SVENSK STANDARD
SS-ISO/IEC 27003:2018

Fastställd/Approved: 2018-02-12
Publicerad/Published: 2018-02-20
Utgåva/Edition: 2
Språk/Language: svenska/Swedish; engelska/English,
ICS: 01.140.30;03.100.70;04.050;35.020;35.030;35.040;35.240.01

Informationsteknik – Säkerhetstekniker – Vägledning för införande av ledningssystem för informationssäkerhet

Information technology – Security techniques – Information security management system – Guidance

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 27003:2017 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO 27003:2017.

Denna standard ersätter SS-ISO 27003:2010 utgåva 1.

The International Standard ISO 27003:2017 has the status of a Swedish Standard. This document contains the Swedish language version of ISO 27003:2017.

This standard supersedes the Swedish Standard SS-EN 27003:2010, edition 1.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS 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, who can also provide general information about Swedish and foreign standards.

Denna standard 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.

Innehåll

Förord

ISO (Internationella standardiseringsorganisationen) och IEC (Internationella elektrotekniska kommissionen) bildar det specialiserade systemet för världsomspännande standardisering. Nationella organ som är medlemmar i ISO eller IEC deltar i utvecklingen av internationella standarder genom tekniska kommittéer, utsedda av respektive organisation, vilka ägnar sig åt olika tekniska områden. ISO:s och IEC:s tekniska kommittéer samarbetar på områden där de har gemensamma intressen. Dessutom deltar andra internationella organisationer, både statliga och icke-statliga, i arbetet tillsammans med ISO och IEC. På området för informationsteknik har ISO och IEC inrättat en gemensam teknisk kommitté, ISO/IEC JTC 1.

De förfaranden som har använts för att utveckla detta dokument och de som är avsedda för dess fortsatta underhåll beskrivs i ISO/IEC-direktiven, del 1. Framför allt bör de olika godkännandekriterierna för de olika typerna av dokument noteras. Det här dokumentet har upprättats i enlighet med de redaktionella reglerna i ISO/IEC-direktiven, Del 2 (se www.iso.org/directives).

Observera att vissa beståndsdelar i denna internationella standard kan vara föremål för patenträtter. ISO och IEC ska inte hållas ansvariga för att identifiera några eller alla sådana patenträtter. Information om eventuella patenträttigheter som identifierats under framtagandet av dokumentet finns i introduktionen och/eller på ISO-listan över mottagna patentförklaringar (se www.iso.org/patents).

Eventuella handelsnamn som används i dokumentet är information avsedd för användarnas bekvämlighet och utgör inget godkännande.

En förklaring av betydelsen av ISO-specifika termer och uttryck som är kopplade till överensstämmelsebedömningar samt information om ISO:s uppfyllande av WTO:s (World Trade Organization) principer i avtalet om tekniska handelshinder (TBT) finns på följande URL: www.iso.org/iso/foreword.html.

Detta dokument har framställts av ISO/IEC JTC 1, *Information Technology*, underkommitté SC 27, *IT Security Techniques*.

Denna andra utgåva av ISO/IEC 27003 ogiltigförklarar och ersätter den första utgåvan (ISO/IEC 27003:2010), som har reviderats tekniskt.

Denna utgåva innehåller följande betydande ändringar i förhållande till den föregående utgåvan:

- Omfattningen och titeln har ändrats för att ge förklaring och vägledning kring kraven i ISO/IEC 27001:2013 i stället för den föregående versionen som gav vägledning till införande av ISO/IEC 27001:2005.
- Strukturen är nu anpassad till strukturen i ISO/IEC 27001:2013 så att den lättare kan användas tillsammans med ISO/IEC 27001:2013.
- Den föregående versionen av ISO/IEC 27003 hade en inriktning på projekt med ett flöde av aktiviteter som inte tillämpas i den här versionen. Den här versionen ger i stället vägledning till kraven oavsett i vilken ordning de införs.

Orientering

Detta dokument ger vägledning till kraven på ledningssystem för informationssäkerhet (LIS) enligt definitionen i ISO/IEC 27001 och ger rekommendationer (”bör”), möjligheter (”kan”) och tillstånd (”får”) för dessa. Syftet med detta dokument är inte att ge allmän vägledning till alla aspekter av informationssäkerhet.

Avsnitt 4 till 10 i det här dokumentet återspeglar strukturen i ISO/IEC 27001:2013.

Det här dokumentet innehåller inga nya krav på ledningssystem för informationssäkerhet (LIS) och dess relaterade termer och definitioner. Organisationer bör använda ISO/IEC 27001 och ISO/IEC 27000 för krav och definitioner. Organisationer som tillämpar ett ledningssystem för informationssäkerhet (LIS) måste inte följa vägledningen i det här dokumentet.

I ett ledningssystem för informationssäkerhet (LIS) betonas vikten av följande faser:

– förståelse för organisationens behov och nödvändigheten av att upprätta en informationssäkerhetspolicy och informationssäkerhetsmål,

– bedömning av organisationens informationssäkerhetsrisker,

– tillämpning och hantering av processer för informationssäkerhet, säkerhetsåtgärder och andra mått för att behandla risker,

– övervakning och granskning av prestanda och effektivitet hos ett ledningssystem för informationssäkerhet (LIS), och

– ständig förbättring.

Ett ledningssystem för informationssäkerhet (LIS) har i likhet med andra typer av ledningssystem följande huvuddelar:

a) policy,

b) personer med definierade ansvarsområden,

c) ledningsprocesser relaterade till:

   1) upprättande av policy

   2) medvetandeskapande och kompetensförsörjning,

   3) planering,

   4) tillämpning,

   5) verksamhet,

   6) bedömning av prestanda,

   7) ledningens genomgång,

   8) förbättring

d) dokumenterad information.

Ett ledningssystem för informationssäkerhet (LIS) har fler viktiga komponenter, t.ex. följande:

e) bedömning av informationssäkerhetsrisker, och

f) behandling av informationssäkerhetsrisker, inklusive fastställande och införande av säkerhetsåtgärder.

Detta dokument är allmänt och är avsett att kunna tillämpas på alla organisationer oavsett typ, storlek och beskaffenhet. Organisationen bör fastställa vilken del av denna vägledning som gäller för den utifrån dess specifika förutsättningar (se ISO/IEC 27001:2013, avsnitt 4).

Till exempel kan viss vägledning lämpa sig bättre för stora organisationer, men för mycket små organisationer (t.ex. med färre än tio personer) kan viss vägledning vara onödig eller olämplig.

Beskrivningarna i avsnitt 4 till 10 har följande struktur:

– **Kravställd aktivitet**: här presenteras aktiviteter som krävs för att uppfylla kraven i det motsvarande underavsnittet i ISO/IEC 27001,

– **Förklaring**: här förklaras vad kraven i ISO/IEC 27001 innebär,

– **Vägledning**: här ges mer detaljerad eller understödjande information för utförande av ”kravställda aktiviteter” med exempel på utförande, och

– **Ytterligare information**: här ges ytterligare information som kan beaktas.

ISO/IEC 27003, ISO/IEC 27004 och ISO/IEC 27005 utgör en uppsättning dokument som ger stöd och vägledning gällande ISO/IEC 27001:2013. Bland dessa dokument är ISO/IEC 27003 ett grundläggande och heltäckande dokument som ger vägledning till alla krav i ISO/IEC 27001. Det innehåller dock inga detaljerade beskrivningar av ”övervakning, mätning, analys och utvärdering” och hantering av informationssäkerhetsrisker. ISO/IEC 27004 och ISO/IEC 27005 behandlar specialområden och ger mer detaljerad vägledning till ”övervakning, mätning, analys och utvärdering” och hantering av informationssäkerhetsrisker.

Det finns flera uttryckliga hänvisningar till dokumenterad information i ISO/IEC 27001. Dock kan en organisation ha ytterligare dokumenterad information som den bedömer vara nödvändig för dess ledningssystem som en del av dess respons på ISO/IEC 27001:2013, 7.5.1 b). I dessa fall används i det här dokumentet frasen ”Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i dess ledningssystem (se ISO/IEC 27001:2013, 7.5.1 b).”

Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Vägledning

1 Omfattning

Detta dokument innehåller förklaringar och vägledning till ISO/IEC 27001:2013.

2 Normativa hänvisningar

I texten hänvisas till de följande dokumenten på ett sådant sätt att hela innehållet i dem eller en del av det utgör krav i detta dokument. För daterade hänvisningar gäller endast den citerade utgåvan. För odaterade hänvisningar gäller den senaste utgåvan av det dokument som hänvisats till (inkl. tillägg).

ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

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

3 Termer och definitioner

För detta dokument gäller de termer och definitioner som anges i ISO/IEC 27000:2016.

ISO och IEC driver terminologiska databaser för användning i standardisering på följande adresser:

– IEC:s Electropedia: http://www.electropedia.org/

– ISO:s Online Browsing Platform: http://www.iso.org/obp

4 Organisationens förutsättningar

4.1 Att förstå organisationen och dess förutsättningar

Kravställd aktivitet

Organisationen avgör vilka externa och interna frågor som är relevanta för dess syfte och som påverkar dess förmåga att nå de avsedda resultaten med ledningssystemet för informationssäkerhet (LIS).

Förklaring

En inneboende egenskap i ett ledningssystem för informationssäkerhet (LIS) är att organisationen kontinuerligt analyserar sig själv och omvärlden. Denna analys berör externa och interna frågor som på något sätt påverkar informationssäkerheten och hur informationssäkerheten kan hanteras, och som är relevanta för organisationens mål.

Analysen av dessa frågor har tre syften:

– att förstå sammanhanget för att besluta om omfattningen av ledningssystemet för informationssäkerhet (LIS),

– att analysera sammanhanget för att fastställa risker och möjligheter,

– att säkerställa att ledningssystemet för informationssäkerhet (LIS) anpassas till föränderliga externa och interna frågor.

Externa frågor är sådana som befinner sig utom organisationens kontroll. Detta kallas ofta organisationens externa kontext. En analys av den externa kontexten kan omfatta följande aspekter:

a) sociala och kulturella,

b) politiska, rättsliga, normativa och reglerande,

c) finansiella och makroekonomiska,

d) tekniska,

e) miljörelaterade

f) konkurrensrelaterade.

Dessa aspekter av organisationens kontext innebär ständigt frågor som påverkar informationssäkerheten och sättet att hantera informationssäkerheten på. Vilka de externa frågorna är beror på organisationens specifika prioriteringar och situation.

Till exempel kan följande externa frågor vara relevanta för en viss organisation:

g) de rättsliga följderna av att använda en outsourcad it-tjänst (rättslig aspekt),

h) naturförhållanden med avseende på risken för katastrofer som bränder, översvämningar och jordbävningar (miljörelaterad aspekt),

i) teknisk utveckling av dataintrångsverktyg och användning av kryptografi (teknisk aspekt),

j) den allmänna efterfrågan på organisationens tjänster (social, kulturell eller finansiell aspekt).

Interna frågor är sådana som är inom organisationens kontroll. En analys av de interna frågorna kan omfatta följande aspekter:

k) organisationens kultur,

l) policy, och tillhörande regelverk, mål samt strategier för att förverkliga dem,

> **Svensk ANM.** Den engelska textens ”policies” översätts till policy och tillhörande regelverk. Denna översättning överensstämmer med definitionen av policy i SS-ISO/IEC 27000 och med svenskt språkbruk.

m) ledning, organisationsstruktur, roller och ansvarsfördelning,

n) interna standarder, riktlinjer och modeller som införs av organisationen,

o) avtalsförhållanden som direkt kan påverka organisationens processer inom ramen för ledningssystemet för informationssäkerhet (LIS),

p) processer och rutiner,

q) förmågor vad gäller resurser och kunskap (t.ex. kapital, tid, personer, processer, system och teknik),

r) fysisk infrastruktur och miljö,

s) informationssystem, informationsflöden och beslutsprocesser (både formella och informella),

t) tidigare revisioner eller resultat av tidigare riskbedömningar.

Resultaten av denna aktivitet används i 4.3 och 6.1.

Vägledning

Med utgångspunkt i en förståelse av organisationens syfte (t.ex. med hänvisning till dess målbeskrivning eller affärsplan) samt det eller de avsedda målen för organisationens ledningssystem för informationssäkerhet (LIS) bör organisationen:

– granska den externa kontexten för att identifiera relevanta externa frågor,

– granska de interna aspekterna för att identifiera relevanta interna frågor.

Vid identifiering av relevanta frågor kan följande behöva beaktas: Hur påverkar en viss kategori (se punkterna a–t ovan) informationssäkerhetsmålen? Detta kan belysas med tre exempel på interna frågor:

Exempel 1 om ledning och organisationsstruktur (se punkt m)): När ett ledningssystem för informationssäkerhet (LIS) införs bör man ta hänsyn till befintliga lednings- och organisationsstrukturer. Ett exempel på detta är att organisationen kan basera strukturen för sitt ledningssystem för informationssäkerhet (LIS) på strukturen hos andra befintliga ledningssystem, och kan kombinera gemensamma funktioner, t.ex. ledningens genomgång och revision.

Exempel 2 om policy, mål samt strategier (se punkt l)): En analys av verksamhetens olika policyer, mål samt strategier kan visa vad organisationen avser att uppnå och hur informationssäkerhetsmålen kan anpassas till verksamhetsmålen så att goda resultat kan säkerställas.

Exempel 3 om informationssystem och informationsflöden (se punkt s)): Vid fastställande av interna frågor bör organisationen på ett tillräckligt detaljerat sätt identifiera informationsflödena mellan dess olika informationssystem.

Eftersom både de externa och interna frågorna förändras med tiden bör frågorna och deras påverkan på omfattningen av, begränsningarna av och kraven på ledningssystem för informationssäkerhet (LIS) granskas regelbundet.

Dokumenterad information om aktiviteten och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effekten av ledningssystemet (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

I ISO/IEC 27000 har definitionen av ”organisation” en anmärkning som lyder: ”Termen ”organisation” innefattar, men är inte begränsad till, egenföretagare, bolag, koncern, firma, företag, myndighet, affärspartner, välgörenhetsorganisation eller institution, eller delar, alternativt kombinationer, av dem, oavsett ägarstruktur eller om de är offentliga eller privata.” Vissa av dessa exempel avser juridiska personer, medan andra inte gör det.

Det finns fyra typfall:

1) organisationen är en juridisk person eller en administrativ enhet (t.ex. egenföretagare, bolag, koncern, firma, företag, myndighet, affärspartner, välgörenhetsorganisation eller institution oavsett ägarstruktur eller om den är offentlig eller privat),

2) organisationen är en underavdelning av en juridisk person eller en administrativ enhet (t.ex. en del av ett bolag, en koncern eller ett företag),

3) organisationen är en uppsättning juridiska personer eller administrativa enheter (t.ex. ett konsortium av egenföretagare, större bolag, koncerner eller firmor),

4) organisationen är en uppsättning underavdelningar av juridiska personer eller administrativa enheter (t.ex. föreningar eller branschorganisationer).

4.2 Att förstå intressenters behov och förväntningar

Kravställd aktivitet

Organisationen fastställer vilka intressenter som är relevanta för ledningssystem för informationssäkerhet (LIS) och vilka av deras krav som är relevanta för informationssäkerheten.

Förklaring

”Intressent” är en term (se ISO/IEC 27000:2016, 2.41) som avser personer eller organisationer som kan påverka, påverkas av eller anse sig vara påverkade av ett beslut eller en aktivitet från organisationens sida. Intressenter finns både i och utanför organisationen och kan ha specifika behov, förväntningar och krav när det gäller organisationens informationssäkerhet.

Följande kan vara externa intressenter:

a) tillsynsmyndigheter och lagstiftare,

b) aktieägare (inkl. ägare och investerare),

c) leverantörer (inkl. underleverantörer, konsulter och samarbetspartner vid outsourcing),

d) branschorganisationer,

e) konkurrenter,

f) kunder och konsumenter,

g) aktivistgrupper.

Följande kan vara interna intressenter:

h) beslutsfattare (inkl. ledande befattningshavare),

i) processansvariga, systemansvariga och informationsansvariga,

j) supportfunktioner, t.ex. it-avdelningar och personalavdelningar,

k) anställda och användare,

l) ansvariga för informationssäkerhet.

Resultaten av denna aktivitet används i 4.3 och 6.1.

Vägledning

Följande åtgärder bör vidtas:

- identifiera externa intressenter,
- identifiera interna intressenter,
- identifiera intressenters krav.

Eftersom intressenternas behov, förväntningar och krav förändras med tiden bör dessa förändringar och deras inverkan på omfattningen, begränsningarna och kraven för ledningssystem för informationssäkerhet (LIS) granskas regelbundet.

Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i dess ledningssystem (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

Ingen ytterligare information.

4.3 Att bestämma ledningssystemets omfattning

Kravställd aktivitet

Organisationen fastställer gränserna och tillämpligheten för ledningssystemet för informationssäkerhet (LIS) för att bestämma dess omfattning.

Förklaring

Omfattningen anger var och exakt för vad ledningssystemet för informationssäkerhet (LIS) är respektive inte är tillämpligt. Att fastställa omfattningen är därför en viktig aktivitet som anger den nödvändiga utgångspunkten för alla andra aktiviteter vid införandet av ett ledningssystem för informationssäkerhet (LIS)S. Exempelvis ger inte riskbedömning och riskbehandling, inklusive fastställande av säkerhetsåtgärder, några tillförlitliga resultat om man inte vet exakt var ledningssystemet för informationssäkerhet (LIS) är tillämpligt. Det är också mycket viktigt att ha ingående kunskaper om ledningssystemet för informationssäkerhets (LIS) begränsningar och tillämplighet samt om gränssnitten och beroendeförhållandena mellan organisationen och andra organisationer. Alla ändringar av omfattningen vid en senare tidpunkt kan resultera i betydande ytterligare merarbete och kostnader.

Följande faktorer kan påverka fastställandet av omfattningen:

a) de externa och interna frågor som beskrivs i 4.1,

b) intressenterna och deras krav som fastställs enligt ISO/IEC 27001:2013, 4.2,

c) verksamhetens förutsättningar och förmåga för att ingå som en del av omfattningen för ledningssystemet för informationssäkerhet (LIS),

d) alla stödfunktioner, dvs. funktioner som krävs för att stödja verksamheten (t.ex. personaladministration, it-tjänster och programvara, förvaltning av byggnader, fysiska zoner, grundläggande tjänster),

e) alla funktioner som outsourcas till andra delar inom organisationen eller till externa leverantörer.

Omfattningen av ett ledningssystem för informationssäkerhet (LIS) kan skilja sig mycket mellan olika implementeringar. Omfattningen kan t.ex. inkludera:

- en eller flera särskilda processer,
- en eller flera särskilda funktioner,
- en eller flera särskilda tjänster,
- en eller flera särskilda sektioner eller platser,
- en juridisk enhet samt
- en administrativ enhet och en eller flera av dess leverantörer.

Vägledning

Vid fastställning av omfattningen kan en strategi i flera steg användas:

f) Fastställande av preliminär omfattning: detta bör göras av en liten men representativ grupp av företrädare för ledningen.

g) Fastställande av reviderad omfattning: de funktionella enheterna inom och utom den preliminära omfattningen bör ses över, eventuellt följt av en inkludering eller exkludering av vissa av dessa funktionella enheter för att minska antalet gränssnitt som berör avgränsningen för omfattningen.

När den preliminära omfattningen revideras bör alla stödfunktioner som anses vara nödvändiga för att stödja affärsverksamheten beaktas.

h) Fastställande av den slutliga omfattningen: den reviderade omfattningen bör utvärderas av alla ledande befattningshavare som berörs av den. Vid behov bör den justeras och sedan noggrant beskrivas.

i) Godkännande av omfattningen: den dokumenterade information som beskriver omfattningen bör godkännas formellt av högsta ledningen.

Organisationen bör också beakta aktiviteter som påverkar ledningssystem för informationssäkerhet (LIS) och aktiviteter som outsourcas till andra delar inom organisationen eller till externa leverantörer. Vad gäller sådana aktiviteter bör gränssnitt (fysiska, tekniska och organisatoriska) och deras inverkan på omfattningen identifieras.

Dokumenterad information som beskriver omfattningen kan innehålla:

j) organisationens omfattning, gränser och gränssnitt,

k) omfattning, gränser och gränssnitt för informationsteknik,

l) fysisk omfattning samt fysiska gränser och gränssnitt.

Ytterligare information

Ingen ytterligare information.

4.4 Ledningssystem för informationssäkerhet (LIS)

Kravställd aktivitet

Organisationen upprättar, inför, underhåller och förbättrar ständigt sitt ledningssystem för informationssäkerhet (LIS).

Förklaring

I ISO/IEC 27001:2013, 4.4 anges det centrala kravet för att upprätta, införa, underhålla och ständigt förbättra ledningssystemet för informationssäkerhet (LIS). I de andra delarna av ISO/IEC 27001 beskrivs de obligatoriska beståndsdelarna i ett ledningssystem för informationssäkerhet (LIS), men enligt detta avsnitt är organisationen skyldig att säkerställa att alla nödvändiga krav är uppfyllda för att upprätta, införa, underhålla och ständigt förbättra sitt ledningssystem för informationssäkerhet (LIS).

Vägledning

Ingen specifik vägledning.

Ytterligare information

Ingen ytterligare information.

5 Ledarskap

5.1 Ledarskap och engagemang

Kravställd aktivitet

Högsta ledningen visar ledarskap och engagemang i fråga om ledningssystem för informationssäkerhet (LIS).

Förklaring

Ledarskap och engagemang är avgörande för ett effektivt ledningssystem för informationssäkerhet (LIS).

Högsta ledningen definieras (se ISO/IEC 27000) som en person eller grupp av personer som leder och styr en organisation på högsta nivå, dvs. högsta ledningen har det övergripande ansvaret för ledningssystemet för informationssäkerhet (LIS). Detta innebär att den leder arbetet med ledningssystemet för informationssäkerhet (LIS) på samma sätt som andra områden inom organisationen, t.ex. fördelning och uppföljning av budget Högsta ledningen kan delegera befogenheter inom organisationen och tillhandahålla resurser för utförande av aktiviteter med anknytning till informationssäkerhet och ledningssystemet för informationssäkerhet (LIS), men den har ändå det övergripande ansvaret.

Till exempel kan den organisation som inför och driver ledningssystemet för informationssäkerhet (LIS) vara en verksamhetsenhet inom en större organisation. I det här fallet är högsta ledningen den person eller grupp av personer som leder och styr denna verksamhetsenhet.

Högsta ledningen deltar också i ledningens genomgång (se 9.3) och främjar ständig förbättring (se 10.2).

Vägledning

Högsta ledningen bör visa ledarskap och engagemang på följande sätt:

a) Högsta ledningen bör säkerställa att informationssäkerhetspolicyn och informationssäkerhetsmålen har upprättats och är förenliga med organisationens strategiska inriktning.

b) Högsta ledningen bör säkerställa att de krav och säkerhetsåtgärder som rör ledningssystemet för informationssäkerhet (LIS) är integrerade i organisationens processer. Hur detta uppnås bör anpassas till organisationens specifika sammanhang. Till exempel kan en organisation som har utsett processägare delegerat ansvar till personer eller grupp av personer för att införa tillämpliga krav.

Högsta ledningens stöd kan också behövas för att övervinna motstånd inom organisationen mot förändringar av processer och säkerhetsåtgärder.

c) Högsta ledningen bör säkerställa tillgången till resurser för ett effektivt ledningssystem för informationssäkerhet (LIS). Resurserna behövs för upprättande, införande, underhåll och förbättring av ledningssystemet för informationssäkerhet (LIS), samt för att införa informationssäkerhetsåtgärder. Resurser som behövs för ledningssystem för informationssäkerhet (LIS) består av:

   1) finansiella resurser,

   2) personal,

   3) anläggningar och

   4) teknisk infrastruktur.

De nödvändiga resurserna beror på organisationens förutsättningar, såsom storlek, komplexitet samt interna och externa krav. Ledningens genomgång bör ge information som indikerar om resurserna är tillräckliga för organisationen.

d) Högsta ledningen bör kommunicera behovet av hantering av informationssäkerhet i organisationen och behovet av att anpassa sig till kraven i ledningssystemet för informationssäkerhet (LIS). Detta kan göras genom att ge praktiska exempel som illustrerar hur det faktiska behovet ser ut inom organisationen och genom att kommunicera informationssäkerhetskrav.

e) Högsta ledningen bör säkerställa att ledningssystemet för informationssäkerhet (LIS) uppnår sina avsedda resultat genom att stödja genomförandet av alla processer för hantering av informationssäkerhet, och i synnerhet genom att begära och granska rapporter om ledningssystemet för informationssäkerhets (LIS) status och effektivitet (se 5.3 b)). Sådana rapporter kan härledas från mätningar (se 6.2 b) och 9.1 a)), ledningens genomgång och revisionsrapporter. Högsta ledningen kan också ställa upp resultatmål för nyckelpersoner som arbetar med ledningssystemet för informationssäkerhet (LIS).

f) Högsta ledningen bör leda och stödja personer i organisationen som är direkt involverade i informationssäkerhet och ledningssystemet för informationssäkerhet (LIS). Om detta inte görs kan det ha en negativ inverkan på effektiviteten hos ledningssystemet för informationssäkerhet (LIS). Återkoppling från högsta ledningen kan inkludera hur planerade aktiviteter är anpassade till organisationens strategiska behov och även prioritering av olika aktiviteter i ledningssystemet för informationssäkerhet (LIS).

g) Högsta ledningen bör bedöma resursbehoven under ledningens genomgång och fastställa mål för ständiga förbättringar samt för övervakning av de planerade aktiviteternas effektivitet.

h) Högsta ledningen bör stödja personer som har tilldelats roller och ansvar i samband med hantering av informationssäkerhet, så att de är motiverade och har förmåga att leda och stödja informationssäkerhetsaktiviteter inom sitt område.

