåvan är att:

- titeln har ändrats,
- dokumentstrukturen har ändrats så att säkerhetsåtgärderna nu presenteras med hjälp av en enkel taxonomi och åtföljande attribut,
- vissa säkerhetsåtgärder har slagits samman, andra har strukits och flera nya säkerhetsåtgärder har införts. Förhållandet mellan de båda utgåvorna anges närmare i bilaga B.

Återkoppling eller frågor som rör det här dokumentet bör framföras till standardiseringsorganet i användarens land. En komplett förteckning över dessa organ finns på www.iso.org/members.html och www.iec.ch/national-committees.

Inledning

0.1 Allmänt

Detta dokument är avsett för organisationer av alla slag och storlekar. Det ska användas som referens för att fastställa och vidta säkerhetsåtgärder i syfte att hantera informationssäkerhetsrisker i ett ledningssystem för informationssäkerhet (LIS) baserat på ISO/IEC 27001. Dokumentet kan även användas som vägledning för organisationer för att fastställa och genomföra allmänt vedertagna informationssäkerhetsåtgärder. Detta dokument är också avsett att användas vid utveckling av bransch- och organisationsspecifika riktlinjer för hantering av informationssäkerhet, med beaktande av organisationens specifika risksituation i fråga om informationssäkerhet. Andra organisatoriska säkerhetsåtgärder eller säkerhetsåtgärder för respektive teknisk miljö än de som anges i detta dokument kan vid behov fastställas genom riskbedömning.

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

Informationens värde handlar om mer än skrivna ord, siffror och bilder; kunskap, koncept, idéer och varumärken är exempel på immateriella former av information. I en sammankopplad värld är information och andra relaterade tillgångar förtjänta av skydd, eller så krävs det att de skyddas, mot olika riskkällor, oavsett om dessa är naturliga, oavsiktliga eller avsiktliga.

Informationssäkerhet uppnås genom att en lämplig uppsättning säkerhetsåtgärder genomförs, inklusive policyer, regler, processer, rutiner, organisatoriska strukturer samt funktioner i program och hårdvara. För att uppfylla organisationens specifika säkerhets- och verksamhetsmål bör den vid behov fastställa, genomföra, övervaka, granska och förbättra dessa säkerhetsåtgärder. I ett LIS, såsom det framställs i ISO/IEC 27001, tas ett samordnat helhetsperspektiv på organisationens informationssäkerhetsrisker i syfte att fastställa och genomföra en uppsättning informationssäkerhetsåtgärder inom ramen för ett sammanhållet ledningssystem.

Många informationssystem, inklusive deras förvaltning och drift, har inte utformats för att vara säkra ur ett LIS-perspektiv enligt vad som anges i ISO/IEC 27001 och detta dokument. Den säkerhetsnivå som kan uppnås enbart genom tekniska åtgärder är begränsad och bör stödjas av lämpliga ledningsaktiviteter och organisationsprocesser. Att identifiera vilka säkerhetsåtgärder som bör finnas på plats kräver noggrann planering och detaljfokus, samtidigt som riskbehandling utförs.

För att ett LIS ska bli framgångsrikt krävs det stöd från all personal i organisationen. Det kan också krävas deltagande från andra intressenter, t.ex. aktieägare eller leverantörer. Råd från ämnesexperter kan också behövas.

Ett lämpligt, tillräckligt och verkningsfullt ledningssystem för informationssäkerhet säkerställer för organisationens ledning och andra intressenter att deras information och andra relaterade tillgångar är rimligt säkra och skyddade mot hot och skador och gör det därigenom möjligt för organisationen att uppnå de angivna verksamhetsmålen.

0.2 Informationssäkerhetskrav

Det är mycket viktigt att organisationen fastställer sina informationssäkerhetskrav. Det finns tre huvudsakliga källor för informationssäkerhetskrav:

a) bedömningen av organisationens risker, med hänsyn tagen till organisationens övergripande verksamhet och mål. Detta kan underlättas eller stödjas av en informationssäkerhetsspecifik riskbedömning. Detta bör resultera i att det fastställs vilka säkerhetsåtgärder som krävs för att säkerställa att den kvarstående risken för organisationen uppfyller dess kriterier för acceptabel risknivå.

b) författnings- och avtalskrav som en organisation och dess intressenter (handelspartner, tjänsteleverantörer osv.) måste uppfylla, samt deras sociokulturella miljö.

c) den uppsättning principer, mål och verksamhetskrav för alla steg i informationens livscykel som en organisation har utvecklat för att stödja sin verksamhet.