I de fall där den organisation som inför och driver ett ledningssystem för informationssäkerhet (LIS) är en del av en större organisation kan ledarskap och engagemang förbättras genom involvering av den person eller den grupp av personer som leder och styr den större organisationen. Om de förstår vad det innebär att införa ett ledningssystem för informationssäkerhet (LIS) kan de ge stöd till högsta ledningen inom omfattningen för ledningssystemet för informationssäkerhet (LIS) och hjälpa dem att visa ledarskap och engagemang för ledningssystemet för informationssäkerhet (LIS). Om t.ex. intressenter som inte omfattas av ledningssystemet för informationssäkerhet (LIS) är engagerade i beslutsfattande som rör informationssäkerhetsmål och riskkriterier och är medvetna om resultaten från arbetet med

informationssäkerhet i ledningssystem för informationssäkerhet (LIS), kan beslut om fördelning av resurser anpassas till kraven från ledningssystemet för informationssäkerhet (LIS).

Ytterligare information

Ingen ytterligare information.

5.2 Policy

Kravställd aktivitet

Högsta ledningen fastställer en informationssäkerhetspolicy.

Förklaring

Informationssäkerhetspolicyn beskriver ledningssystemet för informationssäkerhets (LIS) strategiska betydelse för organisationen och finns tillgänglig som dokumenterad information. Policyn styr informationssäkerhetsaktiviteterna inom organisationen.

Policyn anger hur behovet av informationssäkerhet ser ut för den aktuella organisationen.

Vägledning

Informationssäkerhetspolicyn bör innehålla korta avsiktsförklaringar på hög nivå och styr arbetet med informationssäkerhet. Den kan vara särskilt anpassad till omfattningen för ledningssystemet för informationssäkerhet (LIS) eller ha ett större tillämpningsområde än omfattningen för ledningssystemet för informationssäkerhet (LIS).

Alla regelverk, rutiner, aktiviteter och mål kopplade till informationssäkerhet bör anpassas till informationssäkerhetspolicyn.

Informationssäkerhetspolicyn bör återspegla organisationens affärssituation och kultur samt dess frågor och problem som rör informationssäkerhet. Informationssäkerhetspolicyns omfattning ska överensstämma med organisationens syfte och kultur och man bör sträva efter en balans mellan att vara lättläst och heltäckande. Det är viktigt att de som använder policyn kan identifiera sig med dess strategiska inriktning.

Informationssäkerhetspolicyn kan antingen innehålla organisationens informationssäkerhetsmål eller beskriva ramarna för hur informationssäkerhetsmålen ska fastställas (dvs. vem som fastställer dem för ledningssystemet för informationssäkerhet (LIS) och hur de ska användas inom ramen för ledningssystemet för informationssäkerhet (LIS)). I mycket stora organisationer bör t.ex. högnivåmål fastställas av högsta ledningen för hela organisationen. Därefter bör målen anges i detalj enligt den ram som har fastställts i informationssäkerhetspolicyn för att ge vägledning till alla intressenter.

Informationssäkerhetspolicyn bör innehålla ett tydligt uttalande från högsta ledningen om dess åtagande att uppfylla de krav som rör informationssäkerhet.

Informationssäkerhetspolicyn bör innehålla ett tydligt uttalande om att högsta ledningen stöder ständiga förbättringar inom all verksamhet. Det är viktigt att understryka denna princip i policyn så att personer som omfattas av ledningssystemet för informationssäkerhet (LIS) är medvetna om den.

Informationssäkerhetspolicyn bör kommuniceras till alla personer som omfattas av ledningssystemet för informationssäkerhet (LIS). Därför bör dess format och språk vara utformat så att den kan förstås av alla mottagare.

Högsta ledningen bör besluta vilka intressenter som policyn behöver kommuniceras till. Informationssäkerhetspolicyn kan skrivas på ett sådant sätt att det går att kommunicera den till relevanta intressenter

utanför organisationen. Exempel på sådana externa intressenter är kunder, leverantörer, entreprenörer, underleverantörer och tillsynsmyndigheter. Om informationssäkerhetspolicyn görs tillgänglig för externa intressenter bör den inte innehålla konfidentiell information.

Informationssäkerhetspolicyn kan antingen vara en separat fristående policy eller ingå i en övergripande policy som omfattar flera typer av ledningssystem inom organisationen (t.ex. ledningssystem för kvalitet, miljö och informationssäkerhet).

Informationssäkerhetspolicyn bör finnas tillgänglig som dokumenterad information. Enligt kraven i ISO/IEC 27001 specificeras inte någon särskild form för denna dokumenterade information, därför är det upp till organisationen att avgöra vilken form som är lämpligast. Om organisationen har en mall för policyer bör denna användas för informationssäkerhetspolicyn.

Ytterligare information

Ytterligare information om policy och tillhörande regelverk som rör informationssäkerhet finns i ISO/IEC 27002.

Ytterligare information om förhållandet mellan informationssäkerhetspolicyn och andra policyer finns i bilaga A.

5.3 Befattningar, ansvar och befogenheter inom organisationen

Kravställd aktivitet

Högsta ledningen säkerställer att roller som är relevanta för informationssäkerhet tilldelas ansvar och befogenheter och att dessa kommuniceras inom organisationen.

Förklaring

Högsta ledningen säkerställer att roller och ansvar samt nödvändiga befogenheter som är relevanta för informationssäkerhet tilldelas och kommuniceras.

Syftet med detta krav är att tilldela ansvar och befogenheter för att säkerställa att ledningssystemet för informationssäkerhet (LIS) överensstämmer med kraven i ISO/IEC 27001 och säkerställa att prestandan för ledningssystemet för informationssäkerhet (LIS) rapporteras till högsta ledningen.

Vägledning

Högsta ledningen bör regelbundet säkerställa att ansvar och befogenheter för ledningssystemet för informationssäkerhet (LIS) tilldelas på så sätt att ledningssystemet uppfyller de krav som anges i ISO/IEC 27001. Högsta ledningen behöver inte tilldela alla roller, ansvar och befogenheter, men den bör på lämpligt sätt delegera befogenhet att göra detta. Högsta ledningen bör godkänna viktiga roller, ansvar och befogenheter i ledningssystemet för informationssäkerhet (LIS).

Ansvar och befogenheter relaterade till informationssäkerhetsaktiviteter bör tilldelas. Sådana aktiviteter omfattar:

a) samordning av upprättande, införande, underhåll, prestandarapportering och förbättring av ledningssystemet för informationssäkerhet (LIS),

b) rådgivning om bedömning och behandling av informationssäkerhetsrisker,

c) utformning av processer och system för informationssäkerhet,

d) besluta om interna standarder avseende fastställande, konfiguration och användning av informationssäkerhetsåtgärder,

e) hantering av informationssäkerhetsincidenter samt

f) granskning och revision av ledningssystemet för informationssäkerhet (LIS).

Förutom de roller som är direkt relaterade till informationssäkerhet bör relevanta ansvarsområden och befogenheter för informationssäkerhet även ingå i andra roller. Till exempel kan ansvar för informationssäkerhet införlivas i följande roller:

g) informationsägare,

h) processägare,

i) ägare av tillgång (t.ex. applikationsägare eller ägare av infrastruktur),

j) riskägare,

k) funktion eller person med ansvar för koordinering av informationssäkerhet (denna befattning är normalt en stödjande befattning i ledningssystemet för informationssäkerhet (LIS)),

l) projektledare,

m) linjechefer,

n) informationsanvändare.

Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i dess ledningssystem (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

Ingen ytterligare information.

6 Planering

6.1 Åtgärder för att hantera risker och möjligheter

6.1.1 Allmänt

Översikt

ISO/IEC 27001:2013, 6.1 handlar om planering av åtgärder för att hantera alla typer av risker och möjligheter som är relevanta för ledningssystemet för informationssäkerhet (LIS). Detta inkluderar riskbedömning och planering av riskbehandling.

Enligt strukturen i ISO/IEC 27001 delas risker upp i två kategorier under planeringen:

a) risker och möjligheter som är relevanta för avsedda resultat av ledningssystemet för informationssäkerhet (LIS) i sin helhet,

b) informationssäkerhetsrisker som hänför sig till förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystemet för informationssäkerhet (LIS).

Den första kategorin bör hanteras i enlighet med kraven i ISO/IEC 27001:2013, 6.1.1 (Allmänt). De risker som hör till denna kategori kan vara risker som hänför sig till själva ledningssystemet för informationssäkerhet (LIS), definitionen av omfattningen av ledningssystemet för informationssäkerhet (LIS), högsta ledningens engagemang för informationssäkerhet, resurser för drift av ledningssystem för informationssäkerhet (LIS) etc. De möjligheter som faller inom denna kategori kan vara möjligheter relaterade till resultat för ledningssystem för informationssäkerhet (LIS), det kommersiella värdet av ett ledningssystem för informationssäkerhet (LIS), effektiviteten i genomförandet av processer inom ledningssystemet för informationssäkerhet (LIS) och informationssäkerhetsåtgärder etc.

Den andra kategorin består av alla risker som direkt hänför sig till förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystemet för informationssäkerhet (LIS). Dessa risker ska hanteras i enlighet med 6.1.2 (Bedömning av informationssäkerhetsrisker) och 6.1.3 (Behandling av informationssäkerhetsrisker).

Organisationer kan välja att använda olika tekniker för varje kategori.

Uppdelningen av kraven för att hantera risker kan förklaras på följande sätt:

- Den uppmuntrar kompatibilitet med andra ledningssystemsstandarder för de organisationer som har integrerade ledningssystem för olika aspekter såsom kvalitet, miljö och informationssäkerhet.

- Den kräver att organisationen fastställer och tillämpar en fullständig och detaljerad process för bedömning och behandling av informationssäkerhetsrisker.

- Den betonar att hanteringen av informationssäkerhetsrisker är en grundläggande del i ledningssystemet för informationssäkerhet (LIS).

I ISO/IEC 27001:2013 6.1.1 används uttrycken ”avgöra vilka risker och möjligheter som behöver hanteras” och ”hantera dessa risker och möjligheter”. Ordet ”avgöra” kan anses vara liktydigt med ordet ”bedöma” i ISO/IEC 27001:2013, 6.1.2 (dvs. identifiera, analysera och utvärdera). På samma sätt kan ordet ”hantera” anses vara liktydigt med ordet ”behandla” som används i ISO/IEC 27001:2013, 6.1.3.

Kravställd aktivitet

När organisationen planerar sitt ledningssystem för informationssäkerhet (LIS) bör den avgöra risker och möjligheter genom att beakta de frågor som hänvisas till i 4.1 och de krav som hänvisas till i 4.2.

Förklaring

Organisationen avgör vilka risker och möjligheter som är relevanta för de avsedda resultaten med ledningssystemet för informationssäkerhet (LIS) baserat på interna och externa frågor (se 4.1) och krav från intressenterna (se 4.2). Därefter planerar organisationen sitt ledningssystem för informationssäkerhet (LIS) för att:

a) säkerställa att ledningssystemet för informationssäkerhet (LIS) uppnår de avsedda resultaten, t.ex. att informationssäkerhetsriskerna kommer att vara kända för riskägarna och behandlas till en acceptabel nivå,

b) förebygga eller minska oönskade effekter av risker som är relevanta för ledningssystem för informationssäkerhets (LIS) avsedda resultat och

c) uppnå ständig förbättring (se 10.2), t.ex. genom lämpliga mekanismer för att upptäcka och åtgärda brister i ledningsprocesserna eller ta vara på möjligheter att förbättra informationssäkerheten.

Risker förknippade med a) ovan kan vara oklara processer och ansvarsområden, bristande medvetenhet bland anställda, bristande engagemang från ledningen etc. Risker förknippade med b) ovan kan vara dålig riskhantering eller bristande medvetenhet om risker. Risker förknippade med c) ovan kan vara bristande hantering av dokumentation och processer som rör ledningssystemet för informationssäkerhet (LIS).

När en organisation tar vara på de möjligheter som uppstår i arbetet påverkas organisationens förutsättningar (ISO/IEC 27001:2013, 4.1) eller intressenternas behov och förväntningar (ISO/IEC27001:2013, 4.2), vilket kan förändra riskerna för organisationen. Exempel på sådana möjligheter kan vara att begränsa verksamheten till vissa produkt- eller tjänsteområden, att skapa en marknadsföringsstrategi för vissa geografiska regioner eller utöka partnerskap med andra organisationer.

Möjligheter finns också vad gäller ständig förbättring av processer och dokumentation som rör ledningssystemet för informationssäkerhet (LIS), samt utvärdering av ledningssystem för informationssäkerhets (LIS) avsedda resultat. Till exempel resulterar behandling av ett relativt nytt ledningssystem för informationssäkerhet (LIS) ofta i identifiering av möjligheter till utveckling av processer genom att klargöra gränssnitt, minska administrativa kostnader, eliminera delar av processer som inte är kostnadseffektiva, revidera dokumentation och införa ny informationsteknik.

Planeringen i detta avsnitt omfattar fastställandet av:

d) åtgärder för att hantera risker och möjligheter,

e) hur den ska:

1) integrera och vidta dessa åtgärder i processerna inom ledningssystemet för informationssäkerhet (LIS),

2) utvärdera om åtgärderna har gett avsedd verkan.

Vägledning

Organisationen bör:

f) avgöra vilka risker och möjligheter som kan påverka uppnåendet av de mål som beskrivs i a), b) och c), genom att beakta de frågor som hänvisas till i 4.1 och de krav som hänvisas till i 4.2,

g) utveckla en plan för att vidta de fastställda åtgärderna och utvärdera effektiviteten hos dessa åtgärder. Åtgärderna bör planeras med tanke på integrering av processer för informationssäkerhet och dokumentation i befintliga strukturer. Alla dessa åtgärder är kopplade till informationssäkerhetsmål (6.2) som ligger till grund för bedömning och behandling av informationssäkerhetsriskerna (se 6.1.2 och 6.1.3).

Det allmänna kravet att ständigt förbättra ledningssystemet för informationssäkerhet (LIS) som anges i ISO/IEC 27001:2013, 10.2 stöds av kravet på att uppnå ständig förbättring som anges i 6.1.1 med andra relevanta krav i 5.1 g), 5.2 d), 9.1, 9.2 och 9.3.

De åtgärder som krävs i detta avsnitt kan vara olika för den strategiska, taktiska och operativa nivån, för olika platser eller för olika tjänster eller system.

Flera strategier kan användas för att uppfylla kraven i 6.1.1, varav två är:

– att beakta risker och möjligheter kopplade till planering, genomförande och drift av ledningssystemet för informationssäkerhet (LIS) separat från informationssäkerhetsrisker,

– att beakta alla risker samtidigt.

En organisation som integrerar ett ledningssystem för informationssäkerhet (LIS) i ett befintligt ledningssystem kan finna att kraven i detta avsnitt uppfylls genom organisationens befintliga metoder för verksamhetsplanering. Om så är fallet är det viktigt att kontrollera att metoden omfattar alla krav i detta avsnitt.

Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i dess ledningssystem (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

Mer information om riskhantering finns i ISO 31000.

6.1.2 Bedömning av informationssäkerhetsrisker

Kravställd aktivitet

Organisationen fastställer och tillämpar en process för bedömning av informationssäkerhetsrisker.

Förklaring

Organisationen fastställer en process för bedömning av informationssäkerhetsrisker som:

a) upprättar och upprätthåller:

1) kriterier för riskacceptans och

2) kriterier för att utföra bedömningar av informationssäkerhetsrisker, t.ex. kriterier för att bedöma konsekvens och sannolikhet, samt regler för att bestämma risknivån,

b) säkerställer att upprepade bedömningar av informationssäkerhetsrisker genererar konsekventa, korrekta och jämförbara resultat.

Processen för bedömning av informationssäkerhetsrisker detaljeras sedan genom följande delprocesser:

c) Identifiering av informationssäkerhetsrisker:

   1) Identifiera risker förknippade med förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen hos ledningssystemet för informationssäkerhet (LIS).

   2) Identifiera riskägare förknippade med dessa risker, dvs. identifiera och utse personer med rätt behörighet och ansvar för att hantera identifierade risker.

d) Analys av informationssäkerhetsriskerna:

   1) Bedöma de potentiella konsekvenserna om de identifierade riskerna realiseras, t.ex. direkt påverkan på verksamheten såsom finansiell förlust eller indirekt påverkan på verksamheten såsom anseendeskada. Bedömda konsekvenser kan rapporteras med kvantitativa eller kvalitativa värden.

   2) Bedöma den realistiska sannolikheten för förekomsten av de risker som identifierats, med kvantitativa (dvs. baserat på sannolikhet eller frekvens) eller kvalitativa värden.

   3) Fastställa nivåerna av identifierad risk som en fördefinierad kombination av bedömda konsekvenser och sannolikheter.

e) Utvärdering av informationssäkerhetsriskerna:

   1) Jämföra resultaten av riskanalyser med de kriterier för riskacceptans som fastställts tidigare.

   2) Prioritera de analyserade riskerna för riskbehandling, dvs. besluta om skyndsam behandling av risker som anses vara oacceptabla och fastställa en ordningsföljd om flera risker behöver behandlas.

Processen för bedömning av informationssäkerhetsrisker används sedan.

Organisationen bevarar dokumenterad information om alla steg i processen för bedömning av informationssäkerhetsrisker (6.1.2 a) till e)) samt resultaten av dess tillämpning.

Vägledning

Vägledning om upprättande av riskkriterier (6.1.2 a))

Kriterierna för informationssäkerhetsrisker bör fastställas med tanke på organisationens förutsättningar och kraven från intressenterna och de bör definieras i enlighet med högsta ledningens riskpreferenser och riskuppfattning samtidigt som de bör möjliggöra en genomförbar och lämplig riskhanteringsprocess.

Kriterierna för informationssäkerhetsrisker bör fastställas i relation till ledningssystemet för informationssäkerhets (LIS) avsedda resultat.

Enligt ISO/IEC 27001:2013, 6.1.2 a) bör kriterier för bedömning av informationssäkerhetsrisker fastställas som baseras på en bedömning av sannolikheter och konsekvenser. Dessutom bör kriterier för riskacceptans fastställas.

Efter fastställandet av kriterier för att bedöma informationssäkerhetsriskernas konsekvenser och sannolikhet bör organisationen också fastställa en metod för att kombinera dessa för att bestämma en risknivå. Konsekvenser och sannolikheter kan uttryckas kvalitativt, kvantitativt eller delvis kvantitativt.

Det bör noteras att kriterierna för riskacceptans avser aktiviteter för riskbedömning (i utvärderingsfasen, när organisationen bör avgöra om en risk är acceptabel eller inte), och riskbehandling (när organisationen bör avgöra om den föreslagna riskbehandlingen är tillräcklig för att uppnå en acceptabel risknivå).

Kriterier för riskacceptans kan baseras på en maximal acceptabel risknivå, på överväganden om förhållandet mellan kostnad och nytta eller på konsekvenser för organisationen.

Kriterierna för riskacceptans bör godkännas av den ansvariga ledningen.

Vägledning om att generera konsekventa, tillförlitliga och jämförbara bedömningsresultat (6.1.2 b))

Riskbedömningsprocessen bör baseras på metoder och verktyg som är tillräckligt detaljerade så att den leder till konsekventa, tillförlitliga och jämförbara resultat.

Oavsett vilken metod som väljs bör processen för bedömning av informationssäkerhetsrisker säkerställa att:

- alla risker beaktas på den detaljnivå som krävs,
- dess resultat är konsekventa och reproducerbara (dvs. identifiering, analys och utvärdering av risker kan förstås av personer som ej deltagit i analysen och resultaten blir identiska när olika personer bedömer riskerna i detta sammanhang),
- resultaten av upprepade riskbedömningar är jämförbara (dvs. det går att förstå om risknivåerna har ökat eller minskat).

Inkonsekvenser eller skillnader i resultat när hela eller en del av processen för bedömning av informationssäkerhetsrisker upprepas kan tyda på att den valda riskbedömningsmetoden inte är lämplig.

Vägledning om identifiering av informationssäkerhetsrisker (6.1.2 c))

Riskidentifiering är processen att hitta, känna igen och beskriva risker. Detta innebär att identifiera riskkällor och händelser samt deras orsaker och potentiella konsekvenser.

Syftet med riskidentifiering är att generera en omfattande lista över risker som baseras på dessa händelser som kan möjliggöra, förbättra, förhindra, försämra, påskynda eller fördröja uppnåendet av informationssäkerhetsmålen.

Två metoder används ofta för att identifiera informationssäkerhetsrisker:

- En händelsebaserad metod utgående från generella källor till risk. Det kan röra sig om händelser som har skett i det förflutna eller som kan förväntas ske i framtiden. I det första fallet kan de omfatta historiska data, i det andra fallet kan de baseras på teoretiska analyser och expertutlåtanden.
- En metod som bygger på identifiering av tillgångar, hot och sårbarheter där två olika typer av riskkällor beaktas: tillgångar och deras sårbarheter samt hot. Potentiella händelser som beaktas här är sätt på vilka hot kan utnyttja en viss sårbarhet hos en tillgång för att påverka organisationens mål.

Båda metoderna överensstämmer med principerna och de allmänna riktlinjerna för riskbedömning i ISO 31000.

Andra metoder för riskidentifiering kan användas om de har visat sig vara lika praktiskt användbara och om de uppfyller kraven i 6.1.2 b)).

ANM. Den metod som bygger på tillgångar, hot och sårbarheter motsvarar den metod för identifiering av informationssäkerhetsrisker som krävs enligt 2005 års upplaga av ISO/IEC 27001 och är kompatibel med kraven i 2013 års version. Detta säkerställer att tidigare nedlagt arbete för att identifiera risker inte förloras.

Det rekommenderas inte att riskidentifieringen är alltför detaljerad i den första riskbedömningscykeln. Att ha en översiktlig men tydlig bild av informationssäkerhetsriskerna är mycket bättre än att inte ha någon bild alls.

Vägledning om analys av informationssäkerhetsriskerna (6.1.2 d))

Riskanalys syftar till att fastställa risknivån.

I ISO/IEC 27001 hänvisas det till ISO 31000 som en generell modell. Enligt ISO/IEC 27001 ska riskanalysen grunda sig på en konsekvensbedömning av en identifierad risk och man bör göra en bedömning av sannolikheten att dessa konsekvenser inträffar för att fastställa en risknivå.

Metoder för riskanalys baserad på sannolikhet och konsekvenser kan vara:

1) kvalitativa, baserade på en skala med kvalificerande attribut (t.ex. hög, medium, låg),

2) kvantitativa, baserade på en skala med numeriska värden (t.ex. kostnad, frekvens eller sannolikhet) eller

3) delvis kvantitativa, baserade på kvalitativa skalor med angivna värden.

Oavsett vilken metod för riskanalys som används bör graden av objektivitet beaktas.

Det finns flera metoder för riskanalys. Båda alternativen som nämns ovan (den händelsebaserade metoden och den metod som bygger på identifiering av tillgångar, hot och sårbarheter) kan vara lämpliga för analys av informationssäkerhetsrisker. Processerna för identifiering och analys av risker kan vara som mest effektiva när de utförs med hjälp av experter på de risker som diskuteras.

Vägledning om utvärdering av informationssäkerhetsriskerna (6.1.2 e))

Utvärdering av analyserade risker innebär att man använder organisationens beslutsprocesser för att jämföra den bedömda nivån för varje risk med de förutbestämda acceptanskriterierna för att bestämma alternativen för riskbehandling.

I detta sista steg i riskbedömningen kontrolleras om de risker som har analyserats i de föregående stegen kan accepteras enligt acceptanskriterierna som definieras i 6.1.2 a), eller behöver ytterligare behandling. Steget i 6.1.2 d) ger information om storleken på risken men ingen omedelbar information om hur skyndsamt alternativen för behandling av informationssäkerhetsrisker bör implementeras. Beroende på under vilka omständigheter som riskerna uppstår kan de ha olika prioriteringar vad gäller behandling. Därför bör detta steg utmynna i en förteckning över risker i prioritetsordning. Det är lämpligt att bevara ytterligare information om dessa risker som inhämtats vid riskidentifieringen och riskanalysen som stöd för beslut om riskbehandling.

Ytterligare information

ISO/IEC 27005 ger vägledning för bedömningar av informationssäkerhetsrisker.

6.1.3 Behandling av informationssäkerhetsrisker

Kravställd aktivitet

Organisationen fastställer och tillämpar en process för behandling av informationssäkerhetsrisker.

Förklaring

Behandlingen av informationssäkerhetsrisker är den övergripande processen för att välja alternativ för riskbehandling, fastställa lämpliga säkerhetsåtgärder för genomförandet av dessa alternativ, formulera en riskbehandlingsplan och få denna godkänd av riskägarna.

Organisationen bevarar dokumenterad information om alla steg i processen för behandling av informationssäkerhetsrisker (6.1.3 a) till f)) samt resultaten av dess tillämpning.

Vägledning

Vägledning om alternativ för behandling av informationssäkerhetsrisker (6.1.3 a))

Alternativen för riskbehandling är att:

a) undvika risken genom att besluta att inte inleda eller fortsätta med den verksamhet som ger upphov till risken eller genom att avlägsna riskkällan (t.ex. genom att stänga en e-handelsportal),

b) ta ytterligare risker eller öka risken för att kunna tillvarata en affärsmöjlighet (t.ex. genom att öppna en e-handelsportal),

c) modifiera risken genom att ändra sannolikheten (t.ex. genom att minska sårbarheterna) eller konsekvenserna (t.ex. genom att sprida tillgångar på flera fysiska eller logiska platser) eller båda,

d) dela risken med andra parter genom försäkringar, underleverantörer eller riskfinansiering,

e) behålla risken baserat på kriterierna för riskacceptans eller välgrundade beslut (t.ex. genom att bevara en e-handelsportal i befintligt skick).

Varje enskild risk bör behandlas i linje med informationssäkerhetsmålen genom ett eller flera av dessa alternativ, för att uppfylla kriterierna för riskacceptans.

Vägledning om fastställande av nödvändiga säkerhetsåtgärder (6.1.3 b))

Särskild uppmärksamhet bör ägnas åt att fastställa nödvändiga informationssäkerhetsåtgärder. Alla säkerhetsåtgärder bör fastställas baserat på de informationssäkerhetsrisker som tidigare bedömts. En organisation med bristfällig bedömning av informationssäkerhetsrisker har dåliga förutsättningar att välja informationssäkerhetsåtgärder.

Vid fastställandet av säkerhetsåtgärder bör följande säkerställas:

f) att alla nödvändiga säkerhetsåtgärder finns med och inga onödiga säkerhetsåtgärder väljs,

g) att nödvändiga säkerhetsåtgärder utformas så att de är tillräckligt breda och djupa.

Som en följd av ett dåligt val av säkerhetsåtgärder kan den föreslagna behandlingen av informationssäkerhetsrisker bli:

h) ineffektiv eller

i) icke ändamålsenlig och därmed olämpligt dyr.

För att säkerställa en effektiv och ändamålsenlig behandling av informationssäkerhetsrisker är det viktigt att kunna visa sambandet mellan de säkerhetsåtgärder som krävs och resultaten från processen för bedömning och behandling av informationssäkerhetsrisker.

Det kan vara nödvändigt att använda flera säkerhetsåtgärder för att uppnå den önskade behandlingen av informationssäkerhetsrisken. Om t.ex. möjligheten att ändra konsekvenserna av en viss händelse väljs kan det krävas säkerhetsåtgärder för att åstadkomma en snabb upptäckt av händelsen samt säkerhetsåtgärder för att hantera och återhämta sig från händelsen.

När organisationen fastställer säkerhetsåtgärder bör även hänsyn tas till säkerhetsåtgärder som krävs för tjänster från externa leverantörer, exempelvis applikationer, processer och funktioner. Vanligtvis hanteras dessa säkerhetsåtgärder genom införandet av informationssäkerhetskrav i avtalen med leverantörerna. Avtalen bör inkludera hur organisationen får information om i vilken utsträckning kraven uppfylls (t.ex. rätt till revision). Det kan finnas situationer där organisationen vill fastställa och beskriva detaljerade säkerhetsåtgärder som en del av sitt ledningssystem för informationssäkerhet (LIS) även om säkerhetsåtgärderna vidtas av externa leverantörer. Organisationen bör dock alltid överväga vilka säkerhetsåtgärder som behövs för leverantörer när den fastställer säkerhetsåtgärder för sitt ledningssystem för informationssäkerhet (LIS).

Vägledning om jämförande av säkerhetsåtgärderna med dem i bilaga A (6.1.3 c))

ISO/IEC 27001:2013, Bilaga A innehåller en omfattande lista över åtgärdsmål och säkerhetsåtgärder. Användare av detta dokument hänvisas till den allmänna förteckningen över säkerhetsåtgärder i ISO/IEC 27001:2013, Bilaga A för att säkerställa att inga nödvändiga säkerhetsåtgärder förbises. En jämförelse med ISO/IEC 27001:2013, Bilaga A kan också leda till identifiering av andra säkerhetsåtgärder än dem som har fastställts i 6.1.3 b) och som kan vara mer effektiva när det gäller att påverka informationssäkerhetsrisker.

Åtgärdsmål ingår implicit i valda säkerhetsåtgärder. Listan över åtgärdsmål och säkerhetsåtgärder i ISO/IEC 27001:2013, Bilaga A är inte uttömmande, och ytterligare åtgärdsmål och säkerhetsåtgärder bör läggas till efter behov.

Varje säkerhetsåtgärd i ISO/IEC 27001:2013, Bilaga A behöver inte ingå. De säkerhetsåtgärder i ISO/IEC 27001:2013, Bilaga A som inte bedöms bidra till att påverka riskerna bör uteslutas och en motivering för uteslutningen bör ges.

Vägledning för skapande av ett uttalande om tillämplighet (6.1.3 d))

Uttalandet om tillämplighet (SoA – statement of applicability) innehåller:

- alla nödvändiga säkerhetsåtgärder (i enlighet med 6.1.3 b) och 6.1.3 c)) samt för varje säkerhetsåtgärd:
  - motivering för att inkludera säkerhetsåtgärden och
  - huruvida säkerhetsåtgärden är införd eller inte (t.ex. helt införd, håller på att införas, ännu inte påbörjad),
- motivering för att utesluta någon av säkerhetsåtgärderna i ISO/IEC 27001:2013, Bilaga A.

Inkluderandet av en säkerhetsåtgärd motiveras av dess effekt på ändringen av informationssäkerhetsrisker. En hänvisning till resultatet av bedömningen av informationssäkerhetsrisker och riskbehandlingsplanen för informationssäkerhetsrisker bör vara tillräcklig, tillsammans med den påverkan av informationssäkerhetsrisken som förväntas genom de införda och nödvändiga säkerhetsåtgärderna.

En motivering för uteslutande av en säkerhetsåtgärd som finns i ISO/IEC 27001:2013, Bilaga A kan bestå av följande:

- Det har fastställts att säkerhetsåtgärden inte behövs för att genomföra de valda alternativen för behandling av informationssäkerhetsrisker.

- Den inte är tillämplig eftersom den ligger utanför omfattningen av ledningssystem för informationssäkerhet (LIS) (t.ex. ISO/IEC 27001:2013, A.14.2.7 Outsourcad utveckling är inte tillämplig om hela organisationens systemutveckling sker internt).

- Den har förebyggts genom en egen säkerhetsåtgärd (t.ex. kan ISO/IEC 27001:2013, A.8.3.1 Hantering av flyttbara lagringsmedier kan uteslutas om en egen säkerhetsåtgärd förhindrar användning av flyttbara lagringsmedier).

ANM. En egen säkerhetsåtgärd är en säkerhetsåtgärd som inte ingår i ISO/IEC 27001:2013, Bilaga A.

Ett uttalande om tillämplighet kan med fördel utformas som en tabell som innehåller alla 114 säkerhetsåtgärder från ISO/IEC 27001:2013, Bilaga A samt vid behov ytterligare säkerhetsåtgärder som inte nämns i denna förteckning. En kolumn i tabellen kan ange om en säkerhetsåtgärd är nödvändig för att genomföra alternativen för riskbehandling eller om den kan uteslutas. Kolumnen efter kan innehålla motiveringen för inkludering eller uteslutning av en säkerhetsåtgärd. En sista kolumn i tabellen kan indikera åtgärdens aktuella status. Ytterligare kolumner kan användas, t.ex. för information som inte krävs enligt ISO/IEC 27001 men som vanligtvis är användbar vid granskningar. Detta kan t.ex. röra sig om en mer detaljerad beskrivning av hur säkerhetsåtgärden införs eller en hänvisning till en mer detaljerad beskrivning och dokumenterad information eller regelverk som är relevant för införandet av säkerhetsåtgärden.

Även om det inte är ett särskilt krav enligt ISO/IEC 27001 kan organisationer finna det användbart att ange information om vilka personer som är ansvariga för de säkerhetsåtgärder som finns med i uttalandet om tillämplighet.

Vägledning om formulering av en plan för behandling av informationssäkerhetsrisker (6.1.3 e))

ISO/IEC 27001 specificerar inte hur planen för behandling av informationssäkerhetsrisker ska vara strukturerad eller vad den ska innehålla. Planen bör dock formuleras på grundval av utfallen från 6.1.3 a) till c). Planen bör således för varje behandlad risk innehålla dokumentation om:

- valda alternativ för behandling,

- nödvändiga säkerhetsåtgärder och

- implementeringsstatus.

Övrigt användbart innehåll kan vara:

- riskägare och

- förväntad kvarstående risk efter införandet av åtgärderna.

Om det enligt riskbehandlingsplanen krävs någon aktivitet bör den specificeras med information om ansvar och deadline (se även 6.2). En handlingsplan kan utgöras av förteckningen över dessa åtgärder.

Planen kan med fördel utformas som en tabell sorterad efter de risker som identifierats under riskbedömningen och som visar alla fastställda säkerhetsåtgärder.

Till exempel kan det finnas kolumner tabellen med namnen på de personer som ansvarar för säkerhetsåtgärderna. Ytterligare kolumner kan innehålla tidpunkt för säkerhetsåtgärdens införande, information om hur säkerhetsåtgärden (eller en process) är avsedd att fungera samt implementerings-status.

En förlust eller stöld av en mobiltelefon kan vara ett exempel. Konsekvenserna är förlust av tillgänglighet och potentiellt oönskat avslöjande av information. Om bedömningen av risken har visat att risknivån är oacceptabel kan organisationen besluta att ändra sannolikheten för eller konsekvenserna av risken.

För att ändra sannolikheten för förlust eller stöld av en mobiltelefon kan organisationen bestämma att en lämplig säkerhetsåtgärd är att införa regler för mobila enheter för att tvinga de anställda att ta hand om sina mobiltelefoner och regelbundet kontrollera att de inte har blivit av dem.

För att ändra konsekvenserna av förlust eller stöld av en mobiltelefon kan organisationen fastställa säkerhetsåtgärder, exempelvis:

- en incidenthanteringsprocess som kan användas för att anmäla förlusten,
- ett stöd för hantering av mobila enheter (MDM – Mobile Device Management) för att radera innehållet i telefonen om den går förlorad,
- en plan för säkerhetskopiering av mobila enheter för återställning av telefonens innehåll.

När organisationen förbereder sitt uttalande om tillämplighet (6.1.3 d)) kan den inkludera de valda säkerhetsåtgärderna (regler för mobila enheter och MDM) och motivera detta baserat på deras effekt på ändringen av sannolikheten för, och konsekvenserna av, förlust eller stöld av en mobiltelefon, vilket resulterar i minskad kvarstående risk.

Om dessa säkerhetsåtgärder jämförs med dem som anges i ISO/IEC 27001:2013, Bilaga A (6.1.3 c)), ser man att reglerna för mobila enheter överensstämmer med ISO/IEC 27001:2013, A.6.2.1, men ett stöd för hantering av mobila enheter (MDM) har ingen direkt motsvarighet och bör därför betraktas som en egen säkerhetsåtgärd. Om stödet för hantering av mobila enheter och andra säkerhetsåtgärder betraktas som nödvändiga i en organisations plan för behandling av informationssäkerhetsrisker bör de ingå i uttalandet om tillämplighet (se ”Vägledning för skapande av ett uttalande om tillämplighet” (6.1.3 d)).

Om organisationen vill minska risken ytterligare kan den med hänseende till ISO/IEC 27001:2013, A.9.1.1 (Regler för styrning av åtkomst) dra slutsatsen att den saknar regler för kontroll av åtkomst till mobiltelefoner och ändra sina regler för mobila enheter så att alla mobiltelefoner skyddas av en PIN-kod. Detta bör i så fall betraktas som ytterligare en säkerhetsåtgärd för ändring av konsekvenserna av förlust eller stöld av mobiltelefoner.

Vid utformningen av sin plan för behandling av informationssäkerhetsrisker (6.1.3 e)), bör organisationen sedan inkludera åtgärder för att införa regler och ett stöd för hantering av mobila enheter samt utse ansvariga personer och fastställa deadlines för dessa åtgärder.

Vägledning om att utverka riskägarnas godkännande (6.1.3 f))

När planen för behandling av informationssäkerhetsrisker formuleras bör organisationen få godkännande från riskägarna. Ett sådant godkännande bör baseras på fastställda kriterier för riskacceptans eller en särskild motivering i de fall avvikelser sker från dessa kriterier.

Inom ramen för sina ledningsprocesser bör organisationen dokumentera riskägarens godkännande av kvarstående risker och ledningens godkännande av planen.

Till exempel kan riskägarens godkännande dokumenteras genom en ändring av riskbehandlingsplanen som beskrivs i vägledningen för 6.1.3 e) genom kolumner för effekten av säkerhetsåtgärden, den kvarstående risken och riskägarens godkännande.

Ytterligare information

Mer information om riskbehandling finns i ISO/IEC 27005 och ISO 31000.

6.2 Informationssäkerhetsmål och planering för att uppnå dem

Kravställd aktivitet

Organisationen fastställer informationssäkerhetsmål för relevanta funktioner och nivåer och planerar hur dessa mål ska uppnås.

Förklaring

Informationssäkerhetsmålen bidrar till att uppfylla organisationens strategiska mål och informationssäkerhetspolicyn. Målen för ledningssystemet för informationssäkerhet (LIS) är således informationssäkerhetsmål för informationens konfidentialitet, riktighet och tillgänglighet. Informationssäkerhetsmålen bidrar också till att specificera och mäta prestandan hos informationssäkerhetsåtgärder och processer för informationssäkerhet i enlighet med informationssäkerhetspolicyn (se 5.2).

Organisationen planerar, upprättar och publicerar informationssäkerhetsmål för relevanta funktioner och nivåer.

Kraven i ISO/IEC 27001 angående informationssäkerhetsmål gäller alla informationssäkerhetsmål. Om informationssäkerhetspolicyn innehåller mål måste dessa mål uppfylla kriterierna i detta avsnitt. Om policyn innehåller ramar för fastställande av mål måste de mål som fastställs inom dessa ramar uppfylla kraven i detta avsnitt.

De krav som måste beaktas vid fastställandet av målen är de som bestäms i samband med punkterna Att förstå organisationen och dess förutsättningar (se 4.1) samt Att förstå intressenters behov och förväntningar (se 4.2).

Resultaten från riskbedömningar och riskbehandlingar används som underlag till den pågående granskningen av målen för att säkerställa att de fortfarande är lämpliga med hänsyn till organisationens förutsättningar.

Informationssäkerhetsmålen utgör underlag för riskbedömning: i kriterierna för riskacceptans och kriterierna för att utföra bedömningar av informationssäkerhetsrisker (se 6.1.2) beaktas informationssäkerhetsmålen så att risknivåerna är i linje med dessa.

Enligt ISO/IEC 27001 ska informationssäkerhetsmålen:

a) överensstämma med informationssäkerhetspolicyn,

b) vara mätbara om det är praktiskt möjligt (detta innebär att det är viktigt att kunna avgöra om ett mål har uppfyllts eller ej),

c) vara kopplade till tillämpliga informationssäkerhetskrav, och resultat från riskbedömning och riskbehandling,

d) kommuniceras och

e) uppdateras efter behov.

Organisationen bevarar dokumenterad information om informationssäkerhetsmålen.

När organisationen planerar för att uppnå sina informationssäkerhetsmål avgör den:

f) vad som ska göras,

g) vilka resurser som kommer att krävas,

h) vem som ska vara ansvarig,

i) när det ska vara genomfört och

j) hur resultaten ska utvärderas.

Ovanstående krav på planering är allmänna och gäller för alla planer som krävs enligt ISO/IEC 27001. Planer som en organisation kan beakta för ledningssystemet för informationssäkerhet (LIS) inkluderar:

- planer för att förbättra ledningssystemet för informationssäkerhet (LIS) enligt 6.1.1 och 8.1,
- planer för behandling av identifierade risker enligt 6.1.3 och 8.3,
- andra planer som betraktas som nödvändiga för att ledningssystemet för informationssäkerhet (LIS) ska fungera effektivt (t.ex. planer eller program för kompetensutveckling och ökad medvetenhet, kommunikation, utvärdering av prestanda, internrevisioner och ledningens genomgång).

Vägledning

Informationssäkerhetspolicyn bör innehålla informationssäkerhetsmålen eller tillhandahålla en ram för att fastställa dessa mål.

Informationssäkerhetsmål kan uttryckas på olika sätt. Målen bör uttryckas på lämpligt sätt för att uppfylla kravet på mätbarhet (om det är praktiskt möjligt) (ISO/IEC 27001:2013, 6.2 b)).

Till exempel kan informationssäkerhetsmålen uttryckas som:

- numeriska värden med tillhörande gränser, t.ex. ”överskrid ett visst gränsvärde” eller ”uppnå nivå 4”,
- mål för mätningar av informationssäkerhetsprestanda,
- mål för mätningar av ledningssystemet för informationssäkerhets (LIS) effektivitet (se 9.1),
- efterlevnad av ISO/IEC 27001,
- efterlevnad av ledningssystemet för informationssäkerhets (LIS) regelverk,
- behovet av att komplettera åtgärder och planer samt
- riskkriterier som måste uppfyllas.

Följande riktlinjer gäller för punkterna som tas upp i förklaringen:

- Se a) ovan. I informationssäkerhetspolicyn anges organisations krav på informationssäkerhet. Alla andra specifika krav för relevanta funktioner och nivåer bör vara förenliga med dessa krav. Om informationssäkerhetspolicyn innehåller informationssäkerhetsmål bör alla andra specifika informationssäkerhetsmål kopplas till kraven i informationssäkerhetspolicyn. Om informationssäkerhetspolicyn endast innehåller en ram för att fastställa mål bör denna ram följas och säkerställa att mer specifika mål kopplas till de mer allmänna målen.
- Se b) ovan. Alla mål kan inte mätas, men om målen görs mätbara underlättas uppnående och förbättring. Det är mycket önskvärt att kunna beskriva, kvalitativt eller kvantitativt, i vilken grad ett mål har uppfyllts. Till exempel för att vägleda prioriteringar av ytterligare insatser om målen inte uppfylls, eller ge förståelse för möjligheter till ökad effektivitet om målen överskrids. Det bör vara möjligt att förstå om de har uppnåtts eller inte, hur måluppfyllelsen avgörs, och om det är möjligt att avgöra graden av måluppfyllelse genom kvantitativa mätningar. I kvantitativa beskrivningar av objektiv måluppfyllelse bör det anges hur själva mätningen ska göras. Det kanske inte är möjligt att kvantitativt avgöra graden av uppfyllelse för alla mål. Enligt ISO/IEC 27001 ska mål vara mätbara om det är praktiskt möjligt.

- Se c) ovan. Informationssäkerhetsmålen bör anpassas till informationssäkerhetsbehoven. Därför bör resultaten från bedömningen och behandlingen av risker användas som underlag vid fastställandet av informationssäkerhetsmål.

- Se d) ovan. Informationssäkerhetsmålen bör kommuniceras till relevanta interna intressenter i organisationen. De kan också kommuniceras till externa intressenter, t.ex. kunder och övriga intressenter, i den mån dessa påverkas av och behöver känna till informationssäkerhetsmålen.

- Se e) ovan. Om informationssäkerhetsbehoven förändras över tid bör de informationssäkerhetsmål som är kopplade till dessa behov uppdateras i enlighet därmed. Uppdateringen av dessa mål bör kommuniceras enligt kraven i d), till interna och externa intressenter efter behov.

Organisationen bör planera hur den ska uppnå sina informationssäkerhetsmål. Organisationen kan använda valfri metod eller mekanism för att uppnå sina informationssäkerhetsmål. Det kan finnas en enstaka informationssäkerhetsplan, en eller flera projektplaner, eller åtgärder som ingår i andra organisationsplaner. Oavsett vilken form planeringen tar bör planerna som ett minimum omfatta (se punkterna f–j ovan):

- de aktiviteter som ska göras,

- de resurser som krävs för att utföra aktiviteterna,

- ansvarsområden,

- tidslinjer och milstolpar för aktiviteter samt

- metoder och mätningar för att utvärdera om resultaten uppnår målen, inklusive tidpunkter för dessa utvärderingar.

Enligt ISO/IEC 27001 ska alla organisationer bevara dokumenterad information om informationssäkerhetsmålen. Exempel på sådan dokumenterad information är:

- planer, program, åtgärder, resurser, ansvarsområden, tidsfrister och utvärderingsmetoder,

- krav, uppgifter, resurser, ansvarsområden, utvärderingsfrekvens och utvärderingsmetoder.

Ytterligare information

ANM. Begreppet ”risk” definieras som ’osäkerhetens effekt på mål’ (se ISO/IEC 27000:2016, 2.68).

7 Stöd

7.1 Resurser

Kravställd aktivitet

Organisationen fastställer och tillhandahåller resurser för att upprätta, införa, underhålla och ständigt förbättra ledningssystemet för informationssäkerhet (LIS).

Förklaring

Resurserna är en grundläggande förutsättning för alla former av aktiviteter. Några exempel på resurskategorier:

a) personer som är ansvariga för att aktiviteterna genomförs,

b) tid för att genomföra aktiviteter och tid att hinna utvärdera resultaten innan nästa steg tas,

c) ekonomiska resurser för att förvärva, utveckla och genomföra det som behövs,

d) information för att stödja beslut, mäta åtgärdernas prestanda och öka kunskapen samt

e) infrastruktur och andra medel som kan förvärvas eller byggas, såsom teknik, verktyg och material, oavsett om de är produkter av informationsteknik eller inte.

Dessa resurser ska överensstämma med behoven hos ledningssystemet för informationssäkerhet (LIS) och därmed anpassas vid behov.

Vägledning

Organisationen bör:

f) uppskatta de resurser som krävs för all verksamhet relaterad till ledningssystemet för informationssäkerhet (LIS) vad gäller kvantitet och kvalitet (kapacitet och förmåga),

g) anskaffa de resurser som behövs,

h) tillhandahålla resurserna,

i) säkerställa att resurserna tillhandahålls för alla processer inom ledningssystemet för informationssäkerhet (LIS) och särskilda aktiviteter,

j) se över de resurser som tillhandahålls i förhållande till behoven hos ledningssystemet för informationssäkerhet (LIS), och anpassa dem efter behov.

Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i dess ledningssystem (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

Ingen ytterligare information.

7.2 Kompetens

Kravställd aktivitet

Organisationen avgör kompetensen hos de personer som behövs för informationssäkerhetens prestanda, och säkerställer att dessa personer har rätt kompetens.

Förklaring

Kompetens är förmågan att tillämpa kunskap och färdigheter för att uppnå avsedda resultat. Den påverkas av kunskap, erfarenhet och visdom.

Kompetens kan vara specifik (t.ex. inom teknik eller särskilda områden såsom riskhantering) eller allmän (t.ex. mjuka färdigheter, tillförlitlighet och grundläggande tekniska och administrativa färdigheter).

Kompetensen avser personer som arbetar under organisationens kontroll. Detta innebär att kompetensen ska hanteras för personer som är anställda av organisationen och för andra personer efter behov.

Förvärv av högre eller ny kompetens och nya färdigheter kan uppnås både internt och externt genom erfarenhet, utbildning (t.ex. kurser, seminarier och workshoppar), handledning, inhyrning eller anlitande av utomstående personer.

För kompetens som endast behövs tillfälligt – för en viss aktivitet eller under en kort tid, t.ex. för att kompensera för en oväntad tillfällig brist på intern personal – kan organisationer hyra in eller anlita externa resurser, vars kompetens måste beskrivas och verifieras.

Vägledning

Organisationen bör:

a) fastställa den förväntade kompetensen för varje roll inom ledningssystemet för informationssäkerhet (LIS) och avgöra om den behöver dokumenteras (t.ex. genom en arbetsbeskrivning),

b) tilldela roller inom ledningssystemet för informationssäkerhet (LIS) (se 5.3) till personer med erforderlig kompetens antingen genom att:

   1) identifiera personer inom organisationen som har rätt kompetens (baserat på t.ex. deras utbildning, erfarenhet eller certifieringar),

   2) planera och vidta åtgärder för att få personer inom organisationen att erhålla rätt kompetens (t.ex. genom att ge anställda möjlighet att få utbildning, mentor eller andra arbetsuppgifter) eller

   3) anlita nya personer som har rätt kompetens (t.ex. genom kontraktering),

c) utvärdera effektiviteten hos åtgärderna i b) ovan,

EXEMPEL 1 Överväga om personer har förvärvat kompetens efter utbildningen.

EXEMPEL 2 Analysera kompetensen hos nyanställda eller kontrakterade personer när de har arbetat för organisationen en viss tid.

EXEMPEL 3 Kontrollera om planen för att förvärva nya personer har genomförts som förväntat.

d) kontrollera att personerna har rätt kompetens för sin roll och

e) säkerställa att kompetensen utvecklas efter behov och att den uppfyller förväntningarna.

Lämplig dokumenterad information krävs som bevis på kompetens. Organisationen bör därför behålla dokumentation om den nödvändiga kompetens som påverkar informationssäkerhetsprestandan och hur dessa kompetenskrav uppfylls av relevanta personer.

Ytterligare information

Ingen ytterligare information.

7.3 Medvetenhet

Kravställd aktivitet

Personer som arbetar inom eller åt organisationen görs medvetna om informationssäkerhetspolicyn, sina bidrag till ett väl fungerande ledningssystem för informationssäkerhet (LIS), fördelarna med att informationssäkerhetens prestanda förbättras och konsekvenserna av att kraven i ledningssystemet för informationssäkerhet (LIS) inte uppfylls.

Förklaring

Detta innebär att dessa personer måste ha nödvändig förståelse och motivation i förhållande till vad som förväntas av dem när det gäller informationssäkerhet.

För att betraktas som medvetna i detta sammanhang måste dessa personer veta, förstå, acceptera och

a) stödja de mål som anges i informationssäkerhetspolicyn och

b) följa reglerna för att korrekt utföra sina dagliga arbetsuppgifter till stöd för informationssäkerhet.

Dessutom behöver personer som arbetar inom eller åt organisationen också veta, förstå och acceptera konsekvenserna av att kraven i ledningssystemet för informationssäkerhet (LIS) inte uppfylls. Det kan röra sig om negativa konsekvenser för informationssäkerheten eller för personen själv.

Dessa personer måste vara medvetna om att det finns en informationssäkerhetspolicy och var det finns information om den. Många anställda i en organisation behöver inte känna till policyns innehåll i detalj. Istället behöver de veta, förstå, acceptera och uppfylla informationssäkerhetsmålen och de krav som härrör från de regler som påverkar deras roll inom organisationen. Dessa krav kan ingå i standarder eller rutiner som de förväntas följa för att göra sitt jobb.