0.3 Säkerhetsåtgärder

En säkerhetsåtgärd definieras som en åtgärd som modifierar eller bibehåller risk. Vissa av säkerhetsåtgärderna i detta dokument modifierar risk, medan andra bibehåller risk. En informationssäkerhetspolicy kan t.ex. bara bibehålla risken, medan efterlevnad av informationssäkerhetspolicyn kan modifiera risken. En del säkerhetsåtgärder beskriver dessutom samma generiska åtgärd i olika risksammanhang. Det här dokumentet innehåller en sammanställning av organisatoriska, personrelaterade, fysiska och tekniska informationssäkerhetsåtgärder som bygger på internationellt erkänd bästa praxis.

0.4 Fastställa säkerhetsåtgärder

Säkerhetsåtgärder fastställs utifrån organisationens beslut efter en riskbedömning, med en tydligt definierad omfattning. Beslut som rör identifierade risker bör baseras på kriterierna för riskacceptans, alternativen för riskbehandling samt organisationens strategier för riskhantering. När säkerhetsåtgärder fastställs bör även all relevant nationell och internationell lagstiftning och reglering beaktas. Fastställandet av säkerhetsåtgärder beror också på det sätt som säkerhetsåtgärderna samverkar med varandra för att ge ett flernivåskydd.

Organisationen kan utforma säkerhetsåtgärder efter behov, eller identifiera dem från någon annan källa. När säkerhetsåtgärder specificeras bör organisationen ställa de resurser och investeringar som behövs för att införa och tillämpa en säkerhetsåtgärd mot den verksamhetsnytta som uppnås. Se ISO/IEC TR 27016 för vägledning om beslut som rör investering i ett LIS samt de ekonomiska konsekvenserna av sådana beslut när konkurrerande resurskrav föreligger.

Det bör finnas en balans mellan de resurser som används för att genomföra säkerhetsåtgärder och säkerhetsincidenters potentiella påverkan på verksamheten när säkerhetsåtgärder saknas. Resultatet av en riskbedömning bör tjäna som vägledning vid beslut om lämpliga åtgärder, prioriteringar för att hantera informationssäkerhetsrisker och för att genomföra säkerhetsåtgärder som bedöms vara nödvändiga för att skydda mot dessa risker.

Vissa av säkerhetsåtgärderna i detta dokument kan betraktas som vägledande principer för hantering av informationssäkerhet och som tillämpliga för de flesta organisationer. Mer information om att välja säkerhetsåtgärder och andra riskbehandlingsalternativ kan hittas i ISO/IEC 27005.

0.5 Utarbeta organisationsspecifika riktlinjer

Detta dokument kan betraktas som en utgångspunkt för att utarbeta organisationsspecifika riktlinjer. Alla säkerhetsåtgärder och all vägledning i detta dokument behöver inte vara tillämpliga på alla organisationer. Ytterligare säkerhetsåtgärder och riktlinjer som inte ingår i detta dokument kan även krävas för att hantera organisationens särskilda behov och de risker som har identifierats. När dokument som innehåller ytterligare riktlinjer eller säkerhetsåtgärder utarbetas, kan det i framtiden vara relevant att inkludera korshänvisningar till avsnitt i detta dokument.

0.6 Livscykelbedömningar

Information har en livscykel, från det att den skapas till att den gallras. Informationens värde och riskerna kan variera under hela livscykeln (t.ex. är obehörigt röjande eller stöld av ett företags räkenskaper inte betydelsefullt efter det att de har publicerats, men integriteten är fortfarande av stor betydelse) men därför förblir informationssäkerheten i viss utsträckning viktig i alla stadier.

Informationssystem och andra tillgångar som är relevanta för informationssäkerheten har livscykler där de utformas, specificeras, designas, utvecklas, testas, införs, används, underhålls, tas ur drift och avvecklas. Informationssäkerheten bör beaktas i alla skeden. Nya systemutvecklingsprojekt och

förändringar av befintliga system innebär möjligheter att förbättra säkerhetsåtgärderna, samtidigt som organisationens risker och lärdomar från incidenter beaktas.

0.7 Relaterade internationella standarder

Även om detta dokument ger vägledning avseende ett brett spektrum av informationssäkerhetsåtgärder som vanligen tillämpas i många olika organisationer, innehåller andra dokument i ISO/IEC 27000-serien kompletterande vägledning eller krav som rör andra aspekter i den övergripande processen för hantering av informationssäkerhet.

ISO/IEC 27000 innehåller en allmän introduktion till LIS och standardserien. ISO/IEC 27000 innehåller en ordlista där de flesta av de termer som används i ISO/IEC 27000-serien definieras, och beskriver omfattning och mål för varje standard i serien.