Vägledning

Organisationen bör:

c) utarbeta ett program med specifika budskap fokuserade på respektive mottagare (t.ex. interna och externa personer),

d) inkludera behov och förväntningar rörande informationssäkerhet i material som syftar till att höja säkerhetsmedvetandet, samt i utbildningsunderlag om andra ämnen, i syfte att förtydliga behoven av informationssäkerhet i relevanta sammanhang,

e) utarbeta en plan för att kommunicera budskap med planerade intervall,

f) kontrollera kunskap och förståelse efter att aktiviteter för ökad medvetenhet genomförts samt slumpvis mellan planerade aktiviteter,

g) kontrollera huruvida personer agerar i enlighet med kommunicerade budskap och använda exempel på ”bra” och ”dåligt” beteende för att förstärka budskapet.

Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i dess ledningssystem (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

Ytterligare information om medvetenhet inom informationssäkerhetsområdet finns i ISO/IEC 27002:2013, 7.2.2.

7.4 Kommunikation

Kravställd aktivitet

Organisationen avgör behovet av intern och extern kommunikation som rör ledningssystemet för informationssäkerhet (LIS).

Förklaring

Kommunikation är en viktig process inom ett ledningssystem för informationssäkerhet (LIS). Adekvat kommunikation med interna och externa intressenter är nödvändig. (se 4.2).

Kommunikation kan vara mellan interna intressenter på alla nivåer i organisationen eller mellan organisationen och externa intressenter. Kommunikation kan initieras inom organisationen eller av en extern intressent.

Organisationer måste avgöra:

- vilket innehåll som behöver kommuniceras, t.ex. informationssäkerhetspolicy, informationssäkerhetsmål, informationssäkerhetsregelverk förändringar av dessa samt kunskap om informationssäkerhetsrisker, krav på leverantörer och information om informationssäkerhetens prestanda,
- den föredragna eller optimala tidpunkten för kommunikationsaktiviteter,
- vilka som ska involveras i kommunikationsaktiviteterna, och vilken målgruppen är för varje kommunikationsaktivitet,
- vem som ska initiera kommunikation, t.ex. kan ett visst innehåll kräva att kommunikationen initieras av en viss person eller organisation,
- vilka processer som driver eller initierar kommunikationsaktiviteter, och vilka processer som är föremål för eller påverkas av kommunikationsaktiviteter.

Kommunikation kan ske regelbundet eller efter behov. Den kan antingen vara proaktiv eller reaktiv.

Vägledning

Kommunikation bygger på processer, kanaler och protokoll. Dessa bör väljas för att säkerställa att det kommunicerade budskapet tas emot i sin helhet, förstås korrekt och i förekommande fall leder till lämpliga åtgärder.

Organisationer bör avgöra vilket innehåll som behöver kommuniceras, såsom:

a) planer för och resultat av riskhantering till intresserade parter vid behov, för identifiering, analys, utvärdering och behandling av risker,

b) informationssäkerhetsmål,

c) uppnådda informationssäkerhetsmål, t.ex. sådana som kan stärka organisationens ställning på marknaden (t.ex. ISO/IEC 27001-certifiering eller överensstämmelse med lagar om skydd av personuppgifter),

d) incidenter eller kriser, där transparens ofta är nyckeln för att bevara och öka förtroendet för organisationens förmåga att hantera sin informationssäkerhet och hantera oväntade situationer,

e) roller, ansvar och befogenheter,

f) information som utbyts mellan funktioner och roller i enlighet med krav från processerna inom ledningssystemet för informationssäkerhet (LIS),

g) ändringar av ledningssystemet för informationssäkerhet (LIS),

h) andra frågor som identifierats genom granskning av säkerhetsåtgärder och processer inom omfattningen för ledningssystemet för informationssäkerhet (LIS),

i) frågor (t.ex. uppmärksammande av incidenter eller kriser) som kräver kommunikation med tillsynsorgan eller andra intressenter,

j) förfrågningar eller annan kommunikation från externa parter såsom kunder, potentiella kunder, användare av tjänster eller myndigheter.

Organisationen bör identifiera kraven på kommunikation kring relevanta frågor:

k) Vem som får kommunicera externt och internt (t.ex. i särskilda fall såsom dataintrång), genom att tilldela specifika roller med lämplig behörighet. T.ex. kan personer med kommunikationsansvar ges behörighet för detta. T.ex. kan en informatör ansvara för den externa kommunikationen och den säkerhetsansvarige ansvara för den interna kommunikationen.

l) Kommunikationens utlösande faktorer eller frekvens (för t.ex. rapportering av en händelse utgör identifieringen av händelsen en utlösande faktor),

m) Innehållet i meddelandena till viktiga intressenter (t.ex. kunder, myndigheter, allmänheten, viktiga interna användare) vid händelser med allvarlig konsekvens. Kommunikationen kan bli mer effektiv om den baseras på meddelanden som är förberedda och godkända i förväg av personer på lämplig ledningsnivå som en del av kommunikationsplanering, incidenthantering eller kontinuitetshantering.

n) Kommunikationens avsedda mottagare; i vissa fall bör en förteckning upprättas (t.ex. för att kommunicera ändringar av tjänster eller vid kriser).

o) Kommunikationssätt och kommunikationskanaler. Vid kommunikation bör för ändamålet avsedda kommunikationssätt och kommunikationskanaler användas för att säkerställa att meddelandet är officiellt och har rätt behörighet. Kommunikationskanalerna bör tillgodose eventuella behov av att skydda konfidentialiteten och riktigheten hos den information som överförs.

p) En särskilt utformad process och metod för att säkerställa att meddelanden skickas och tas emot och blir korrekt förstådda.

Kommunikation bör klassificeras och hanteras i enlighet med organisationens krav.

Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i dess ledningssystem (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

Ingen ytterligare information.

7.5 Dokumenterad information

7.5.1 Allmänt

Kravställd aktivitet

Organisationen ser till att ledningssystemet för informationssäkerhet (LIS) innehåller dokumenterad information som krävs direkt enligt ISO/IEC 27001 och dokumenterad information som organisationen har bestämt är nödvändig för ett väl fungerande ledningssystem för informationssäkerhet (LIS).

Förklaring

Dokumenterad information behövs för att definiera och kommunicera mål, policy, riktlinjer, säkerhetsåtgärder, processer, rutiner rörande informationssäkerhet samt vad olika personer eller grupper av personer förväntas göra och hur de förväntas bete sig. Dokumenterad information behövs också för revisioner av ledningssystemet för informationssäkerhet och för att det ska förbli stabilt om personer med viktiga roller byts ut. Dokumenterad information behövs dessutom för att registrera

åtgärder, beslut samt resultat av processer inom ledningssystemet för informationssäkerhet och informationssäkerhetsåtgärder.

Dokumenterad information kan innehålla:

- information om mål, risker, krav och riktlinjer rörande informationssäkerhet
- information om processer och rutiner som ska följas samt
- dokumentation av underlag (t.ex. för ledningens genomgång) och resultat av processer (inklusive planer för, och resultat från, den operativa verksamheten).

Det finns mycket verksamhet inom ledningssystemet för informationssäkerhet (LIS) som genererar dokumenterad information som för det mesta används som insats för annan verksamhet.

Enligt ISO/IEC 27001 krävs en uppsättning obligatorisk dokumenterad information. Där finns också ett allmänt krav på att ytterligare dokumenterad information krävs om den är nödvändig för ett väl fungerande ledningssystem för informationssäkerhet (LIS).

Mängden dokumenterad information som behövs är ofta relaterad till organisationens storlek.

Totalt sett ska den obligatoriska och icke obligatoriska dokumenterade informationen vara tillräcklig för att möjliggöra en utvärdering av prestanda såsom det anges i avsnitt 9.

Vägledning

Organisationen ska avgöra vilken dokumenterad information, utöver den obligatoriska dokumenterade information som krävs enligt ISO/IEC 27001, som behövs för att säkerställa ett väl fungerande ledningssystem för informationssäkerhet (LIS).

Den dokumenterade informationen bör finnas för att passa ändamålet. Saklig och koncis information är vad som behövs.

Exempel på dokumenterad information som organisationen har bestämt är nödvändig för ett väl fungerande ledningssystem för informationssäkerhet (LIS) är:

- resultaten av fastställandet av organisationens förutsättningar (se avsnitt 4),
- roller, ansvar och befogenheter (se avsnitt 5),
- rapporter från riskhanteringens olika faser (se avsnitt 6),
- fastställda och tillhandahållna resurser (se 7.1),
- den förväntade kompetensen (se 7.2),
- planer och resultat från insatser för att öka medvetenheten (se 7.3),
- planer och resultat från kommunikationsinsatser (se 7.4),
- dokumenterad information av externt ursprung som är nödvändig för ledningssystemet för informationssäkerhet (LIS) (se 7.5.3),
- en process för styrning av dokumenterad information (se 7.5.3),
- policy och tillhörande regelverk för att styra och genomföra informationssäkerhetsaktiviteter,

- processer och rutiner som används för att införa, underhålla och förbättra ledningssystemet för informationssäkerhet (LIS) och den övergripande statusen rörande informationssäkerhet (se avsnitt 9),

- handlingsplaner samt

- bevis på resultaten från processer inom ledningssystemet för informationssäkerhet (LIS) (t.ex. incidenthantering, åtkomstkontroll, kontinuitetshantering, underhåll av utrustning etc.).

Dokumenterad information kan vara av internt eller externt ursprung.

Ytterligare information

Om organisationen vill hantera sin dokumenterade information i ett dokumenthanteringssystem kan detta skapas i enlighet med kraven i ISO 30301.

7.5.2 Skapande och uppdatering

Kravställd aktivitet

När dokumenterad information skapas och uppdateras ska organisationen säkerställa lämplig identifiering och beskrivning, lämpligt format och medium samt granskning och godkännande.

Förklaring

Organisationen identifierar i detalj hur den dokumenterade informationen ska struktureras på bästa sätt och fastställer en lämplig dokumentationsmetod.

Granskning och godkännande på lämplig ledningsnivå säkerställer att den dokumenterade informationen är korrekt, lämplig för ändamålet, i en lämplig form och på lämplig detaljnivå för den avsedda målgruppen. Regelbundna granskningar säkerställer fortsatt lämplighet och att den dokumenterade informationen är tillräcklig.

Vägledning

Dokumenterad information kan bevaras i valfri form, t.ex. traditionella dokument (både på papper och i elektronisk form), webbsidor, databaser, loggar, datorgenererade rapporter, ljud och video. Dokumenterad information kan också bestå av avsiktsspecifikationer (t.ex. informations-säkerhetspolicyn) eller uppgifter om prestanda (t.ex. resultaten av en revision) eller en blandning av båda. Följande riktlinjer har en direkt giltighet för traditionella dokument och bör tolkas på lämpligt sätt när de tillämpas på andra former av dokumenterad information.

Organisationer bör skapa ett strukturerat bibliotek med dokumenterad information och sammankoppla olika delar av dokumenterad information genom att:

a) fastställa strukturen på ramverket för dokumenterad information,

b) fastställa standardstrukturen på dokumenterad information,

c) tillhandahålla mallar för olika typer av dokumenterad information,

d) fastställa ansvarsområden för att förbereda, godkänna, publicera och hantera dokumenterad information samt

e) fastställa och dokumentera processen för revision och godkännande för att säkerställa kontinuerlig lämplighet och tillräcklighet.

Organisationer bör fastställa rutiner för dokumenterad information som innehåller gemensamma attribut för varje dokument och möjliggör en tydlig och unik identifikation. Dessa attribut omfattar vanligtvis dokumenttyp (t.ex. policy, direktiv, regel, riktlinje, plan, formulär, process eller rutin), syfte och omfattning, titel, datum för offentliggörande, klassificering, referensnummer, versionsnummer och en revisionshistorik. Identifieringen av författaren och de personer som för närvarande ansvarar för dokumentet, dess tillämpning och utveckling, samt de eller de personer som har godkänt dokumentet bör inkluderas.

Formatkrav kan omfatta fastställande av lämpliga dokumentationsspråk, filformat, programvaru-versioner för att arbeta med dem och grafiskt innehåll. Mediekraven definierar på vilka fysiska och elektroniska lagringsmedier informationen ska vara tillgänglig.

Uttalanden och formuleringar bör anpassas till målgruppen och dokumentationens omfattning.

Samma information bör helst inte förekomma på olika ställen i den dokumenterade informationen, och korsreferenser bör användas i stället för att upprepa samma information i olika dokument.

Rutinerna för dokumenterad information bör säkerställa att informationen revideras med jämna mellanrum och att alla ändringar godkänns. Lämpliga revisionskriterier kan vara tidsrelaterade (t.ex. maximala tidsperioder mellan revidering) eller innehållsrelaterade. Godkännandekriterier bör fastställas, vilket säkerställer att den dokumenterade informationen är korrekt, lämplig för ändamålet, i en lämplig form och på lämplig detaljnivå för den avsedda målgruppen.

Ytterligare information

Ingen ytterligare information.

7.5.3 Styrning av dokumenterad information

Kravställd aktivitet

Organisationen hanterar den dokumenterade informationen under hela dess livscykel och gör den tillgänglig där och när det behövs.

Förklaring

Efter godkännande av dokumenterad information kommuniceras den till målgruppen. Dokumenterad information är tillgänglig där och när den behövs, samtidigt som dess riktighet, konfidentialitet och relevans bevaras under hela livscykeln.

Observera att aktiviteter som ska utföras i ”tillämplig utsträckning” enligt ISO/IEC 27001:2013, 7.5.3 måste utföras om de kan och är användbara, med hänsyn till organisationens behov och förväntningar.

Vägledning

Ett strukturerat bibliotek med dokumenterad information kan användas för att underlätta tillgängligheten.

All dokumenterad information bör klassificeras (se ISO/IEC 27001:2013, A.8.2.1) i enlighet med organisationens klassificeringssystem. Dokumenterad information ska skyddas och hanteras i enlighet med sin klassificeringsnivå (se ISO/IEC 27001:2013, A.8.2.3).

En ändringshanteringsprocess för dokumenterad information bör säkerställa att endast behöriga personer har rätt att ändra och distribuera den efter behov på lämpliga och i förväg definierade sätt. Dokumenterad information bör skyddas för att säkerställa att den behåller sin giltighet och autenticitet.

Dokumenterad information bör distribueras och göras tillgänglig för behöriga intressenter. För detta ändamål bör organisationen fastställa vilka de relevanta intressenterna är för varje dokumenterad information (eller typ av dokumenterad information), och vilka sätt som ska användas för distribution, åtkomst, inhämtning och användning (t.ex. en webbplats med lämpliga mekanismer för åtkomstkontroll). Distributionen bör uppfylla alla krav som är kopplade till skydd och hantering av sekretessbelagd information.

Organisationen bör fastställa en lämplig arkiveringsperiod för dokumenterad information i enlighet med dess avsedda giltighet och andra relevanta krav. Organisationen bör säkerställa att informationen är läsbar under hela arkiveringsperioden (t.ex. genom att använda format som kan läsas av tillgänglig programvara eller kontrollera att papperet inte skadas).

Organisationen ska fastställa vad som ska göras med dokumenterad information efter att arkiveringstiden har löpt ut.

Organisationen bör också hantera dokumenterad information av externt ursprung (dvs. från kunder, partner, leverantörer, tillsynsmyndigheter etc.).

Dokumenterad information om denna aktivitet och dess resultat är kravställd endast i den form och utsträckning som organisationen bedömer vara nödvändig för effektiviteten i ledningssystemet för informationssäkerhet (LIS) (se ISO/IEC 27001:2013, 7.5.1 b)).

Ytterligare information

Ingen ytterligare information.

8 Verksamhet

8.1 Planering och styrning av verksamheten

Kravställd aktivitet

Organisationen planerar, inför och styr processer för att uppfylla informationssäkerhetskraven och uppnå sina informationssäkerhetsmål.

Organisationen bevarar den dokumenterade information som krävs för att ge tilltro till att processerna genomförs som planerat.

Organisationen styr planerade ändringar och granskar konsekvenserna av oavsiktliga ändringar, och ser till att outsourcade processer identifieras, definieras och styrs.

Förklaring

De processer som en organisation använder för att uppfylla kraven på informationssäkerhet planeras, och när de har införts ska organisationen styra dem, särskilt när ändringar behövs.

På grundval av planeringen av ledningssystemet för informationssäkerhet (LIS) (se 6.1 och 6.2) utför organisationen den planering av verksamheten och de aktiviteter som behövs för att införa de processer som krävs för att uppfylla informationssäkerhetskraven.

Processer för att uppfylla informationssäkerhetskraven inkluderar:

a) processer inom ledningssystemet för informationssäkerhet (LIS) (t.ex. ledningens genomgång, internrevision) och

b) processer som krävs för att genomföra planen för behandling av informationssäkerhetsrisker.

Genomförandet av planer leder till processer som fungerar och styrs.

Organisationen förblir i slutändan ansvarig för planering och styrning av eventuella outsourcade processer för att uppnå informationssäkerhetsmålen. Organisationen behöver således:

c) fastställa outsourcade processer under övervägande av informationssäkerhetsriskerna i samband med outsourcing och

d) säkerställa att outsourcade processer styrs (dvs. planeras, övervakas och granskas) på ett sätt som garanterar att de fungerar som avsett (även med tanke på informationssäkerhetsmålen och planen för behandling av informationssäkerhetsrisker).

Efter införandet hanterar, övervakar och granskar organisationen processerna för att säkerställa att de fortsätter att uppfylla de fastställda kraven när organisationen har förstått intressenternas behov och förväntningar (se 4.2).

Förändringar av ledningssystemet för informationssäkerhet (LIS) när systemet är i drift kan antingen planeras eller ske oavsiktligt. När organisationen gör ändringar av ledningssystemet för informationssäkerhet (LIS) (som ett resultat av planering eller oavsiktligt) bedömer den ändringarnas potentiella konsekvenser för att kontrollera eventuella negativa effekter.

Organisationen kan försäkra sig om ett effektivt genomförande av planerna genom att dokumentera aktiviteter och använda dokumenterad information som underlag till processer för utvärdering av prestanda enligt avsnitt 9. Organisationen fastställer därför vilken dokumenterad information som behöver bevaras.

Vägledning

De processer som har fastställts som ett resultat av planeringen enligt avsnitt 6 bör införas, drivas och styras i hela organisationen. Följande bör övervägas och införas:

e) processer som är specifika för hantering av informationssäkerhet (t.ex. riskhantering, incidenthantering, kontinuitetshantering, internrevisioner och ledningens genomgång),

f) processer som härrör från informationssäkerhetssäkerhetsåtgärder i planen för behandling av informationssäkerhetsrisker,

g) rapporteringsstrukturer (innehåll, frekvens, format, ansvarsområden etc.) inom området informationssäkerhet, exempelvis incidentrapporter, rapporter om att mäta uppfyllandet av informationssäkerhetsmål, rapporter om utförda aktiviteter etc.,

h) mötesstrukturer (frekvens, deltagare, syfte och tillstånd) inom området informationssäkerhet. Informationssäkerhetsaktiviteter bör samordnas av representanter från olika delar av organisationen med relevanta roller och funktioner för att hanteringen av informationssäkerheten ska bli effektiv.

För planerade ändringar bör organisationen:

i) planera införandet och tilldela uppgifter, ansvar, tidsfrister och resurser,

j) genomföra ändringar enligt planen,

k) övervaka genomförandet för att bekräfta att ändringarna genomförs enligt planen och

l) samla in och bevara dokumenterad information om genomförandet av ändringar som bevis på att de har genomförts som planerat (t.ex. med ansvar, tidsfrister, utvärderingar av effektivitet etc.).

För observerade oavsiktliga förändringar bör organisationen:

m) granska deras konsekvenser,

n) avgöra om eventuella negativa effekter redan har inträffat eller kan inträffa i framtiden,

o) planera och vidta åtgärder för att mildra eventuella negativa effekter vid behov,

p) samla in och bevara dokumenterad information om oavsiktliga förändringar och åtgärder för att mildra negativa effekter.

Om en del av organisationens funktioner eller processer har outsourcats till leverantörer ska organisationen:

q) fastställa alla relationer vid outsourcing

r) fastställa lämpliga gränssnitt till leverantörerna,

s) hantera frågor om informationssäkerhet i leverantörsavtal,

t) övervaka och granska leverantörers tjänster för att säkerställa att de utförs som avsett och att tillhörande säkerhetsrisker uppfyller organisationens kriterier för riskacceptans,

u) hantera ändringar av leverantörers tjänster efter behov.

Ytterligare information

Ingen ytterligare information.

8.2 Bedömning av informationssäkerhetsrisker

Kravställd aktivitet

Organisationen gör bedömningar av informationssäkerhetsrisker och bevarar dokumenterad information om resultaten från dessa.

Förklaring

Vid bedömningar av informationssäkerhetsrisker använder organisationen den process som definieras i 6.1.2. Dessa bedömningar görs antingen i enlighet med en plan som fastställts i förväg, eller som svar på betydande förändringar eller informationssäkerhetsincidenter. Resultaten av bedömningarna av informationssäkerhetsrisker bevaras i form av dokumenterad information som bevis på att processen i 6.1.2 har genomförts enligt definitionen.

Dokumenterad information från bedömningar av informationssäkerhetsrisker är avgörande för behandlingen av informationssäkerhetsrisker och värdefull för utvärdering av prestanda (se avsnitt 9).

Vägledning

Organisationer bör ha en plan för att genomföra planerade bedömningar av informationssäkerhetsrisker.

När betydande förändringar av ledningssystemet för informationssäkerhet (LIS) (eller dess förutsättningar) eller informationssäkerhetsincidenter har skett bör organisationen bestämma:

a) vilka av dessa förändringar eller incidenter som kräver ytterligare bedömning av informationssäkerhetsrisker och

b) utlösande faktorer för dessa bedömningar.

En bred bedömning av informationssäkerhetsrisker bör göras minst en gång per år. Riskidentifieringens detaljnivå bör ökas stegvis i ytterligare iterationer av bedömningen av informationssäkerhetsrisker i samband med den ständiga förbättringen av ledningssystemet för informationssäkerhet (LIS).

Ytterligare information

ISO/IEC 27005 ger vägledning för bedömningar av informationssäkerhetsrisker.

8.3 Behandling av informationssäkerhetsrisker

Kravställd aktivitet

Organisationen genomför planen för behandling av informationssäkerhetsrisker och bevarar dokumenterad information om resultaten av behandlingen av informationssäkerhetsrisker.

Förklaring

För att behandla informationssäkerhetsrisker måste organisationen genomföra processen för behandling av informationssäkerhetsrisker som definieras i 6.1.3. Varje gång riskbedömningen uppdateras enligt 8.1 genomför organisationen riskbehandlingen enligt 6.1.3 och uppdaterar riskbehandlingsplanen. Den uppdaterade riskbehandlingsplanen införs på nytt.

Resultaten av behandlingen av informationssäkerhetsrisker bevaras i form av dokumenterad information som bevis på att processen i 6.1.3 har genomförts enligt fastställd metod.

Vägledning

Inom den fastställda processen för riskbedömning och riskbehandling bör en ny behandling av informationssäkerhetsrisker utföras efter varje ny riskbedömning i enlighet med 8.2, eller när införandet av riskbehandlingsplanen eller delar av den misslyckas.

Införandet av planen för behandling av informationssäkerhetsrisker bör styras och övervakas genom denna aktivitet.

Ytterligare information

Ingen ytterligare information.

9 Utvärdering av prestanda

9.1 Övervakning, mätning, analys och utvärdering

Kravställd aktivitet

Organisationen utvärderar informationssäkerhetsprestandan och effektiviteten hos ledningssystemet för informationssäkerhet (LIS).

Förklaring

Syftet med övervakningen och mätningen är att hjälpa organisationen att bedöma huruvida det planerade resultatet av informationssäkerhetsaktiviteterna inklusive bedömning och behandling av risker uppnås.

Övervakning innebär att statusen hos ett system, en process eller en aktivitet bestäms, medan mätning är en process för att bestämma ett värde. Således kan övervakning åstadkommas genom en rad liknande mätningar under en viss tidsperiod.

För övervakning och mätning fastställer organisationen:

a) vad som ska övervakas och mätas,

b) vem som ska övervaka och mäta och när det ska göras,

c) vilka metoder som ska användas så att de genererar tillförlitliga resultat (dvs. jämförbara och reproducerbara).

För analys och utvärdering fastställer organisationen:

d) vem som ska analysera och utvärdera resultaten från övervakning och mätning och när detta ska ske,

e) vilka metoder som ska användas så att de genererar tillförlitliga resultat.

Det finns två aspekter av utvärderingen:

f) utvärdering av informationssäkerhetsprestandan för att avgöra om organisationen beter sig som väntat, vilket inkluderar att avgöra hur väl processerna inom ledningssystemet för informationssäkerhet (LIS) överensstämmer med kraven,

g) utvärdering av effektiviteten hos ledningssystemet för informationssäkerhet (LIS), för att avgöra om organisationen gör rätt saker, vilket inkluderar att avgöra i vilken utsträckning informationssäkerhetsmålen uppnås.

Observera att ”i tillämplig utsträckning” (ISO/IEC 27001:2013, 9.1, b)) innebär att metoder för övervakning, mätning, analys och utvärdering måste fastställas om detta är möjligt.

Vägledning

En god praxis är att definiera ”informationsbehovet” vid planering av övervakning, mätning, analys och utvärdering. Ett informationsbehov uttrycks vanligen som en fråga eller uttalande om informationssäkerhet som hjälper organisationen att utvärdera informationssäkerhetens prestanda och ledningssystem för informationssäkerhets (LIS) effektivitet. Med andra ord bör övervakning och mätning göras för att uppnå ett definierat informationsbehov.

Försiktighet bör iakttas vid fastställandet av de attribut som ska mätas. Det är praktiskt ogenomförbart, kostsamt och kontraproduktivt att mäta alltför många eller fel attribut. Förutom kostnaderna för att mäta, analysera och utvärdera många attribut finns det en möjlighet att viktiga frågor kan försvinna i mängden eller missas helt och hållet.

Det finns två generella typer av mätningar:

h) **prestandamätningar**, som uttrycker de planerade resultaten när det gäller egenskaperna hos den planerade aktiviteten, såsom antal anställda, uppnående av milstolpar, eller i vilken grad informationssäkerhetsåtgärder genomförs,

i) **effektivitetsmätningar**, som uttrycker vilken effekt realiseringen av de planerade aktiviteterna har på organisationens informationssäkerhetsmål.

Det kan vara lämpligt att identifiera och tilldela särskilda roller till dem som deltar i övervakning, mätning, analys och utvärdering. Dessa roller kan vara mätningsklient, mätningsplanerare, mätningsgranskare, informationsägare, informationssamlare, informationsanalytiker och kommunikatör för insatser och utfall av utvärdering (se ISO/IEC 27004:2016, 6.5).

Ansvaret för övervakning och mätning samt för analys och utvärdering tilldelas ofta separata personer med olika kompetens.

Ytterligare information

Övervakning, mätning, analys och utvärdering är avgörande för ett väl fungerande ledningssystem för informationssäkerhet (LIS). Det finns ett antal avsnitt i ISO/IEC 27001 som innehåller uttryckliga krav på utvärdering av vilken verkan vissa åtgärder har haft. Till exempel ISO/IEC 27001:2013, 6.1.1 e), 7.2 c) och 10.1 d).

Ytterligare information finns i ISO/IEC 27004, som ger vägledning om att uppfylla kraven i ISO/IEC 27001:2013, 9.1. Standarden innehåller närmare förklaringar av alla termer som nämns ovan, såsom roller, ansvar och former och ger många exempel.

9.2 Internrevision

Kravställd aktivitet

Organisationen genomför internrevisioner för att få information om i vilken utsträckning ledningssystemet för informationssäkerhet (LIS) överensstämmer med kraven.

Förklaring

Utvärderingen av ett ledningssystem för informationssäkerhet (LIS) med planerade intervall med hjälp av internrevisioner ger försäkran om statusen hos ledningssystemet för informationssäkerhet (LIS) till högsta ledningen. Revisionen kännetecknas av ett antal principer: integritet, opartisk rapportering, yrkesmässig noggrannhet, sekretess, oberoende samt angreppssätt baserat på belägg (se ISO 19011).

Internrevisioner ger information om huruvida ledningssystemet för informationssäkerhet (LIS) överensstämmer med ”organisationens egna krav” på sitt ledningssystem för informationssäkerhet (LIS) samt kraven i ISO/IEC 27001. Organisationens egna krav inkluderar:

a) krav som anges i organisationens policy och rutiner för informationssäkerhet,

b) krav som fastställs inom ramverket för att sätta informationssäkerhetsmål, inklusive resultaten från processen för behandling av risker,

c) juridiska och avtalsmässiga krav,

d) krav på dokumenterad information.

Revisorn utvärderar även om ledningssystemet för informationssäkerhet (LIS) har införts och underhållits på ett ändamålsenligt sätt.

Ett revisionsprogram beskriver den övergripande ramen för en eller flera revisioner planerade att utföras under en viss tidsperiod och för ett visst ändamål. Detta skiljer sig från en revisionsplan, som beskriver aktiviteter och arrangemang för en enskild revision. Revisionskriterier är en uppsättning policyer, rutiner eller krav som används som referens och som revisionsbelägg jämförs mot, dvs. revisionskriterierna beskriver det som revisorn räknar med ska finnas på plats.

En internrevision kan identifiera avvikelser, risker och möjligheter. Avvikelser hanteras enligt kraven i 10.1. Risker och möjligheter hanteras enligt kraven i 4.1 och 6.1.

Organisationen ska bevara dokumenterad information om revisionsprogram och revisionsresultat.

Vägledning

Hantering av ett revisionsprogram

Ett revisionsprogram definierar strukturen och ansvarsområden för planering, utförande, rapportering och uppföljning av enskild revisionsverksamhet. Det bör säkerställa att revisioner som genomförs är lämpliga, har rätt omfattning, minimerar påverkan på organisationens verksamhet och håller den nödvändiga revisionskvaliteten. Ett revisionsprogram bör också säkerställa kompetensen hos revisionsgrupper, lämpligt underhåll av revisionsdokument samt övervakning och granskning av revisionernas verksamhet, risker och verkan. Vidare bör ett revisionsprogram säkerställa att ledningssystemet för informationssäkerhet (LIS) (dvs. alla relevanta processer, funktioner och säkerhetsåtgärder) revideras inom en viss tidsram. Slutligen bör ett revisionsprogram innehålla dokumenterad

information om vilka typer av revisioner det rör sig om samt revisionernas varaktighet, platser, och tidsplan.

Omfattningen av och frekvensen för internrevisioner bör baseras på organisationens storlek och typ samt på ledningssystemet för informationssäkerhets (LIS) typ, funktionalitet, komplexitet och mognad (riskbaserad revision).

Effektiviteten hos genomförda säkerhetsåtgärder bör undersökas inom ramen för internrevisioner. Ett revisionsprogram bör utformas för att säkerställa att alla nödvändiga säkerhetsåtgärder omfattas och bör innefatta utvärdering av effektiviteten hos utvalda säkerhetsåtgärder över tiden. Viktiga säkerhetsåtgärder (enligt det riskbaserade revisionsprogrammet) bör ingå i varje revision medan säkerhetsåtgärder som genomförs för att hantera lägre risker kan revideras mindre ofta.

I revisionsprogrammet bör man också beakta att processer och säkerhetsåtgärder bör ha använts en viss tid för att det ska vara möjligt att utvärdera lämpliga belägg.

Interna revisioner av ett ledningssystem för informationssäkerhet (LIS) kan med fördel utföras som en del av, eller i samarbete med, organisationens övriga internrevisioner. Revisionsprogrammet kan inkludera revisioner kopplade till en eller flera standarder för ledningssystem, som genomförs som separata eller kombinerade revisioner.

Ett revisionsprogram bör omfatta dokumenterad information om: revisionskriterier, revisionsmetoder, val av revisionsgrupper, processer för hantering av konfidentialitet, informationssäkerhet, hälsa och säkerhet samt andra liknande frågor.

Kompetens och utvärdering av revisorer

När det gäller kompetens och utvärdering av revisorer ska organisationen

e) identifiera kompetenskrav för sina revisorer,

f) välja interna eller externa revisorer med lämplig kompetens,

g) ha en process för att övervaka prestandan hos revisorer och revisionsgrupper,

h) i interna revisionsgrupper inkludera personal som har lämplig sektorsspecifik kunskap och kunskap om informationssäkerhet.

Revisorer som väljs bör vara kompetenta, oberoende och ha lämplig utbildning.

Det kan vara svårt för mindre företag att välja interna revisorer. Om de resurser och den kompetens som krävs inte finns inom organisationen bör externa revisorer utses. När organisationer använder externa revisorer bör de säkerställa att revisorerna har eller kan förvärva tillräcklig kunskap om organisationens förutsättningar. Denna information bör tillhandahållas av intern personal.

Organisationer bör beakta att anställda som agerar som interna revisorer kan ha möjlighet att utföra detaljerade revisioner med tanke på organisationens förutsättningar, men kanske inte har tillräcklig kunskap om hur revisioner ska utföras.

Organisationer bör då beakta egenskaper och potentiella brister hos interna och externa revisorer och skapa lämpliga revisionsgrupper med nödvändig kunskap och kompetens.

Utförande av revisionen

När revisionen utförs bör ledaren för revisionsgruppen utarbeta en revisionsplan under beaktande av resultaten från tidigare revisioner och behovet av att följa upp tidigare rapporterade avvikelser och

oacceptabla risker. Revisionsplanen bör bevaras som dokumenterad information och bör innehålla revisionens kriterier, omfattning och metoder.

Revisionsgruppen bör granska:

- lämplighet och verkan hos processer och fastställda säkerhetsåtgärder,
- uppfyllande av informationssäkerhetsmål,
- efterlevnaden av kraven i ISO/IEC 27001:2013, avsnitt 4–10,
- efterlevnaden av organisationens egna krav på informationssäkerhet,
- i vilken mån uttalandet om tillämplighet överensstämmer med resultatet av processen för behandling av informationssäkerhetsrisker,
- i vilken mån den faktiska planen för behandling av informationssäkerhetsrisker överensstämmer med de identifierade bedömda riskerna och kriterierna för riskacceptans,
- relevansen (med tanke på organisationens storlek och komplexitet) hos insatser och utfall i samband med ledningens genomgång,
- hur utfallen av ledningens genomgång (inklusive förbättringsbehov) påverkar organisationen.

Omfattningen och tillförlitligheten hos den övervakning av säkerhetsåtgärdernas verkan som sker inom ramen för ledningssystemet för informationssäkerhet (LIS) (se 9.1) kan göra det möjligt för revisorerna att minska sina egna utvärderingsansträngningar, förutsatt att de har bekräftat mätmetodernas verkan.

Om resultatet av revisionen innefattar avvikelser bör organisationen utarbeta en handlingsplan för varje avvikelse som ska godkännas av revisionsgruppens ledare. En uppföljande handlingsplan innehåller vanligtvis:

i) beskrivning av den upptäckta avvikelsen,

j) beskrivning av orsaken eller orsakerna till avvikelsen,

k) beskrivning av kortsiktiga korrigeringar och långsiktiga korrigerande åtgärder för att eliminera en upptäckt avvikelse inom en viss tidsram,

l) vilka personer som ansvarar för att genomföra planen.

Revisionsrapporter inklusive revisionsresultat bör distribueras till högsta ledningen.

Resultat från tidigare revisioner bör granskas och revisionsprogrammet justeras för att bättre kunna hantera områden med högre risk på grund av avvikelser.

Ytterligare information

Ytterligare information finns i ISO 19011, som innehåller allmän vägledning om revision av ledningssystem inklusive revisionsprinciper, ledning av revisionsprogram och genomförande av revisioner av ledningssystem. Den ger också vägledning om bedömning av kompetensen hos de personer eller grupper av personer som deltar i revisionen, inklusive den person som leder revisionsprogrammet, revisorer och revisionsgrupper.

Utöver den vägledning som finns i ISO 19011 finns dessutom ytterligare information i:

a) ISO/IEC 27007, som innehåller specifik vägledning om hantering av ett revisionsprogram för ledningssystem för informationssäkerhet (LIS), om genomförandet av revisioner, och om kompetensen hos revisorer för ledningssystem för informationssäkerhet (LIS),

b) ISO/IEC/TR 27008[1], som innehåller vägledning för bedömning av informationssäkerhetsåtgärder.

9.3 Ledningens genomgång

Kravställd aktivitet

Högsta ledningen går igenom ledningssystemet för informationssäkerhet (LIS) vid planerade intervall.

Förklaring

Syftet med ledningens genomgång är att säkerställa ledningssystemet för informationssäkerhets (LIS) fortsatta lämplighet, tillräcklighet och verkan. Lämplighet avser fortsatt överensstämmelse med organisationens mål. Tillräcklighet och verkan avser lämplig utformning och organisatorisk inbäddning av ledningssystemet för informationssäkerhet (LIS), liksom ett effektivt genomförande av processer och säkerhetsåtgärder som drivs av ledningssystemet för informationssäkerhet (LIS).

Sammantaget är ledningens genomgång en process som utförs på olika nivåer i organisationen. Dessa aktiviteter kan variera från dagliga, veckovisa eller månadsvisa möten hos organisationsenheter till enkla diskussioner om rapporter. Högsta ledningen är ytterst ansvarig för ledningens genomgång, med insatser från alla nivåer i organisationen.

Vägledning

Högsta ledningen bör kräva och regelbundet granska rapportering om prestandan hos ledningssystemet för informationssäkerhet (LIS).

Det finns många sätt på vilka ledningen kan granska ledningssystemet för informationssäkerhet (LIS), såsom att ta emot och granska mätningar och rapporter, elektronisk kommunikation, muntliga uppdateringar. Viktiga underlag är resultaten av de informationssäkerhetsmätningar som beskrivs i 9.1 och resultaten av de interna granskningar som beskrivs i 9.2 samt resultat från riskbedömningar och riskbehandlingsplanens status. Vid granskning av resultaten av bedömningar av informationssäkerhetsrisker och statusen hos planen för behandling av informationssäkerhetsrisker, bör ledningen bekräfta att kvarstående risker uppfyller kriterierna för riskacceptans och att riskbehandlingsplanen tar upp alla relevanta risker och deras behandlingsalternativ.

Sammantaget bör alla aspekter av ledningssystemet för informationssäkerhet (LIS) granskas av ledningen med planerade intervall, minst en gång per år, genom skapande av lämpliga tidsplaner och punkter på dagordningen vid ledningsmöten. Nya eller mindre mogna ledningssystem för informationssäkerhet (LIS) bör granskas oftare av ledningen för att främja ökad effektivitet.

Ledningens genomgång ska behandla följande ämnen:

a) status för åtgärder som beslutats vid ledningens tidigare genomgångar,

b) förändringar i externa och interna frågor (se 4.1) som är relevanta för ledningssystem för informationssäkerhet (LIS),

c) information om informationssäkerhetens prestanda, innefattande trender i fråga om:

[1] Andra utgåvan under utarbetande.

1) avvikelser och korrigerande åtgärder,

2) resultat från övervakning och mätning,

3) revisionsresultat,

4) uppfyllande av informationssäkerhetsmål.

d) återkoppling från intressenterna, inklusive förslag till förbättringar, begäran om förändring och klagomål,

e) resultat av bedömningar av informationssäkerhetsrisker och status för planen för behandling av informationssäkerhetsrisker,

f) möjligheter till ständig förbättring, inklusive effektivisering av både ledningssystemet för informationssäkerhet (LIS) och informationssäkerhetsåtgärder.

Underlag för ledningens genomgång bör vara på lämplig detaljnivå, i enlighet med de mål som fastställts för den del av ledningen som deltar i granskningen. Till exempel bör högsta ledningen endast utvärdera en sammanfattning av alla delar, enligt informationssäkerhetsmålen eller de övergripande målen.

Ledningens genomgång bör resultera i beslut som rör möjligheter till ständig förbättring och behov av ändringar i ledningssystemet för informationssäkerhet (LIS). Den kan också resultera i bevis på beslut om:

g) ändringar i informationssäkerhetspolicyn och informationssäkerhetsmålen, t.ex. drivna av ändringar i externa och interna frågor och krav från intressenterna,

h) ändringar av kriterierna för riskacceptans och kriterierna för att utföra bedömningar av informationssäkerhetsrisker (se 6.1.2),

i) vid behov åtgärder efter bedömning av informationssäkerhetsprestandan,

j) ändringar av resurserna, eller budgeten för, ledningssystemet för informationssäkerhet (LIS),

k) uppdateringar av planen för behandling av informationssäkerhetsrisker eller uttalandet om tillämplighet,

l) nödvändiga förbättringar av övervaknings- och mätningsverksamhet.

Dokumenterad information från ledningens genomgång krävs. Den bör bevaras som bevis på att man har beaktat (som ett minimum) alla de områden som anges i ISO/IEC 27001, även i de fall där det har beslutats att ingen åtgärd är nödvändig.

När flera ledningsgenomgångar görs på olika nivåer i organisationen bör dessa kopplas till varandra på ett lämpligt sätt.

Ytterligare information

Ingen ytterligare information.

10 Förbättringar

10.1 Avvikelser och korrigerande åtgärder

Kravställd aktivitet

Organisationen reagerar på avvikelser, utvärderar dem, gör korrigeringar och vidtar korrigerande åtgärder vid behov.

Förklaring

En avvikelse är en bristande uppfyllelse av ett krav inom ledningssystemet för informationssäkerhet (LIS). Krav är behov eller förväntningar som är angivna, underförstådda eller obligatoriska. Det finns flera olika typer av avvikelser såsom:

a) underlåtenhet att uppfylla ett krav (helt eller delvis) enligt ISO/IEC 27001 i ledningssystemet för informationssäkerhet (LIS),

b) underlåtenhet att korrekt genomföra eller uppfylla ett krav, en regel en eller säkerhetsåtgärd som anges i ledningssystemet för informationssäkerhet (LIS),

c) delvis eller total underlåtenhet att uppfylla juridiska, avtalsmässiga eller överenskomna kundkrav.

Avvikelser kan exempelvis vara:

d) personer som inte beter sig så som förväntas enligt policy och tillhörande regelverk,

e) leverantörer som inte tillhandahåller överenskomna produkter eller tjänster,

f) projekt som inte levererar förväntade resultat,

g) säkerhetsåtgärder som inte fungerar som tänkt.

Avvikelser kan kännas igen genom:

h) brister i aktiviteter som utförs inom ledningssystemets omfattning,

i) ineffektiva säkerhetsåtgärder som inte åtgärdas på lämpligt sätt,

j) analys av informationssäkerhetsincidenter som visar på icke-uppfyllande av ett krav enligt ledningssystemet för informationssäkerhet (LIS),

k) klagomål från kunder,

l) varningar från användare eller leverantörer,

m) övervakning och mätresultat som inte uppfyller acceptanskriterierna,

n) mål som inte uppnås.

Korrigeringar syftar till att omedelbart hantera avvikelsen och dess konsekvenser (10.1 a)).

Korrigerande åtgärder syftar till att eliminera orsaken till en avvikelse och förebygga dess upprepning (10.1 b) till g)).

Observera att ”i tillämplig utsträckning” (ISO/IEC 27001:2013, 10.1 a)) innebär att åtgärder för att styra och korrigera en avvikelse måste vidtas om detta är möjligt.

Vägledning

Informationssäkerhetsincidenter innebär inte nödvändigtvis att en avvikelse föreligger, men de kan vara en indikator på en avvikelse. Intern och extern revision samt kundklagomål är andra viktiga källor som kan bidra till att identifiera avvikelser.

Reaktionen på den avvikelsen bör baseras på en definierad hanteringsprocess. Processen bör innehålla:

- Identifikation av avvikelsens omfattning och konsekvenser.
- Beslut om korrigeringar för att begränsa avvikelsens konsekvenser. Korrigeringar kan t.ex. vara att byta till tidigare, felsäkra eller andra lämpliga tillstånd. Det är viktigt att säkerställa att korrigeringar inte förvärrar situationen.
- Kommunikation med berörd personal för att säkerställa att korrigeringarna genomförs.
- Genomförande av de korrigeringar som det beslutats om.
- Övervakning av situationen för att säkerställa att korrigeringarna har haft avsedd effekt och inte har resulterat i oavsiktliga bieffekter.
- Ytterligare åtgärder för att korrigera avvikelsen om den kvarstår.
- Kommunikation med andra relevanta intressenter efter behov.

Som ett övergripande resultat bör hanteringsprocessen leda till en hanterad status om avvikelsen och dess konsekvenser. Det är dock inte säkert att det räcker med enbart korrigeringar för att förhindra att avvikelsen upprepas.

Korrigerande åtgärder kan vidtas efter eller samtidigt med korrigeringar. Följande åtgärder bör vidtas:

1. Avgör om det finns ett behov av att vidta en korrigerande åtgärd, i enlighet med fastställda kriterier (t.ex. avvikelsens konsekvenser, tendens till upprepning etc.).
2. Gör en granskning av avvikelsen, med beaktande av:
   - om liknande avvikelser har noterats,
   - alla konsekvenser och bieffekter som härrör från avvikelsen,
   - de korrigeringar som gjorts.
3. Utför en fördjupad orsaksanalys av avvikelsen, med beaktande av:
   - vad som gick fel, den specifika utlösande faktor eller situation som ledde till avvikelsen (t.ex. den mänskliga faktorn, metoder, processer eller rutiner, hårdvara eller mjukvara, felaktiga mätningar, miljö),
   - mönster och kriterier som kan bidra till att identifiera liknande situationer i framtiden.
4. Gör en analys av de potentiella konsekvenserna för ledningssystemet för informationssäkerhet (LIS), med beaktande av:
   - om liknande avvikelser förekommer inom andra områden, t.ex. genom att använda de mönster och kriterier som identifierades under orsaksanalysen,
   - om andra områden motsvarar de identifierade mönstren eller kriterierna, så att det är bara en tidsfråga innan en liknande avvikelse inträffar.
5. Bestäm vilka åtgärder som behövs för att korrigera orsaken, bedöm om de står i proportion till avvikelsens konsekvenser och effekter och kontrollera att de inte har bieffekter som kan leda till andra avvikelser eller nya informationssäkerhetsrisker av betydande art,

6. Planera de korrigerande åtgärderna och prioritera om möjligt områden där det är högre sannolikhet för upprepningar och där avvikelsen har större konsekvenser. Planeringen bör inkludera vem som är ansvarig för den korrigerande åtgärden och en tidsfrist för genomförandet.

7. Vidta de korrigerande åtgärderna i enlighet med planen.

8. Bedöm de korrigerande åtgärderna för att avgöra om de faktiskt har hanterat orsaken till avvikelsen och om de har förhindrat att relaterade avvikelser uppstår. Denna bedömning bör vara opartisk och evidensbaserad, och den bör dokumenteras. Den bör också kommuniceras till lämpliga roller och intressenter.

Som ett resultat av korrigeringar och korrigerande åtgärder är det möjligt att nya möjligheter till förbättringar identifieras. Dessa bör tillvaratas på vederbörligt sätt (se 10.2).

Tillräcklig dokumenterad information måste bevaras för att det ska gå att visa att organisationen har agerat korrekt för att hantera avvikelsen och dess konsekvenser. Alla viktiga steg i hanteringen av avvikelsen (med början från upptäckt och korrigeringar) och hantering av korrigerande åtgärder (orsaksanalys, granskning, beslut om genomförande av åtgärder, granskning och ändring av beslut som fattats för själva ledningssystemet för informationssäkerhet (LIS)) bör dokumenteras. Den dokumenterade informationen behöver också innehålla bevis på huruvida de åtgärder som har vidtagits har fått avsedd effekt eller ej.

Vissa organisationer upprätthåller register för att dokumentera avvikelser och korrigerande åtgärder. Det kan finnas mer än ett register (t.ex. ett för varje funktionsområde eller process) och de kan finnas på olika medier (papper, fil, ett program etc.). Om så är fallet bör de betraktas och kontrolleras som dokumenterad information, och de bör möjliggöra en omfattande granskning av alla avvikelser och korrigerande åtgärder för att säkerställa en korrekt bedömning av behovet av åtgärder.

Ytterligare information

ISO/IEC 27001 innehåller inte uttryckligen några krav på ”förebyggande åtgärder”. Detta beror på att ett av de viktigaste syftena med ett formellt ledningssystem är att fungera som ett förebyggande verktyg. Följaktligen krävs enligt den gemensamma text som används i ISO-standarder för ledningssystem en bedömning av organisationens ”externa och interna frågor som är relevanta för dess syfte och som påverkar dess förmåga att nå de avsedda resultaten” i 4.1 som ska ”avgöra vilka risker och möjligheter som behöver hanteras för att: säkra att ledningssystemet för informationssäkerhet kan ge avsett resultat, förebygga eller minska oönskade effekter, och uppnå ständig förbättring” i 6.1. Dessa två uppsättningar av krav anses täcka in begreppet ”förebyggande åtgärder” och även inkludera en vidare syn på risker och möjligheter.

10.2 Ständig förbättring

Kravställd aktivitet

Organisationen förbättrar ständigt ledningssystemet för informationssäkerhets (LIS) lämplighet, tillräcklighet och verkan.

Förklaring

Organisationer och deras förutsättningar är aldrig statiska. Dessutom förändras riskerna för informationssystemen, och de sätt på vilka de kan äventyras, snabbt. Slutligen finns det inget ledningssystem för informationssäkerhet (LIS) som är perfekt; det finns alltid sätt som det kan förbättras på, även om organisationen och dess förutsättningar inte förändras.

Som ett exempel på förbättringar som inte är kopplade till avvikelser eller risker kan bedömningen av en beståndsdel av ledningssystemet för informationssäkerhet (LIS) (vad gäller lämplighet, tillräcklighet och

verkan) visa att den överskrider kraven i ledningssystemet för informationssäkerhet (LIS) eller saknar verkan. Om den gör det kan det finnas en möjlighet att förbättra ledningssystemet för informationssäkerhet (LIS) genom att ändra den bedömda beståndsdelen.

Ett systematiskt tillvägagångssätt med ständig förbättring kommer att leda till ett effektivare ledningssystem för informationssäkerhet (LIS), som kommer att förbättra organisationens informationssäkerhet. Ledningssystemet för informationssäkerhet (LIS) leder organisationens operativa verksamhet i syfte att undvika att organisationen blir alltför reaktiv, dvs. att de flesta av resurserna används för att hitta problem och hantera dessa problem. Ledningssystemet för informationssäkerhet (LIS) arbetar systematiskt genom ständig förbättring så att organisationen kan få ett mer proaktivt förhållningssätt. Högsta ledningen kan fastställa mål för ständig förbättring, t.ex. genom mätningar av verkan, kostnad eller processmognad.

Som en följd av detta ser organisationen på sitt ledningssystem för informationssäkerhet (LIS) som en lärande och levande del av verksamheten som är under ständig utveckling. För att ledningssystemet för informationssäkerhet (LIS) ska kunna hålla jämna steg med förändringarna måste det utvärderas regelbundet med avseende på dess ändamålsenlighet, verkan och överensstämmelse med organisationens mål. Ingenting kan tas för givet och ingenting kan betraktas som att det inte behöver granskas bara för att det var tillräckligt bra när det infördes.