Det finns sektorspecifika standarder som innehåller ytterligare säkerhetsåtgärder för specifika områden (t.ex. ISO/IEC 27017 för molntjänster, ISO/IEC 27701 för hantering av personuppgifter, ISO/IEC 27019 för energi, ISO/IEC 27011 för telekomsektorn och ISO 27799 för hälso- och sjukvård). Dessa standarder anges i litteraturförteckningen och det finns även hänvisningar till vissa av dem i vägledningen samt i avsnitt 5–8.

Informationssäkerhet, cybersäkerhet och integritetsskydd – Informationssäkerhetsåtgärder

1 Omfattning

Detta dokument innehåller en referensuppsättning allmänna informationssäkerhetsåtgärder, inklusive vägledning för genomförande av dessa. Denna standard är utformad för att användas av organisationer:

a) inom ramen för ett ledningssystem för informationssäkerhet (LIS) baserat på ISO/IEC 27001,

b) för att genomföra informationssäkerhetsåtgärder som bygger på internationellt erkänd bästa praxis,

c) för att utveckla organisationsspecifika riktlinjer för hantering av informationssäkerhet.

2 Normativa hänvisningar

Detta dokument innehåller inga normativa hänvisningar.

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

'This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27002:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27002:2013/Cor. 1:2014 and ISO/IEC 27002:2013/Cor. 2:2015.

The main changes are as follows:

— the title has been modified;

— the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;

— some controls have been merged, some deleted and several new controls have been introduced. The complete correspondence can be found in Annex B.

This corrected version of ISO/IEC 27002:2022 incorporates the following corrections:

— non-functioning hyperlinks throughout the document have been restored;

— in the introductory table in subclause 5.22 and in Table A.1 (row 5.22), "#information_security_assurance" has been moved from the column headed "Security domains" to the column headed "Operational capabilities".

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

0.1 Background and context

This document is designed for organizations of all types and sizes. It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. Furthermore, this document is intended for use in developing industry and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.

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

The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and other associated assets deserve or require protection against various risk sources, whether natural, accidental or deliberate.

Information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions. To meet its specific security and business objectives, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001 takes a holistic, coordinated view of the organization's information security risks in order to determine and implement a comprehensive suite of information security controls within the overall framework of a coherent management system.

Many information systems, including their management and operations, have not been designed to be secure in terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail while carrying out risk treatment.

A successful ISMS requires support from all personnel in the organization. It can also require participation from other interested parties, such as shareholders or suppliers. Advice from subject matter experts can also be needed.

A suitable, adequate and effective information security management system provides assurance to the organization's management and other interested parties that their information and other associated assets are kept reasonably secure and protected against threats and harm, thereby enabling the organization to achieve the stated business objectives.

0.2 Information security requirements

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

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;

b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their socio-cultural environment;

c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

0.3 Controls

A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

0.4 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment, with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

The organization can design controls as required or identify them from any source. In specifying such controls, the organization should consider the resources and investment needed to implement and operate a control against the business value realized. See ISO/IEC TR 27016 for guidance on decisions regarding the investment in an ISMS and the economic consequences of these decisions in the context of competing requirements for resources.

There should be a balance between the resources deployed for implementing controls and the potential resulting business impact from security incidents in the absence of those controls. The results of a risk assessment should help guide and determine the appropriate management action, priorities for managing information security risks and for implementing controls determined necessary to protect against these risks.

Some of the controls in this document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can be applicable to all organizations. Additional controls and guidelines not included in this document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document for future reference.

0.6 Life cycle considerations

Information has a life cycle, from creation to disposal. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical) therefore, information security remains important to some extent at all stages.

Information systems and other assets relevant to information security have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be considered at every stage. New system development projects and changes to existing systems provide opportunities to improve security controls while taking into account the organization's risks and lessons learned from incidents.

0.7 Related International Standards

While this document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, other documents 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 ISMS and the family of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the family.

There are sector-specific standards that have additional controls which aim at addressing specific areas (e.g. ISO/IEC 27017 for cloud services, ISO/IEC 27701 for privacy, ISO/IEC 27019 for energy, ISO/IEC 27011 for telecommunications organizations and ISO 27799 for health). Such standards are included in the Bibliography and some of them are referenced in the guidance and other information sections in Clauses 5-8.

Information security, cybersecurity and privacy protection — Information security controls

1 Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing organization-specific information security management guidelines.

2 Normative references

There are no normative references in this document.