Vägledning

Ständig förbättring av ledningssystemet för informationssäkerhet (LIS) bör innebära att själva ledningssystemet för informationssäkerhet (LIS) och alla dess beståndsdelar bedöms med beaktande av interna och externa frågor (4.1), intressenternas krav (4.2) och resultaten av prestandautvärderingen (avsnitt 9). Bedömningen bör innehålla en analys av:

a) lämpligheten hos ledningssystemet för informationssäkerhet (LIS), dvs. om externa och interna frågor, intressenternas krav, fastställda informationssäkerhetsmål och identifierade informationssäkerhetsrisker hanteras på rätt sätt genom planering och genomförande av ledningssystemet för informationssäkerhet (LIS) och informationssäkerhetsåtgärderna,

b) tillräckligheten hos ledningssystemet för informationssäkerhet (LIS), dvs. om processerna och informationssäkerhetsåtgärderna är förenliga med organisationens övergripande syften, aktiviteter och processer,

c) verkan hos ledningssystemet för informationssäkerhet (LIS), dvs. om de avsedda resultaten med ledningssystemet för informationssäkerhet (LIS) uppnås, om intressenternas krav uppfylls, om informationssäkerhetsriskerna hanteras för att uppfylla informationssäkerhetsmålen, om avvikelser hanteras samt om de resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra ledningssystemet för informationssäkerhet (LIS) står i proportion till dessa resultat.

Bedömningen kan också innehålla en analys av effektiviteten hos ledningssystemet för informationssäkerhet (LIS) och dess beståndsdelar, dvs. om resursanvändningen är lämplig, om det finns en risk för att bristande effektivitet kan leda till att ledningssystemet för informationssäkerhet (LIS) inte fungerar som det ska eller om det finns möjligheter att öka effektiviteten.

Förbättringsmöjligheter kan också identifieras vid hantering av avvikelser och korrigerande åtgärder.

När möjligheter till förbättringar identifieras bör organisationen enligt 6.1.1:

d) utvärdera dem för att fastställa om de är värda att genomföra,

e) avgöra vilka ändringar av ledningssystemet för informationssäkerhet (LIS) och dess beståndsdelar som krävs för att uppnå en förbättring,

f) planera och vidta åtgärder för att tillvarata möjligheterna och säkerställa att nyttoeffekterna realiseras samtidigt som inga avvikelser uppstår,

g) utvärdera om åtgärderna har gett avsedd verkan.

Dessa åtgärder bör betraktas som en del av de åtgärder för att hantera risker och möjligheter som beskrivs i 6.1.1.

Ytterligare information

Ingen ytterligare information.

Bilaga A
(informativ)
Policy och tillhörande regelverk

Bilaga A innehåller vägledning om strukturen för informationssäkerhetspolicyn och tillhörande regelverk.

I allmänhet är en policy ett uttalande om en organisations avsikter och inriktning, formellt uttalade av dess högsta ledning (se ISO/IEC 27000:2016, 2.84).

Innehållet i en policy fungerar som vägledning för åtgärder och beslut inom policyns ämne.

En organisation kan ha ett antal policyer, en för vart och ett av de verksamhetsområden som är viktiga för organisationen. Vissa policyer är oberoende av varandra, medan andra har en hierarkisk relation.

Normalt har en organisation en allmän policy, t.ex. en uppförandekod, på den högsta nivån i policy-hierarkin. Den allmänna policyn stöds av andra policyer som behandlar olika ämnen och kan tillämpas på vissa områden eller funktioner inom organisationen. Informationssäkerhetspolicyn är en av dessa specifika policyer.

Informationssäkerhetspolicyn stöds av en rad ämnesspecifika regler som är relaterade till olika aspekter av informationssäkerhet. Ett antal av dessa diskuteras i ISO/IEC 27002, t.ex. kan informations-säkerhetspolicyn stödjas av regler som rör åtkomstkontroll, klassning (och hantering) av information, fysisk och miljörelaterad säkerhet, slutanvändarorienterade ämnen etc. Ytterligare skikt av regler kan tillkomma. Detta arrangemang visas i figur A.1. Observera att organisationer använder olika uttryck för ämnesspecifika regeldokument, såsom ”riktlinjer”, ”vägledningar”, ”interna föreskrifter”, ”instruktioner”, ”rutiner” eller ”direktiv”.

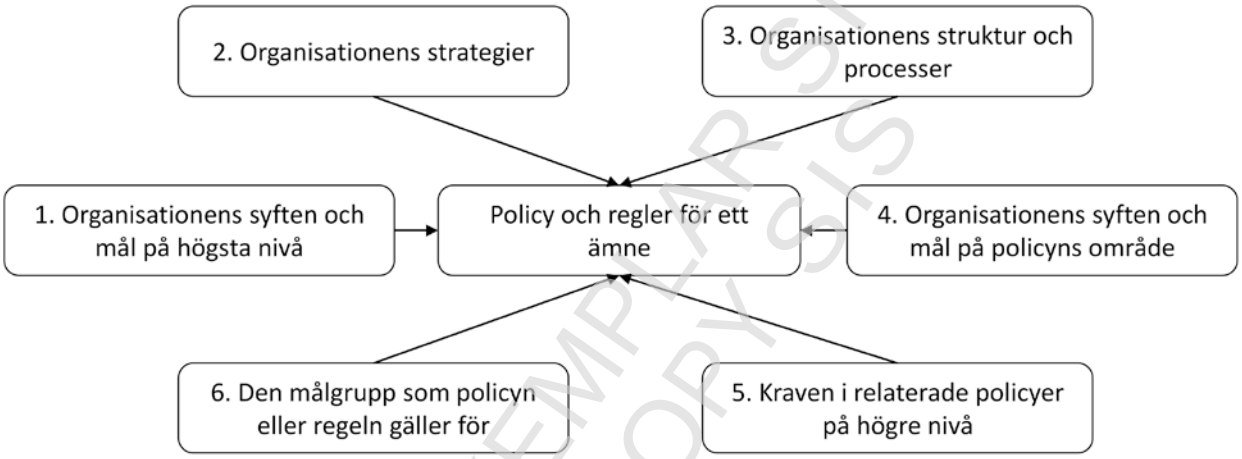
Figur A.1 – Hierarki över policy och regler

Enligt ISO/IEC 27001 måste alla organisationer ha en informationssäkerhetspolicy. Dock specificeras inte någon särskild relation mellan denna policy och andra regler i organisationen.

Informationssäkerhetspolicyns och tillhörande regelverks innehåll baseras på det sammanhang som en organisation verkar i. I synnerhet bör följande beaktas vid utarbetandet:

1. organisationens syften och mål,
2. strategier som antagits för att uppnå målen,
3. organisationens struktur och processer,
4. syften och mål kopplade till policyns ämne,
5. kraven i relaterade policyer på högre nivå,
6. den målgrupp som policyn eller regeln gäller för.

Detta visas i figur A.2.



Figur A.2 – Underlag för utvecklingen av en policy eller regel

Policy eller regler kan ha följande struktur:

a) Administrativa uppgifter – policyns eller regelns titel, version, publiceringsdatum, giltighetsdatum, ändringshistorik, ägare och godkännare, klassificering, målgrupp etc.

b) Sammanfattning av policyn eller regeln – en översikt bestående av en eller två meningar. (Denna del kan ibland slås ihop med introduktionen.)

c) Introduktion – en kort förklaring av policyns eller regelns ämne.

d) Omfattning – beskriver de delar eller aktiviteter hos en organisation som berörs av policyn eller regeln. Om det är relevant innehåller detta avsnitt en förteckning över andra policyer, regler eller andra dokument som stöds av policyn eller regeln.

e) Mål – beskriver policyns eller regelns syfte.

f) Principer – beskriver de regler som rör åtgärder och beslut för att uppnå målen. I vissa fall kan det vara lämpligt att identifiera de viktigaste processerna som är förknippade med policyns eller regelns ämne och sedan reglerna för hur processerna fungerar.

g) Ansvarsområden – Beskriver vilka personer som är ansvariga för åtgärder för att uppfylla kraven i policyn eller regeln. I vissa fall kan detta innefatta en beskrivning av organisatoriska arrangemang samt ansvar och befogenheter för personer som har tilldelats roller.

h) Viktiga resultat – beskriver vilka resultat det leder till för verksamheten om målen uppfylls. I vissa fall kan detta avsnitt slås ihop med avsnittet om mål.

i) Relaterade policyer eller regler – beskriver andra policyer, regler eller andra dokument som är relevanta för att uppnå målen, vanligen genom att tillhandahålla ytterligare detaljer om särskilda ämnen.

j) Policykrav eller regelkrav – beskriver policyns eller regelns detaljerade krav.

Policyns eller regelns innehåll kan organiseras på många olika sätt. Till exempel kan organisationer som lägger tyngdpunkten på roller och ansvar förenkla beskrivningen av målen och tillämpa principerna specifikt på beskrivningen av ansvarsområden.

Litteraturförteckning

[1] ISO 19011, *Guidelines for auditing management systems*

Svensk ANM. Denna standard är översatt och fastställd som svensk standard SS-EN ISO 19011:2011, utgåva 2, *Vägledning för revision av ledningssystem (ISO 19011:2011)*.

[2] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

Svensk ANM. Denna standard är översatt och fastställd som svensk standard SS-ISO/IEC 27002:2014, utgåva 2, *Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2013, IDT).*

[3] ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management system implementation guidance*

Svensk ANM. Denna standard är översatt och fastställd som svensk standard SS-ISO/IEC 27003:2010, utgåva 1, *Informationsteknik – Säkerhetstekniker – Vägledning för införande av ledningssystem för informationssäkerhet (ISO/IEC 27003:2010, IDT).*

[4] ISO/IEC 27004:2016, *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*

Svensk ANM. Denna standard är fastställd som svensk standard SS-ISO/IEC 27004:2017, utgåva 2, *Informationsteknik – Säkerhetstekniker – Styrning av informationssäkerhet – Mätning (ISO/IEC 27004:2016, IDT).*

[5] ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*

Svensk ANM. Denna standard är översatt och fastställd som svensk standard SS-ISO/IEC 27005:2013, utgåva 2, *Informationsteknik – Säkerhetstekniker – Riskhantering för informationssäkerhet (ISO/IEC 27005:2011, IDT).*

[6] ISO/IEC 27007, *Information technology – Security techniques – Guidelines for information security management systems auditing*

[7] ISO/IEC/TR 27008[2], *Information technology – Security techniques – Guidelines for auditors on information security controls*

Svensk ANM. Den första utgåvan av denna standard är översatt och fastställd som svensk standard SIS-ISO/IEC TR 27008:2013, utgåva 1, Informationsteknik – *Säkerhetstekniker – Vägledning om säkerhetsåtgärder för revisorer (ISO/IEC TR 27008:2011, IDT).*

[8] ISO 30301, *Information and documentation – Management systems for records – Requirements*

Svensk ANM. Denna standard är översatt och fastställd som svensk standard SS-ISO 30301:2011, utgåva 1, *Information och dokumentation – Ledningssystem för verksamhetsinformation – Krav (ISO 30301:2011, IDT).*

[2] Andra utgåvan under utarbetande.

[9] ISO 31000, *Risk management – Principles and guidelines*

Svensk ANM. Denna standard är översatt och fastställd som svensk standard SS-ISO 31000:2009, utgåva 1, *Riskhantering – Principer och riktlinjer (ISO 31000:2009, IDT)*.

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.

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).

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition of ISO/IEC 27003 cancels and replaces the first edition (ISO/IEC 27003:2010), of which it constitutes a minor revision.

The main changes compared to the previous edition are as follows:

— the scope and title have been changed to cover explanation of, and guidance on the requirements of, ISO/IEC 27001:2013 rather than the previous edition (ISO/IEC 27001:2005);

— the structure is now aligned to the structure of ISO/IEC 27001:2013 to make it easier for the user to use it together with ISO/IEC 27001:2013;

— the previous edition had a project approach with a sequence of activities. This edition instead provides guidance on the requirements regardless of the order in which they are implemented.

Introduction

This document provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them. It is not the intention of this document to provide general guidance on all aspects of information security.

Clauses 4 to 10 of this document mirror the structure of ISO/IEC 27001:2013.

This document does not add any new requirements for an ISMS and its related terms and definitions. Organizations should refer to ISO/IEC 27001 and ISO/IEC 27000 for requirements and definitions. Organizations implementing an ISMS are under no obligation to observe the guidance in this document.

An ISMS emphasizes the importance of the following phases:

— understanding the organization's needs and the necessity for establishing information security policy and information security objectives;

— assessing the organization's risks related to information security;

— implementing and operating information security processes, controls and other measures to treat risks;

— monitoring and reviewing the performance and effectiveness of the ISMS; and

— practising continual improvement.

An ISMS, similar to any other type of management system, includes the following key components:

a) policy;

b) persons with defined responsibilities;

c) management processes related to:

   1) policy establishment;

   2) awareness and competence provision;

   3) planning;

   4) implementation;

   5) operation;

   6) performance assessment;

   7) management review; and

   8) improvement; and

d) documented information.

An ISMS has additional key components such as:

e) information security risk assessment; and

f) information security risk treatment, including determination and implementation of controls.

This document is generic and intended to be applicable to all organizations, regardless of type, size or nature. The organization should identify which part of this guidance applies to it in accordance with its specific organizational context (see ISO/IEC 27001:2013, Clause 4).

For example, some guidance can be more suited to large organizations, but for very small organizations (e.g. with fewer than 10 persons) some of the guidance can be unnecessary or inappropriate.

The descriptions of Clauses 4 to10 are structured as follows:

— **Required activity**: presents key activities required in the corresponding subclause of ISO/IEC 27001;

— **Explanation**: explains what the requirements of ISO/IEC 27001 imply;

— **Guidance**: provides more detailed or supportive information to implement "required activity" including examples for implementation; and

— **Other information**: provides further information that can be considered.

ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005 form a set of documents supporting and providing guidance on ISO/IEC 27001:2013. Among these documents, ISO/IEC 27003 is a basic and comprehensive document that provides guidance for all the requirements of ISO/IEC 27001, but it does not have detailed descriptions regarding "monitoring, measurement, analysis and evaluation" and information security risk management. ISO/IEC 27004 and ISO/IEC 27005 focus on specific contents and give more detailed guidance on "monitoring, measurement, analysis and evaluation" and information security risk management.

There are several explicit references to documented information in ISO/IEC 27001. Nevertheless, an organization can retain additional documented information that it determines as necessary for the effectiveness of its management system as part of its response to ISO/IEC 27001:2013, 7.5.1 b). In these cases, this document uses the phrase "Documented information on this activity and its outcome is mandatory only in the form and to the extent that the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b))."

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

1 Scope

This document provides explanation and guidance on ISO/IEC 27001:2013.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2016 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

4 Context of the organization

4.1 Understanding the organization and its context

Required activity

The organization determines external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS).

Explanation

As an integral function of the ISMS, the organization continually analyses itself and the world surrounding it. This analysis is concerned with external and internal issues that in some way affect information security and how information security can be managed, and that are relevant to the organization's objectives.

Analysis of these issues has three purposes:

— understanding the context in order to decide the scope of the ISMS;

— analysing the context in order to determine risks and opportunities; and

— ensuring that the ISMS is adapted to changing external and internal issues.

External issues are those outside of the organization's control. This is often referred to as the organization's environment. Analysing this environment can include the following aspects:

a) social and cultural;

b) political, legal, normative and regulatory;

c) financial and macroeconomic;

d) technological;

e) natural; and

f) competitive.

These aspects of the organization's environment continually present issues that affect information security and how information security can be managed. The relevant external issues depend on the organization's specific priorities and situation.

For example, external issues for a specific organization can include:

g) the legal implications of using an outsourced IT service (legal aspect);

h) characteristics of the nature in terms of possibility of disasters such as fire, flood and earthquakes (natural aspect);

i) technical advances of hacking tools and use of cryptography (technological aspect); and

j) the general demand for the organization's services (social, cultural or financial aspects).

Internal issues are subject to the organization's control. Analysing the internal issues can include the following aspects:

k) the organization's culture;

l) policies, objectives, and the strategies to achieve them;

m) governance, organizational structure, roles and responsibilities;

n) standards, guidelines and models adopted by the organization;

o) contractual relationships that can directly affect the organization's processes included in the scope of the ISMS;

p) processes and procedures;

q) the capabilities, in terms of resources and knowledge (e.g. capital, time, persons, processes, systems and technologies);

r) physical infrastructure and environment;

s) information systems, information flows and decision making processes (both formal and informal); and

t) previous audits and previous risk assessment results.

The results of this activity are used in 4.3, 6.1 and 9.3.

Guidance

Based on an understanding of the organization's purpose (e.g. referring to its mission statement or business plan) as well as the intended outcome(s) of the organization's ISMS, the organization should:

— review the external environment to identify relevant external issues; and

— review the internal aspects to identify relevant internal issues.

In order to identify relevant issues, the following question can be asked: How does a certain category of issues (see a) to t) above) affect information security objectives? Three examples of internal issues serve as an illustration by:

Example 1 on governance and organizational structure (see item m)): When establishing an ISMS, already existing governance and organizational structures should be taken into account. As an example, the organization can model the structure of its ISMS based on the structure of other existing management systems, and can combine common functions, such as management review and auditing.

Example 2 on policy, objectives and strategies (see item l)): An analysis of existing policies, objectives and strategies, can indicate what the organization intends to achieve and how the information security objectives can be aligned with business objectives to ensure successful outcomes.

Example 3 on information systems and information flows (see item s)): When determining internal issues, the organization should identify, at a sufficient level of detail, the information flows between its various information systems.

As both the external and the internal issues will change over time, the issues and their influence on the scope, constraints and requirements of the ISMS should be reviewed regularly.

Documented information on this activity and its outcome is mandatory only in the form and to the extent that the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

In ISO/IEC 27000, the definition of "organization" has a note which states that: "The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private." Some of these examples are whole legal entities, whilst others are not.

There are four cases:

1) the organization is a legal or administrative entity (e.g. sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution whether incorporated or not, public or private);

2) the organization is a subset of a legal or administrative entity (e.g. part of a company, corporation, enterprise);

3) the organization is a set of a legal or administrative entities (e.g. a consortium of sole-traders, larger companies, corporations, firms); and

4) the organization is a set of subsets of legal or administrative entities (e.g. clubs, trade associations).

4.2 Understanding the needs and expectations of interested parties

Required activity

The organization determines interested parties relevant to the ISMS and their requirements relevant to information security.

Explanation

Interested party is a defined term (see ISO/IEC 27000:2016, 2.41) that refers to persons or organizations that can affect, be affected by, or perceive themselves to be affected by a decision or activity of the organization. Interested parties can be found both outside and inside the organization and can have specific needs, expectations and requirements for the organization's information security.

External interested parties can include:

a) regulators and legislators;

b) shareholders including owners and investors;

c) suppliers including subcontractors, consultants, and outsourcing partners;

d) industry associations;

e) competitors;

f) customers and consumers; and

g) activist groups.

Internal interested parties can include:

h) decision makers including top management;

i) process owners, system owners, and information owners;

j) support functions such as IT or Human Resources;

k) employees and users; and

l) information security professionals.

The results of this activity are used in 4.3 and 6.1.

Guidance

The following steps should be taken:

— identify external interested parties;

— identify internal interested parties; and

— identify requirements of interested parties.

As the needs, expectations and requirement of interested parties change over time, these changes and their influence on the scope, constraints and requirements of the ISMS should be reviewed regularly.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

No other information.

4.3 Determining the scope of the information security management system

Required activity

The organization determines the boundaries and applicability of the ISMS to establish its scope.

Explanation

The scope defines where and for what exactly the ISMS is applicable and where and for what it is not.

Establishing the scope is therefore a key activity that determines the necessary foundation for all other activities in the implementation of the ISMS. For instance, risk assessment and risk treatment, including the determination of controls, will not produce valid results without having a precise understanding of

where exactly the ISMS is applicable. Precise knowledge of the boundaries and applicability of the ISMS and the interfaces and dependencies between the organization and other organizations is critical as well. Any later modifications of the scope can result in considerable additional effort and costs.

The following factors can affect the determination of the scope:

a) the external and internal issues described in 4.1;

b) the interested parties and their requirements that are determined according to ISO/IEC 27001:2013,4.2;

c) the readiness of the business activities to be included as part of ISMS coverage;

d) all support functions, i.e. functions that are necessary to support these business activities (e.g. human resources management; IT services and software applications; facility management of buildings, physical zones, essential services and utilities); and

e) all functions that are outsourced either to other parts within the organization or to independent suppliers.

The scope of an ISMS can be very different from one implementation to another. For instance, the scope can include:

— one or more specific processes;

— one or more specific functions;

— one or more specific services;

— one or more specific sections or locations;

— an entire legal entity; and

— an entire administrative entity and one or more of its suppliers.

Guidance

To establish the scope of an ISMS, a multi-step approach can be followed:

f) determine the preliminary scope: this activity should be conducted by a small, but representative group of management representatives;

g) determine the refined scope: the functional units within and outside the preliminary scope should be reviewed, possibly followed by inclusion or exclusion of some of these functional units to reduce the number of interfaces along the boundaries. When refining the preliminary scope, all support functions should be considered that are necessary to support the business activities included in the scope;

h) determine the final scope: the refined scope should be evaluated by all management within the refined scope. If necessary, it should be adjusted and then precisely described; and

i) approval of the scope: the documented information describing the scope should be formally approved by top management.

The organization should also consider activities with impact on the ISMS or activities that are outsourced, either to other parts within the organization or to independent suppliers. For such activities, interfaces (physical, technical and organizational) and their influence on the scope should be identified.

Documented information describing the scope should include:

j) the organizational scope, boundaries and interfaces;

k) the information and communication technology scope, boundaries and interfaces; and

l) the physical scope, boundaries and interfaces.

Other information

No other information.

4.4 Information security management system

Required activity

The organization establishes, implements, maintains and continually improves the ISMS.

Explanation

ISO/IEC 27001:2013, 4.4 states the central requirement for establishing, implementing, maintaining and continually improving an ISMS. While the other parts of ISO/IEC 27001 describe the required elements of an ISMS, 4.4 mandates the organization to ensure that all required elements are met in order to establish, implement, maintain and continually improve the ISMS.

Guidance

No specific guidance.

Other information

No other information.

5 Leadership

5.1 Leadership and commitment

Required activity

Top management demonstrates leadership and commitment with respect to the ISMS.

Explanation

Leadership and commitment are essential for an effective ISMS.

Top management is defined (see ISO/IEC 27000) as a person or group of people who directs and controls the organization of the ISMS at the highest level, i.e. top management has the overall responsibility for the ISMS. This means that top management directs the ISMS in a similar way to other areas in the organization, for example the way budgets are allocated and monitored. Top management can delegate authority in the organization and provide resources for actually performing activities related to information security and the ISMS, but it still retains overall responsibility.

As an example, the organization implementing and operating the ISMS can be a business unit within a larger organization. In this case, top management is the person or group of people that directs and controls that business unit.

Top management also participates in management review (see 9.3) and promotes continual improvement (see 10.2).

Guidance

Top management should provide leadership and show commitment through the following:

a) top management should ensure that the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) top management should ensure that ISMS requirements and controls are integrated into the organization's processes. How this is achieved should be tailored to the specific context of the organization. For example, an organization that has designated process owners can delegate the responsibility to implement applicable requirements to these persons or group of people. Top management support can also be needed to overcome organizational resistance to changes in processes and controls;

c) top management should ensure the availability of resources for an effective ISMS. The resources are needed for the establishment of the ISMS, its implementation, maintenance and improvement, as well as for implementing information security controls. Resources needed for the ISMS include:

   1) financial resources;

   2) personnel;

   3) facilities; and

   4) technical infrastructure.

   The needed resources depend on the organization's context, such as the size, the complexity, and internal and external requirements. The management review should provide information that indicates whether the resources are adequate for the organization;

d) top management should communicate the need for information security management in the organization and the need to conform to ISMS requirements. This can be done by giving practical examples that illustrate what the actual need is in the context of the organization and by communicating information security requirements;

e) top management should ensure that the ISMS achieves its intended outcome(s) by supporting the implementation of all information security management processes, and in particular through requesting and reviewing reports on the status and effectiveness of the ISMS (see 5.3 b)). Such reports can be derived from measurements (see 6.2 b) and 9.1 a)), management reviews and audit reports. Top management can also set performance objectives for key personnel involved with the ISMS;

f) top management should direct and support persons in the organization directly involved with information security and the ISMS. Failing to do this can have a negative impact on the effectiveness of the ISMS. Feedback from top management can include how planned activities are aligned to the strategic needs for the organization and also for prioritizing different activities in the ISMS;

g) top management should assess resource needs during management reviews and set objectives for continual improvement and for monitoring effectiveness of planned activities; and

h) top management should support persons to whom roles and responsibilities relating to information security management have been assigned, so that they are motivated and able to direct and support information security activities within their area.

In cases where the organization implementing and operating an ISMS is part of a larger organization, leadership and commitment can be improved by engagement with the person or group of people that controls and directs the larger organization. If they understand what is involved in implementing an ISMS, they can provide support for top management within the ISMS scope and help them provide leadership and demonstrate commitment to the ISMS. For example, if interested parties outside the scope of the ISMS are engaged in decision making concerning information security objectives and risk criteria and are kept aware of information security outcomes produced by the ISMS, their decisions regarding resource allocations can be aligned to the requirements of the ISMS.

Other information

No other information.

5.2 Policy

Required activity

Top management establishes an information security policy.

Explanation

The information security policy describes the strategic importance of the ISMS for the organization and is available as documented information. The policy directs information security activities in the organization.

The policy states what the needs for information security are in the actual context of the organization.

Guidance

The information security policy should contain brief, high level statements of intent and direction concerning information security. It can be specific to the scope of an ISMS, or can have wider coverage.

All other policies, procedures, activities and objectives related to information security should be aligned to the information security policy.

The information security policy should reflect the organization's business situation, culture, issues and concerns relating to information security. The extent of the information security policy should be in accordance with the purpose and culture of the organization and should seek a balance between ease of reading and completeness. It is important that users of the policy can identify themselves with the strategic direction of the policy.

The information security policy can either include information security objectives for the organization or describe the framework for how information security objectives are set (i.e. who sets them for the ISMS and how they should be deployed within the scope of the ISMS). For example, in very large organizations, high level objectives should be set by the top management of the entire organization, then, according to a framework established in the information security policy, the objectives should be detailed in a way to give a sense of direction to all interested parties.

The information security policy should contain a clear statement from the top management on its commitment to satisfy information security related requirements.

The information security policy should contain a clear statement that top management supports continual improvement in all activities. It is important to state this principle in the policy, so that persons within the scope of the ISMS are aware of it.

The information security policy should be communicated to all persons within the scope of the ISMS. Therefore, its format and language should be appropriate so that it is easily understandable by all recipients.

Top management should decide to which interested parties the policy should be communicated. The information security policy can be written in such a way that it is possible to communicate it to relevant external interested parties outside of the organization. Examples of such external interested parties are customers, suppliers, contractors, subcontractors and regulators. If the information security policy is made available to external interested parties, it should not include confidential information.

The information security policy may either be a separate standalone policy or included in a comprehensive policy, which covers multiple management system topics within the organization (e.g. quality, environment and information security).

The information security policy should be available as documented information. The requirements in ISO/IEC 27001 do not imply any specific form for this documented information, and therefore is up to the organization to decide what form is most appropriate. If the organization has a standard template for policies, the form of the information security policy should use this template.

Other information

Further information on policies related to information security can be found in ISO/IEC 27002.

Further information about the relationship between the information security policy and other policies in a policy framework can be found in Annex A.

5.3 Organizational roles, responsibilities and authorities

Required activity

Top management ensures that responsibilities and authorities for roles relevant to information security are assigned and communicated throughout the organization.

Explanation

Top management ensures that roles and responsibilities as well as the necessary authorities relevant to information security are assigned and communicated.

The purpose of this requirement is to assign responsibilities and authorities to ensure conformance of the ISMS with the requirements of ISO/IEC 27001, and to ensure reporting on the performance of the ISMS to the top management.

Guidance

Top management should regularly ensure that the responsibilities and authorities for the ISMS are assigned so that the management system fulfils the requirements stated in ISO/IEC 27001. Top management does not need to assign all roles, responsibilities and authorities, but it should adequately delegate authority to do this. Top management should approve major roles, responsibilities and authorities of the ISMS.

Responsibilities and authorities related to information security activities should be assigned. Activities include:

a) coordinating the establishment, implementation, maintenance, performance reporting, and improvement of the ISMS;

b) advising on information security risk assessment and treatment;

c) designing information security processes and systems;

d) setting standards concerning determination, configuration and operation of information security controls;

e) managing information security incidents; and

f) reviewing and auditing the ISMS.

Beyond the roles specifically related to information security, relevant information security responsibilities and authorities should be included within other roles. For example, information security responsibilities can be incorporated in the roles of:

g) information owners;

h) process owners;

i) asset owners (e.g. application or infrastructure owners);

j) risk owners;

k) information security coordinating functions or persons (this particular role is normally a supporting role in the ISMS);

l) project managers;

m) line managers; and

n) information users.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

No other information.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

Overview

ISO/IEC 27001:2013, 6.1 is concerned with the planning of actions to address all types of risks and opportunities that are relevant to the ISMS. This includes risk assessment and planning for risk treatment.

The structure of ISO/IEC 27001 subdivides risks into two categories during planning:

a) risks and opportunities relevant to the intended outcome(s) of the ISMS as a whole; and

b) information security risks that relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS.

The first category should be handled in accordance with requirements specified in ISO/IEC 27001:2013, 6.1.1 (general). Risks that fall into this category can be risks relating to the ISMS itself, the ISMS scope definition, top management's commitment to information security, resources for operating the ISMS, etc. Opportunities that fall into this category can be opportunities relating to the outcome(s) of the ISMS, the commercial value of an ISMS, the efficiency of operating ISMS processes and information security controls, etc.

The second category consists of all risks that directly relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS. These risks should be handled in accordance with 6.1.2 (information security risk assessment) and 6.1.3 (information security risk treatment).

Organizations may choose to use different techniques for each category.

The subdivision of requirements for addressing risks can be explained as follows:

— it encourages compatibility with other management systems standards for those organizations that have integrated management systems for different aspects like quality, environment and information security;

— it requires that the organization defines and applies complete and detailed processes for information security risk assessment and treatment; and

— it emphasizes that information security risk management is the core element of an ISMS.

ISO/IEC 27001:2013, 6.1.1 uses the expressions 'determine the risks and opportunities' and 'address these risks and opportunities'. The word "determine" can be considered to be equivalent to the word "assess" used in ISO/IEC 27001:2013, 6.1.2 (i.e. identify, analyse and evaluate). Similarly, the word "address" can be considered equivalent to the word "treat" used in ISO/IEC 27001:2013, 6.1.3.

Required activity

When planning for the ISMS, the organization determines the risks and opportunities considering issues referred to in 4.1 and requirements referred to in 4.2.

Explanation

For risks and opportunities relevant to the intended outcome(s) of the ISMS, the organization determines them based on internal and external issues (see 4.1) and requirements from interested parties (see 4.2). Then the organization plans its ISMS to:

a) ensure that intended outcomes are delivered by the ISMS, e.g. that the information security risks are known to the risk owners and treated to an acceptable level;

b) prevent or reduce undesired effects of risks relevant to the intended outcome(s) of the ISMS; and

c) achieve continual improvement (see 10.2), e.g. through appropriate mechanisms to detect and correct weaknesses in the management processes or taking opportunities for improving information security.

Risks connected to a) above could be unclear processes and responsibilities, poor awareness among employees, poor engagement from management, etc. Risks connected to b) above could be poor risk management or poor awareness of risks. Risks connected to c) above could be poor management of the ISMS documentation and processes.

When an organization pursues opportunities in its activities, these activities then affect the context of the organization (ISO/IEC 27001:2013, 4.1) or the needs and expectations of interested parties (ISO/IEC 27001:2013, 4.2), and can change the risks to the organization. Examples of such opportunities can be: focusing its business on some areas of products or services, establishing marketing strategy for some geographical regions, or expanding business partnerships with other organizations.

Opportunities also exist in continual improvements of the ISMS processes and documentation, along with evaluation of the intended outcomes delivered by the ISMS. For example, consideration of a relatively new ISMS often results in identification of opportunities to refining processes by clarifying interfaces, reducing administrative overhead, eliminating parts of processes that are not cost effective, by refining documentation and introducing new information technology.

The planning in 6.1.1 includes the determination of:

d) actions to address the risks and opportunities; and

e) the way to:

   1) integrate and implement these actions into the ISMS processes; and

   2) evaluate the effectiveness of these actions.

Guidance

The organization should:

f) determine risks and opportunities that can affect the achievement of the goals described in a), b) and c), considering the issues referred to in 4.1 and the requirements referred to in 4.2; and

g) develop a plan to implement the determined actions and to evaluate the effectiveness of those actions; actions should be planned considering integration of information security processes and documentation in existing structures; all these actions are linked with information security objectives (6.2) against which the information security risks are assessed and treated (see 6.1.2 and 6.1.3).

The general requirement to continually improve the ISMS stated in ISO/IEC 27001:2013, 10.2 is supported by the requirement to achieve continual improvement given in 6.1.1 with other relevant requirements of ISO/IEC 27001:2013, 5.1 g), 5.2 d), 9.1, 9.2 and 9.3.

The actions required in 6.1.1 can be different for strategical, tactical and operational levels, for different sites, or for different services or systems.

Several approaches can be taken to meet the requirements of 6.1.1, two of which are:

— considering risks and opportunities associated with planning, implementing and operating the ISMS separately from information security risks; and

— considering all risks simultaneously.

An organization that is integrating an ISMS into an established management system can find that the requirements of 6.1.1 are met by the organization's existing business planning methodology. Where this is the case, care should be taken to verify that the methodology covers all the requirements of 6.1.1.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

Further information about risk management can be found in ISO 31000.

NOTE The term "risk" is defined as the "effect of uncertainty on objectives" (see ISO/IEC 27000:2016, 2.68).

6.1.2 Information security risk assessment

Required activity

The organization defines and applies an information security risk assessment process.

Explanation

The organization defines an information security risk assessment process that:

a) establishes and maintains:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments, which can include criteria for assessing the consequence and likelihood, and rules for the determination of the level of risk; and

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results.

The information security risk assessment process is then defined along the following sub-processes:

c) identification of information security risks:

   1) identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS; and

   2) identify the risk owners associated with these risks, i.e. identify and appoint persons with the appropriate authority and responsibility for managing identified risks.

d) analysis of the information security risks:

   1) assess the potential consequences in case the identified risks materialize, e.g. direct business impacts such as monetary loss or indirect business impacts such as damage in reputation. Assessed consequences can be reported with quantitative or qualitative values;

   2) assess the realistic likelihood of occurrence of the identified risks, with quantitative (i.e. probability or frequency) or qualitative values; and

3) determine the levels of identified risk as a predefined combination of assessed consequences and assessed likelihoods; and

e) evaluation of the information security risks:

1) compare the results of risk analysis with the risk acceptance criteria established before; and

2) prioritize the analysed risks for risk treatment, i.e. determine urgency of treatment for risks that are considered as unacceptable, and sequence if several risks need treatment.

The information security risk assessment process is then applied.

All steps of the information security risk assessment process (6.1.2 a) to e)) as well as the results of its application are retained by the organization as documented information.

Guidance

Guidance on establishing risk criteria (6.1.2 a))

The information security risk criteria should be established considering the context of the organization and requirements of interested parties and should be defined in accordance with top management's risk preferences and risk perceptions on one hand and should allow for a feasible and appropriate risk management process on the other hand.

The information security risk criteria should be established in connection with the intended outcome(s) of the ISMS.

According to ISO/IEC 27001:2013, 6.1.2 a), criteria concerning information security risk assessment that consider the assessment of likelihood and consequences should be established. Further, risk acceptance criteria should be established.

After establishing criteria for assessing consequences and likelihoods of information security risks, the organization should also establish a method for combining them in order to determine a level of risk. Consequences and likelihoods may be expressed in a qualitative, quantitative or semi-quantitative manner.

Risk acceptance criteria relates to risk assessment (in its evaluation phase, when the organization should understand if a risk is acceptable or not), and risk treatment activities (when the organization should understand if the proposed risk treatment is sufficient to reach an acceptable level of risk).

Risk acceptance criteria can be based on a maximum level of acceptable risks, on cost-benefits considerations, or on consequences for the organization.

The risk acceptance criteria should be approved by the responsible management.

Guidance on producing consistent, valid and comparable assessment results (6.1.2 b))

The risk assessment process should be based on methods and tools designed in sufficient detail so that it leads to consistent, valid and comparable results.

Whatever the chosen method, the information security risk assessment process should ensure that:

— all risks, at the needed level of detail, are considered;

— its results are consistent and reproducible (i.e. the identification of risks, their analysis and their evaluation can be understood by a third party and results are the same when different persons assess the risks in the same context); and

— the results of repeated risk assessments are comparable (i.e. it is possible to understand if the levels of risk are increased or decreased).

Inconsistencies or discrepancies in the results when the whole or part of the information security risk assessment process is repeated can indicate that the chosen risk assessment method is not adequate.

Guidance on identification of information security risks (6.1.2 c))

Risk identification is the process of finding, recognizing and describing risks. This involves the identification of risk sources, events, their causes and their potential consequences.

The aim of risk identification is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of information security objectives.

Two approaches are commonly used for the identification of information security risks:

— event-based approach: considers risk sources in a generic way. Events considered can have happened in the past or can be anticipated for the future. In the first case they can involve historical data, in the second case they can be based on theoretical analysis and expert opinions; and

— approach based on identification of assets, threats, and vulnerabilities: considers two different types of risk sources: assets with their intrinsic vulnerabilities, and threats. Potential events considered here are ways as to how threats could exploit a certain vulnerability of an asset to impact the organization's objectives.

Both approaches are consistent with the principles and generic guidelines on risk assessment in ISO 31000.

Other approaches of risk identification may be used if they have proven a similar practical usefulness and if they can ensure the requirements in 6.1.2 b).

NOTE The approach based on assets, threats, and vulnerabilities corresponds to the information security risk identification approach by, and compatible with, the requirements in ISO/IEC 27001 to ensure that previous investments in risk identification are not lost.

It is not recommended that the risk identification be too detailed in the first cycle of risk assessment. Having a high level but clear picture of the information security risks is far better than having no picture at all.

Guidance on analysis of the information security risks (6.1.2 d))

Risk analysis has the objective to determine the level of the risk.

ISO 31000 is referenced in ISO/IEC 27001 as a general model. ISO/IEC 27001 requires that for each identified risk the risk analysis is based on assessing the consequences resulting from the risk and assessing the likelihood of those consequences occurring to determine a level of risk.

Techniques for risk analysis based on consequences and likelihood can be:

1) qualitative, using a scale of qualifying attributes (e.g. high, medium, low);

2) quantitative, using a scale with numerical values (e.g. monetary cost, frequency or probability of occurrence); or

3) semi-quantitative, using qualitative scales with assigned values.

Whatever technique for risk analysis is used, its level of objectivity should be considered.

There are several methods for analysing the risks. The two approaches mentioned (event based approach and approach based on identification of assets, threats, and vulnerabilities) can be suitable for information security risk analysis. Risk identification and analysis processes can be most effective when carried out with the help of experts in the relevant risks under discussion.

Guidance on evaluation of the information security risks (6.1.2 e))

Evaluation of analysed risks involves using the organization's decision making processes to compare the assessed level of risk for each risk with the pre-determined acceptance criteria in order to determine the risk treatment options.

This final step of the risk assessment verifies whether the risks that have been analysed in the previous steps can be accepted according to the acceptance criteria defined under 6.1.2 a), or need further treatment. The step in 6.1.2 d) delivers information about the magnitude of the risk but no immediate information about the urgency of implementing risk treatment options. Depending on the circumstances in which risks occur, they can have different priorities for treatment. Therefore, the output of this step should be a list of risks in priority order. It is useful to retain further information about these risks from the risk identification and risk analysis steps to support decisions for risk treatment.

Other information

ISO/IEC 27005 provides guidance for performing information security risk assessments.

6.1.3 Information security risk treatment

Required activity

The organization defines and applies an information security risk treatment process.

Explanation

Information security risk treatment is the overall process of selecting risk treatment options, determining appropriate controls to implement such options, formulating a risk treatment plan and obtaining approval of the risk treatment plan by the risk owner(s).

All steps of the information security risk treatment process (6.1.3 a) to f)) as well as the results of its application are retained by the organization as documented information.

Guidance

Guidance on information security risk treatment options (6.1.3 a))

Risk treatment options are:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk or by removing the risk source (e.g. closing an e-commerce portal);

b) taking additional risk or increasing risk in order to pursue a business opportunity (e.g. opening an e-commerce portal);

c) modifying the risk by changing the likelihood (e.g. reducing vulnerabilities) or the consequences (e.g. diversifying assets) or both;

d) sharing the risk with other parties by insurance, sub-contracting or risk financing; and

e) retaining the risk based on the risk acceptance criteria or by informed decision (e.g. maintaining the existing e-commerce portal as it is).

Each individual risk should be treated in line with information security objectives by one or more of these options, in order to meet risk acceptance criteria.

Guidance on determining necessary controls (6.1.3 b))

Special attention should be given to the determination of the necessary information security controls. Any control should be determined based on information security risks previously assessed. If an organization has a poor information security risk assessment, it has a poor foundation for its choice of information security controls.

Appropriate control determination ensures:

f) all necessary controls are included, and no unnecessary controls are chosen; and

g) the design of necessary controls satisfies an appropriate breadth and depth.

As a consequence of a poor choice of controls, the proposed information security risk treatment can be:

h) ineffective; or

i) inefficient and therefore inappropriately expensive.

To ensure that information security risk treatment is effective and efficient, it is therefore important to be able to demonstrate the relationship from the necessary controls back to the results of the risk assessment and risk treatment processes.

It can be necessary to use multiple controls to achieve the required treatment of the information security risk. For example, if the option to change the consequences of a particular event is chosen, it may require controls to effect prompt detection of the event as well as controls to respond to and recover from the event.

When determining controls, the organization should also take into account controls needed for services from outside suppliers of e.g. applications, processes and functions. Typically, these controls are mandated by entering information security requirements in the agreements with these suppliers, including ways to get information about to which extent these requirements are met (e.g. right of audit). There may be situations where the organization wishes to determine and describe detailed controls as being part of its own ISMS even though the controls are carried out by outside suppliers. Independently of the approach taken, the organization always should consider controls needed at their suppliers when determining controls for its ISMS.

Guidance on comparing controls with those in ISO/IEC 27001:2013, Annex A (6.1.3 c))

ISO/IEC 27001:2013, Annex A contains a comprehensive list of control objectives and controls. Users of this document are directed to the generic representation of controls in ISO/IEC 27001:2013, Annex A to ensure that no necessary controls are overlooked. Comparison with ISO/IEC 27001:2013, Annex A can also identify alternative controls to those determined in 6.1.3 b) which can be more effective at modifying information security risk.

Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in ISO/IEC 27001:2013, Annex A are not exhaustive and additional control objectives and controls should be added as needed.

Not every control within ISO/IEC 27001:2013, Annex A needs to be included. Any control within ISO/IEC 27001:2013, Annex A that does not contribute to modifying risk should be excluded and justification for the exclusion should be given.

Guidance on producing a Statement of Applicability (SoA) (6.1.3 d))

The SoA contains:

— all necessary controls (as determined in 6.1.3 b) and 6.1.3 c)) and, for each control:
  — the justification for the control's inclusion; and
  — whether the control is implemented or not (e.g. fully implemented, in progress, not yet started); and
— the justification for excluding any of the controls in ISO/IEC 27001: 2013, Annex A.

Justification for including a control in part relies on the effect of the control in modifying an information security risk. A reference to information security risk assessment results and the information security risk treatment plan should be sufficient, along with the information security risk modification expected by the implementation of necessary controls.

Justification for excluding a control contained within ISO/IEC 27001:2013, Annex A can include the following:

— it has been determined that the control is not necessary to implement the chosen information security risk treatment option(s);

— the control is not applicable because it is outside the scope of the ISMS (e.g. ISO/IEC 27001:2013, A.14.2.7 Outsourced development is not applicable if all the organization's system development is performed in-house); and

— it is obviated by a custom control (e.g. in ISO/IEC 27001:2013, A.8.3.1 management of removable media could be excluded if a custom control prevents the use of removable media).

NOTE A custom control is a control not included in ISO/IEC 27001:2013, Annex A.

A useful SoA can be produced as a table containing all 114 controls of ISO/IEC 27001:2013, Annex A along the rows plus rows with the additional controls that are not mentioned in ISO/IEC 27001:2013, Annex A, if needed. One column of the table can indicate whether a control is necessary to implement the risk treatment option(s) or can be excluded. A next column can contain the justification for inclusion or exclusion of a control. A last column of the table can indicate the current implementation status of the control. Further columns can be used, such as for details not required by ISO/IEC 27001 but usually useful for subsequent reviews; these details can be a more detailed description of how the control is implemented or a cross-reference to a more detailed description and documented information or policies relevant for implementing the control.

Although it is not a specific requirement of ISO/IEC 27001, organizations can find it useful to include responsibilities for the operation of each control included in the SoA.

Guidance on formulating an information security risk treatment plan (6.1.3 e))

ISO/IEC 27001 does not specify a structure or content for the information security risk treatment plan. However, the plan should be formulated from the outputs of 6.1.3 a) to c). Thus the plan should document for each treated risk:

— selected treatment option(s);

— necessary control(s); and

— implementation status.

Other useful content can include:

— risk owner(s); and

— expected residual risk after the implementation of actions.

If any action is required by the risk treatment plan, then it should be planned indicating responsibilities and deadlines (see also 6.2); such an action plan can be represented by a list of these actions.

A useful information security risk treatment plan can be designed as a table sorted by risks identified during the risk assessment, showing all the determined controls. As an example, there can be columns in this table which indicate the names of the persons responsible for providing the controls. Further columns can indicate the date of implementation of the control, information about how the control (or a process) is intended to operate and a column about the target implementation status.

As an example for part of the risk treatment process, consider the theft of a mobile phone. The consequences are loss of availability and potential undesirable disclosure of information. If the assessment of the risk showed that the level of risk is out of acceptance, the organization can decide to change the likelihood, or change the consequences of the risk.

To change the likelihood of loss or theft of a mobile phone, the organization can determine that a suitable control is to oblige employees through a mobile device policy to take care of mobile phones and periodically check for loss.

To change the consequence of loss or theft of a mobile phone, the organization can determine controls such as:

— an incident management process so users can report the loss;

— a Mobile Device Management (MDM) solution to delete the content of the phone if lost; and

— a backup plan of mobile devices for recovering the phone's content.

When preparing its SoA (6.1.3 d)), the organization can include its chosen controls (mobile device policy and MDM), justifying their inclusion based on their effect of changing the likelihood and consequences of mobile phone loss or theft, resulting in reduced residual risk.

Comparing these controls with those listed in ISO/IEC 27001:2013, Annex A (6.1.3 c)), it can be seen that the mobile device policy is aligned with ISO/IEC 27001:2013, A.6.2.1, but the MDM control does not directly align and should be considered as an additional custom control. If MDM and other controls are determined as necessary control(s) in an organization's information security risk treatment plan, they should be included in the SoA (see "Guidance on producing an SoA (6.1.3 d)).

If the organization wants to further reduce the risk, it can consider from ISO/IEC 27001:2013, A.9.1.1 (access control policy) that it lacked control of access to mobile phones and modify its mobile device policy to mandate the use of PINs on all mobile phones. This should then be a further control to change the consequences of loss or theft of mobile phones.

When formulating its information security risk treatment plan (6.1.3 e)), the organization should then include actions to implement mobile device policy and MDM and assign responsibilities and timeframes.

Guidance on obtaining risk owners' approval (6.1.3 f))

When the information security risk treatment plan is formulated, the organization should obtain the authorization from the risk owners. Such authorization should be based on defined risk acceptance criteria or justified concession if there is any deviance from them.

Through its management processes the organization should record the risk owner's acceptance of the residual risk and management approval of the plan.

As an example, this risk owner's approval can be documented by amending the risk treatment plan described under guidance on 6.1.3 e) by columns indicating the effectiveness of the control, the residual risk, and the risk owner's approval.

Other information

Further information on risk treatment can be found in ISO/IEC 27005 and ISO 31000.

6.2 Information security objectives and planning to achieve them

Required activity

The organization establishes information security objectives and plans to achieve them at relevant functions and levels.

Explanation

Information security objectives help to implement strategic goals of an organization as well as to implement the information security policy. Thereby, objectives in an ISMS are the information security objectives for confidentiality, integrity and availability of information. Information security objectives also help to specify and measure the performance of information security controls and processes, in accordance with the information security policy (see 5.2).

The organization plans, establishes and issues information security objectives to relevant functions and levels.

Requirements in ISO/IEC 27001 concerning information security objectives apply to all information security objectives. If the information security policy contains objectives, then those objectives are required to meet the criteria in 6.2. If the policy contains a framework for setting objectives, then the objectives produced by that framework are required to meet the requirements of 6.2.

Requirements to be taken into account when establishing objectives are those determined when understanding the organisation and its context (see 4.1) as well as the needs and expectations of interested parties (see 4.2).

The results from risk assessments and risk treatments are used as input to the on-going review of objectives to ensure that they remain appropriate to the circumstances of an organization.

Information security objectives are inputs for risk assessment: risk acceptance criteria and criteria for performing information security risk assessments (see 6.1.2) take into account these information security objectives and thus ensure that levels of risk are aligned with them.

Information security objectives as per ISO/IEC 27001 are:

a) consistent with the information security policy;

b) measurable if practicable; this means that it is important to be able to determine whether or not an objective has been met;

c) connected to applicable information security requirements, and results from risk assessment and risk treatment;

d) communicated; and

e) updated as appropriate.

The organization retains documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization determines:

f) what will be done;

g) what resources will be required;

h) who will be responsible;

i) when it will be completed; and

j) how the results will be evaluated.

The above requirement concerning planning is generic and applicable to other plans required by ISO/IEC 27001. Plans to consider for an ISMS include:

— plans for improving the ISMS as described in 6.1.1 and 8.1;

— plans for treating identified risks as described in 6.1.3 and 8.3; and

— any other plans that are found necessary for effective operation (e.g. plans for developing competence and increasing awareness, communication, performance evaluation, internal audits and management reviews).

Guidance

The information security policy should state the information security objectives or provide a framework for setting the objectives.

Information security objectives can be expressed in various ways. The expression should be suitable to meet the requirement of being measurable (if practicable) (ISO/IEC 27001:2013, 6.2 b)).

For example, information security objectives can be expressed in terms of:

— numerical values with their limits, e.g. “not go over a certain limit”, and “reach level 4”;

— the targets for measurements of information security performance;

— the targets for measurements of the effectiveness of the ISMS (see 9.1);

— compliance with ISO/IEC 27001;

— compliance with ISMS procedures;

— the need to complete actions and plans; and

— risk criteria to be met.

The following guidance applies to the bullets addressed in the explanation:

— see a) above. The information security policy specifies the requirements for information security in an organization. All other specific requirements set for relevant functions and levels should be consistent with them. If the information security policy has information security objectives, then any other specific information security objective should be linked to the ones in the information security policy. If the information security policy only provides the framework for setting objectives, then that framework should be followed and should ensure that more specific objectives are linked to the more generic ones;

— see b) above. Not every objective can be measurable, but making objectives measurable supports achievement and improvement. It is highly desirable to be able to describe, qualitatively or quantitatively, the degree to which an objective has been met. For example, to guide priorities for additional effort if objectives are not met, or to provide insights into opportunities for improved effectiveness if objectives are exceeded. It should be possible to understand whether they have been achieved or not, how achievement of objectives is determined, and whether it is possible to determine the degree of achievement of objectives using quantitative measurements. Quantitative descriptions of objective attainment should specify how associated measurement is done. It may not be possible to quantitatively determine the degree of attainment of all objectives. ISO/IEC 27001 requires objectives to be measurable if practicable;

— see c) above. Information security objectives should be aligned with information security needs; for this reason, risk assessment and treatment results should be used as inputs when setting information security objectives;

— see d) above. Information security objectives should be communicated to relevant internal interested parties of the organization. They may also be communicated to external interested parties, e.g. customers, stakeholders, to the extent they need to know and are affected by the information security objectives; and

— see e) above. When information security needs change over time, related information security objectives should be updated accordingly. Their update should be communicated as required in d), to internal and external interested parties as appropriate.

The organization should plan how to achieve its information security objectives. The organisation may use any methodology or mechanism it chooses to plan for the achievement of its information security objectives. There may be a single information security plan, one or more project plans, or actions included in other organisational plans. Whatever form planning takes, the resulting plans should define as a minimum (see f) to j) above):

— the activities to be done;

— the required resources to be committed to execute the activities;

— the responsibilities;

— the timelines and milestones of activities; and

— the methods and measurements to evaluate whether the results achieve objectives, which includes timing of such evaluations.

ISO/IEC 27001 requires organizations to retain documented information on the information security objectives. Such documented information can include:

— plans, actions, resources, responsibilities, deadlines and evaluation methods; and

— requirements, tasks, resources, responsibilities, evaluation frequency and methods.

Other information

No other information.

7 Support

7.1 Resources

Required activity

The organization determines and provides the resources for establishing, implementing, maintaining and continually improving the ISMS.

Explanation

Resources are fundamental to perform any kind of activity. Categories of resources can include:

a) persons to drive and operate the activities;

b) time to perform activities and time to allow results to settle down before making a new step;

c) financial resources to acquire, develop and implement what is needed;

d) information to support decisions, measure performance of actions, and improve knowledge; and

e) infrastructure and other means that can be acquired or built, such as technology, tools and materials, regardless of whether they are products of information technology or not.

These resources are to be kept aligned with the needs of the ISMS and hence are to be adapted when required.

Guidance

The organization should:

f) estimate the resources needed for all the activities related to the ISMS in terms of quantity and quality (capacities and capabilities);

g) acquire the resources as needed;

h) provide the resources;

i) maintain the resources across the whole ISMS processes and specific activities; and

j) review the provided resources against the needs of the ISMS, and adjust them as required.

Documented information on this activity and its outcome is mandatory only in the form and to the extent that the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

No other information.

7.2 Competence

Required activity

The organization determines the competence of persons needed for information security performance, and ensures that the persons are competent.

Explanation

Competence is the ability to apply knowledge and skills to achieve intended results. It is influenced by knowledge, experience and wisdom.

Competence can be specific (e.g. about technology or specific management areas such as risk management) or general (e.g. soft skills, trustworthiness, and basic technological and managerial subjects).

Competence relates to persons that work under control of the organization. This means that competence should be managed for persons that are employees of the organization and for other people as needed.

Acquisition of higher or new competence and skills can be achieved both internally and externally through experience, training (e.g. courses, seminars and workshops), mentoring, hiring or contracting external persons.

For competence that is only temporarily needed – for a specific activity or for a short period of time, e.g. to cover unexpected temporary shortage of internal personnel – organizations can hire or contract external resources, whose competence is to be described and verified.

Guidance

The organization should:

a) determine the expected competence for each role within the ISMS and decide if it needs to be documented (e.g. in a job description);

b) assign the roles within the ISMS (see 5.3) to persons with the required competence either by:

   1) identifying persons within the organization who have the competence (based e.g. on their education, experience, or certifications);

   2) planning and implementing actions to have persons within the organization obtain the competence (e.g. through provision of training, mentoring, reassignment of current employees); or

   3) engaging new persons who have the competence (e.g. through hiring or contracting);

c) evaluate the effectiveness of actions in b) above;

EXAMPLE 1 Consider if persons have acquired competence after the training.

EXAMPLE 2 Analyse the competence of newly hired or contracted persons some time after their arrival in the organization.

EXAMPLE 3 Verify if the plan for acquiring new persons has been completed as expected.

d) verify that the persons are competent for their roles; and

e) ensure that the competence evolves over time as necessary and that it meets expectations.

Appropriate documented information is required as evidence of competence. The organization should therefore retain documentation about the necessary competence affecting information security performance and how this competence is met by relevant persons.

Other information

No other information.

7.3 Awareness

Required activity

The persons doing work under the organization's control are made aware of the information security policy, their contribution to the effectiveness of the ISMS, benefits of improved information security performance and implications of not conforming to the requirements of the ISMS.

Explanation

Awareness of persons working under the organization's control refers to having the necessary understanding and motivation about what is expected of them with regard to information security.

Awareness concerns persons who have to know, understand, accept and:

a) support the objectives stated in the information security policy; and

b) follow the rules to correctly perform their daily tasks in support of information security.

Additionally, the persons doing work under the organization's control also need to know, understand and accept the implications of not conforming with the ISMS requirements. Implications can be negative consequences for information security or repercussions for the person.

These persons need to be aware that an information security policy exists and where to find information about it. Many staff in an organization do not need to know the detailed content of the policy. Instead, they should know, understand, accept and implement the information security objectives and requirements derived from the policy that affect their job role. These requirements can be included in the standards or procedures they are expected to follow to do their job.

Guidance

The organization should:

c) prepare a programme with the specific messages focused on each audience (e.g. internal and external persons);

d) include information security needs and expectations within awareness and training materials on other topics to place information security needs into relevant operational contexts;

e) prepare a plan to communicate messages at planned intervals;

f) verify the knowledge and understanding of messages both at the end of an awareness session and at random between sessions; and

g) verify whether persons act according to the communicated messages and use examples of 'good' and 'bad' behaviour to reinforce the message.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

Further information on awareness in the field of information security can be found in ISO/IEC 27002:2013, 7.2.2.

7.4 Communication

Required activity

The organization determines the needs for internal and external communications related to the ISMS.

Explanation

Communication is a key process within an ISMS. Adequate communication is necessary with internal and external interested parties (see 4.2).

Communication can be between internal interested parties at all levels of the organization or between the organization and external interested parties. Communication can be initiated within the organization or by an external interested party.

Organizations need to determine:

— which content needs to be communicated, e.g. information security policies, objectives, procedures, their changes, knowledge on information security risks, requirements to suppliers and feedback on the information security performance;

— the preferred or optimal point in time for communication activities;

— who is to be involved in communication activities, and which is the target audience of each communication effort;

— who is to initiate communication activities, e.g. specific content can require communication to be initiated by a specific person or organization; and

— which processes are driving or initiating communication activities, and which processes are targeted or affected by communication activities.

Communication can take place regularly or as needs arise. It can be either proactive or reactive.

Guidance

Communication relies on processes, channels and protocols. These should be chosen to ensure the communicated message is integrally received, correctly understood and, when relevant, acted upon appropriately.

Organizations should determine which content needs to be communicated, such as:

a) plans and results of risk management to interested parties as needed and appropriate, in the identification, analysis, evaluation, and treatment of the risks;

b) information security objectives;

c) achieved information security objectives including those that can support their position in the market (e.g. ISO/IEC 27001 certificate granted; claiming conformance with personal data protection laws);

d) incidents or crises, where transparency is often key to preserve and increase trust and confidence in the organization's capability to manage its information security and deal with unexpected situations;

e) roles, responsibilities and authority;

f) information exchanged between functions and roles as required by the ISMS's processes;

g) changes to the ISMS;

h) other matters identified by reviewing the controls and processes within the scope of the ISMS;

i) matters (e.g. incident or crisis notification) that require communication to regulatory bodies or other interested parties; and

j) requests or other communications from external parties such as customers, potential customers, users of services and authorities.

The organization should identify the requirements for communication on relevant issues:

k) who is allowed to communicate externally and internally (e.g. in special cases such as a data breach), allocating to specific roles with the appropriate authority. For example, official communication officers can be defined with the appropriate authority. They could be a public relations officer for external communication and a security officer for internal communication;

l) the triggers or frequency of communication (e.g. for communication of an event, the trigger is the identification of the event);

m) the contents of messages for key interested parties (e.g. customers, regulators, general public, important internal users) based on high level impact scenarios. Communication can be more effective if based on messages prepared and pre-approved by an appropriate level of management as part of a communication plan, the incident response plan or the business continuity plan;

n) the intended recipients of the communication; in some cases, a list should be maintained (e.g. for communicating changes to services or crisis);

o) the communication means and channels. Communication should use dedicated means and channels, to make sure that the message is official and bears the appropriate authority. Communication channels should address any needs for the protection of the confidentiality and integrity of the information transmitted; and

p) the designed process and the method to ensure messages are sent and have been correctly received and understood.

Communication should be classified and handled according to the organization's requirements.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

No other information.

7.5 Documented information

7.5.1 General

Required activity

The organization includes documented information in the ISMS as directly required by ISO/IEC 27001, as well as determined by the organization as being necessary for the effectiveness of the ISMS.

Explanation

Documented information is needed to define and communicate information security objectives, policy, guidelines, instructions, controls, processes, procedures, and what persons or groups of people are expected to do and how they are expected to behave. Documented information is also needed for audits of the ISMS and to maintain a stable ISMS when persons in key roles change. Further, documented information is needed for recording actions, decisions and outcome(s) of ISMS processes and information security controls.

Documented information can contain:

— information about information security objectives, risks, requirements and standards;

— information about processes and procedures to be followed; and

— records of the input (e.g. for management reviews) and the outcomes of processes (including plans and outcomes of operational activities).

There are many activities within the ISMS that produce documented information that is used, most of the time, as an input for another activity.

ISO/IEC 27001 requires a set of mandatory documented information and contains a general requirement that additional documented information is required if it is necessary for the effectiveness of the ISMS.

The amount of documented information needed is often related to the size of the organization.

In total, the mandatory and additional documented information contains sufficient information to allow the performance evaluation requirements specified in Clause 9 to be carried out.

Guidance

The organization should determine what documented information is necessary for ensuring effectiveness of its ISMS in addition to mandatory documented information required by ISO/IEC 27001.

The documented information should be there to fit the purpose. Factual and 'to the point' information is what is needed.

Examples of documented information that can be determined by the organization to be necessary for ensuring effectiveness of its ISMS are:

— the results of the context establishment (see Clause 4);

— the roles, responsibilities and authorities (see Clause 5);

— reports of the different phases of the risk management (see Clause 6);

— resources determined and provided (see 7.1);

— the expected competence (see 7.2);

— plans and results of awareness activities (see 7.3);

— plans and results of communication activities (see 7.4);

— documented information of external origin that is necessary for the ISMS (see 7.5.3);

— process to control documented information (see 7.5.3);

— policies, rules and directives for directing and operating information security activities;

— processes and procedures used to implement, maintain and improve the ISMS and the overall information security status (see Clause 9);

— action plans; and

— evidence of the results of ISMS processes (e.g. incident management, access control, information security continuity, equipment maintenance, etc.).

Documented information can be of internal or external origin.

Other information

If the organization wants to manage its documented information in a document management system, this can be built according to the requirements in ISO 30301.

7.5.2 Creating and updating

Required activity

When creating and updating documented information, the organization ensures its appropriate identification and description, format and media, and review and approval.

Explanation

The organization identifies in detail how the documented information is best structured and defines a suitable documentation approach.

Review and approval by appropriate management ensures that the documented information is correct, suitable for the purpose, and in an adequate form and detail for the intended audience. Regular reviews ensure continued suitability and adequacy of documented information.

Guidance

Documented information may be retained in any form, e.g. traditional documents (in both paper and electronic form), web pages, databases, computer logs, computer generated reports, audio and video. Moreover, documented information may consist of specifications of intent (e.g. the information security policy) or records of performance (e.g. the results of an audit) or a mixture of both. The following guidance applies directly to traditional documents and should be interpreted appropriately when applied to other forms of documented information.

Organizations should create a structured documented information library, linking different parts of documented information by:

a) determining the structure of the documented information framework;

b) determining the standard structure of the documented information;

c) providing templates for different types of documented information;

d) determining the responsibilities for preparing, approving, publishing and managing the documented information; and

e) determining and documenting the revision and approval process to ensure continual suitability and adequacy.

Organizations should define a documentation approach that includes common attributes of every document, which allow clear and unique identification. These attributes usually include document type (e.g. policy, directive, rule, guideline, plan, form, process or procedure), the purpose and scope, title, date of publication, classification, reference number, version number, and a revision history. The identification of the author and the person(s) currently responsible for the document, its application and evolution, as well as the approver(s) or approval authority should be included.

Format requirements can include definition of suitable documentation languages, file formats, software version for working with them and graphical content. Media requirements define on which physical and electronic media the information should be available.

Statements and writing style should be tailored to the audience and scope of the documentation.

Duplication of information in documented information should be avoided and cross-references used rather than replicating the same information in different documents.

The documentation approach should ensure timely review of the documented information and that all documentation changes are subject to approval. Suitable review criteria can be timing related (e.g. maximum time periods between document reviews) or content related. Approval criteria should be defined, which ensures that the documented information is correct, suitable for the purpose, and in an adequate form and detail for the intended audience.

Other information

No other information.

7.5.3 Control of documented information

Required activity

The organization manages documented information throughout its lifecycle and makes it available where and when needed.

Explanation

Once approved, the documented information is communicated to its intended audience. Documented information is available where and when it is needed, while preserving its integrity, confidentiality, and relevance throughout the whole lifecycle.

Note that activities described "as applicable" in ISO/IEC 27001:2013, 7.5.3 need to be performed if they can be performed and are useful, considering the organization's needs and expectations.

Guidance

A structured documented information library can be used to facilitate access to documented information.

All of the documented information should be classified (see ISO/IEC 27001:2013, A.8.2.1) in accordance with the organization's classification scheme. Documented information should be protected and handled in accordance with its classification level (see ISO/IEC 27001:2013, A.8.2.3).

A change management process for documented information should ensure that only authorised persons have the right to change and distribute it as needed through appropriate and predefined means. Documented information should be protected to ensure it keeps its validity and authenticity.

Documented information should be distributed and made available to authorized interested parties. For this, the organization should establish who are the relevant interested parties for each documented information (or groups of documented information), and the means to use for distribution, access, retrieval and use (e.g. a web site with appropriate access control mechanisms). The distribution should comply with any requirements related to protecting and handling of classified information.

The organization should establish the appropriate retention period for documented information according to its intended validity and other relevant requirements. The organization should ensure that information is legible throughout its retention period (e.g. using formats that can be read by available software, or verifying that paper is not corrupted).

The organization should establish what to do with documented information after its retention period has expired.

The organization should also manage documented information of external origin (i.e. from customers, partners, suppliers, regulatory bodies, etc.).

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

No other information.

8 Operation

8.1 Operational planning and control

Required activity

The organization plans, implements and controls the processes to meet its information security requirements and to achieve its information security objectives.

The organization keeps documented information as necessary to have confidence that processes are carried out as planned.

The organization controls planned changes and reviews the consequences of unintended changes, and ensures that outsourced processes are identified, defined and controlled.

Explanation

The processes that an organization uses to meet its information security requirements are planned, and once implemented, they are controlled, particularly when changes are required.

Building on the planning of the ISMS (see 6.1 and 6.2), the organization performs the necessary operational planning and activities to implement the processes needed to fulfil the information security requirements.

Processes to meet information security requirements include:

a) ISMS processes (e.g. management review, internal audit); and

b) processes required for implementing the information security risk treatment plan.

Implementation of plans results in operated and controlled processes.

The organization ultimately remains responsible for planning and controlling any outsourced processes in order to achieve its information security objectives. Thus the organization needs to:

c) determine outsourced processes considering the information security risks related to the outsourcing; and

d) ensure that outsourced processes are controlled (i.e. planned, monitored and reviewed) in a manner that provides assurance that they operate as intended (also considering information security objectives and the information security risk treatment plan).

After the implementation is completed, the processes are managed, monitored and reviewed to ensure that they continue to fulfil the requirements determined after understanding the needs and expectations of interested parties (see 4.2).

Changes of the ISMS in operation can be either planned or they occur unintended. Whenever the organization makes changes to the ISMS (as a result of planning or unintentionally), it assesses the potential consequences of the changes to control any adverse effects.

The organization can get confidence about the effectiveness of the implementation of plans by documenting activities and using documented information as input to the performance evaluation processes specified in Clause 9. The organization therefore establishes the required documented information to keep.

Guidance

The processes that have been defined as a result of the planning described in Clause 6 should be implemented, operated and verified throughout the organization. The following should be considered and implemented:

e) processes that are specific for the management of information security (such as risk management, incident management, continuity management, internal audits, management reviews);

f) processes emanating from information security controls in the information security risk treatment plan;

g) reporting structures (contents, frequency, format, responsibilities, etc.) within the information security area, for example incident reports, reports on measuring the fulfilment of information security objectives, reports on performed activities; and

h) meeting structures (frequency, participants, purpose and authorization) within the information security area. Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions for effective management of the information security area.

For planned changes, the organization should:

i) plan their implementation and assign tasks, responsibilities, deadlines and resources;

j) implement changes according to the plan;

k) monitor their implementation to confirm that they are implemented according to the plan; and

l) collect and retain documented information on the execution of the changes as evidence that they have been carried out as planned (e.g. with responsibilities, deadlines, effectiveness evaluations).

For observed unintended changes, the organization should:

m) review their consequences;

n) determine whether any adverse effects have already occurred or can occur in the future;

o) plan and implement actions to mitigate any adverse effects as necessary; and

p) collect and retain documented information on unintended changes and actions taken to mitigate adverse effects.

If part of the organization's functions or processes are outsourced to suppliers, the organization should:

q) determine all outsourcing relationships;

r) establish appropriate interfaces to the suppliers;

s) address information security related issues in the supplier agreements;

t) monitor and review the supplier services to ensure that they are operated as intended and associated information security risks meet the risk acceptance criteria of the organization; and

u) manage changes to the supplier services as necessary.

Other information

No other information.

8.2 Information security risk assessment

Required activity

The organization performs information security risk assessments and retains documented information on their results.

Explanation

When performing information security risk assessments, the organization executes the process defined in 6.1.2. These assessments are either executed according to a schedule defined in advance, or in response to significant changes or information security incidents. The results of the information security risk assessments are retained in documented information as evidence that the process in 6.1.2 has been performed as defined.

Documented information from information security risk assessments is essential for information security risk treatment and is valuable for performance evaluation (see Clause 9).

Guidance

Organizations should have a plan for conducting scheduled information security risk assessments.

When any significant changes of the ISMS (or its context) or information security incidents have occurred, the organization should determine:

a) which of these changes or incidents require an additional information security risk assessment; and

b) how these assessments are triggered.

The level of detail of the risk identification should be refined step by step in further iterations of the information security risk assessment in the context of the continual improvement of the ISMS. A broad information security risk assessment should be performed at least once a year.

Other information

ISO/IEC 27005 provides guidance for performing information security risk assessments.

8.3 Information security risk treatment

Required activity

The organization implements the information security risk treatment plan and retains documented information on the results of the information security treatment.

Explanation

In order to treat information security risks, the organization needs to carry out the information security risk treatment process defined in 6.1.3. During operation of the ISMS, whenever the risk assessment is updated according to 8.2, the organization then applies the risk treatment according to 6.1.3 and updates the risk treatment plan. The updated risk treatment plan is again implemented.

The results of the information security risk treatment are retained in documented information as evidence that the process in 6.1.3 has been performed as defined.

Guidance

The information security risk treatment process should be performed after each iteration of the information security assessment process in 8.2 or when the implementation of the risk treatment plan or parts of it fails.

The progress of implementation of the information security risk treatment plan should be driven and monitored by this activity.

Other information

No other information.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

Required activity

The organization evaluates the information security performance and the effectiveness of the ISMS.

Explanation

The objective of monitoring and measurement is to help the organization to judge whether the intended outcome of information security activities including risk assessment and treatment is achieved as planned.

Monitoring determines the status of a system, a process or an activity, whilst measurement is a process to determine a value. Thus monitoring can be achieved through a succession of similar measurements over some time period.

For monitoring and measurement, the organization establishes:

a) what to monitor and measure;

b) who monitors and measures, and when; and

c) methods to be used so as to produce valid results (i.e. comparable and reproducible).

For analysis and evaluation, the organization establishes:

d) who analyses and evaluates the results from monitoring and measurement, and when; and

e) methods to be used so as to produce valid results.

There are two aspects of evaluation:

f) evaluating the information security performance, for determining whether the organization is doing as expected, which includes determining how well the processes within the ISMS meet their specifications; and

g) evaluating the effectiveness of the ISMS, for determining whether or not the organization is doing the right things, which includes determining the extent to which information security objectives are achieved.

Note that as “as applicable” (ISO/IEC 27001:2013, 9.1, b)) means that if methods for monitoring, measurement, analysis and evaluation can be determined, they need to be determined.

Guidance

A good practice is to define the ‘information need’ when planning the monitoring, measurement, analysis and evaluation. An information need is usually expressed as a high level information security question or statement that helps the organization evaluate information security performance and ISMS effectiveness. In other words, monitoring and measurement should be undertaken to achieve a defined information need.

Care should be taken when determining the attributes to be measured. It is impracticable, costly and counterproductive to measure too many, or the wrong attributes. Besides the costs of measuring, analysing and evaluating numerous attributes, there is a possibility that key issues could be obscured or missed altogether.

There are two generic types of measurements:

h) **performance measurements**, which express the planned results in terms of the characteristics of the planned activity, such as head counts, milestone accomplishment, or the degree to which information security controls are implemented; and

i) **effectiveness measurements**, which express the effect that realization of the planned activities has on the organization's information security objectives.

It can be appropriate to identify and assign distinctive roles to those participating in the monitoring, measurement, analysis and evaluation. Those roles can be measurement client, measurement planner, measurement reviewer, information owner, information collector, information analyst and information communicator of input or output of evaluation (see ISO/IEC 27004:2016, 6.5).

The responsibilities for monitoring and measurement and those for analysis and evaluation are often assigned to separate persons whom different competence is required.

Other information

Monitoring, measurement, analysis and evaluation is critical to the success of an effective ISMS. There are a number of clauses in ISO/IEC 27001 that explicitly require determination of the effectiveness of some activities. For example, ISO/IEC 27001:2013, 6.1.1 e), 7.2 c) or 10.1 d).

Further information can be found in ISO/IEC 27004, which provides guidance on meeting the requirements of ISO/IEC 27001:2013, 9.1. In particular, it expands on all of the concepts mentioned above, such as roles and responsibilities, and forms, and gives numerous examples.

9.2 Internal audit

Required activity

The organization conducts internal audits to provide information on conformity of the ISMS to the requirements.

Explanation

Evaluating an ISMS at planned intervals by means of internal audits provides assurance of the status of the ISMS to top management. Auditing is characterized by a number of principles: integrity; fair presentation; due professional care; confidentiality; independence; and evidence-based approach (see ISO 19011).

Internal audits provide information on whether the ISMS conforms to the organization's own requirements for its ISMS as well as to the requirements in ISO/IEC 27001. The organization's own requirements include:

a) requirements stated in the information security policy and procedures;

b) requirements produced by the framework for setting information security objectives, including outcomes of the risk treatment process;

c) legal and contractual requirements; and

d) requirements on the documented information.

Auditors also evaluate whether the ISMS is effectively implemented and maintained.

An audit programme describes the overall framework for a set of audits, planned for specific time frames and directed towards specific purposes. This is different from an audit plan, which describes the activities and arrangements for a specific audit. Audit criteria are a set of policies, procedures or requirements used as a reference against which audit evidence is compared, i.e. the audit criteria describe what the auditor expects to be in place.

An internal audit can identify nonconformities, risks and opportunities. Nonconformities are managed according to requirements in 10.1. Risks and opportunities are managed according to requirements in 4.1 and 6.1.

The organization is required to retain documented information about audit programme(s) and audit results.

Guidance

Managing an audit programme

An audit programme defines the structure and responsibilities for planning, conducting, reporting and following up on individual audit activities. As such it should ensure that audits conducted are appropriate, have the right scope, minimize the impact on the operations of the organization and maintain the necessary quality of audits. An audit programme should also ensure the competence of audit teams, appropriate maintenance of audit records, and the monitoring and review of the operations, risks and effectiveness of audits. Further, an audit programme should ensure that the ISMS (i.e. all relevant processes, functions and controls) is audited within a specified time frame. Finally, an audit programme should include documented information about types, duration, locations, and schedule of the audits.

The extent and frequency of internal audits should be based on the size and nature of the organization as well as on the nature, functionality, complexity and the level of maturity of the ISMS (risk-based auditing).

The effectiveness of the implemented controls should be examined within the scope of internal audits. An audit programme should be designed to ensure coverage of all necessary controls and should include evaluation of the effectiveness of selected controls over time. Key controls (according to the audit programme) should be included in every audit whereas controls implemented to manage lower risks may be audited less frequently.

The audit programme should also consider that processes and controls should have been in operation for some time to enable evaluation of suitable evidence.

Internal audits concerning an ISMS can be performed effectively as a part of, or in collaboration with, other internal audits of the organization. The audit programme can include audits related to one or more management system standards, conducted either separately or in combination.

An audit programme should include documented information about: audit criteria, audit methods, selection of audit teams, processes for handling confidentiality, information security, health and safety provisions for auditors, and other similar matters.

Competence and evaluation of auditors

Regarding competence and evaluation of auditors, the organization should:

e) identify competence requirements for its auditors;

f) select internal or external auditors with the appropriate competence;

g) have a process in place for monitoring the performance of auditors and audit teams; and

h) include personnel on internal audit teams that have appropriate sector specific and information security knowledge.

Auditors should be selected considering that they should be competent, independent, and adequately trained.

Selecting internal auditors can be difficult for smaller companies. If the necessary resources and competence are not available internally, external auditors should be appointed. When organizations use external auditors, they should ensure that they have acquired enough knowledge about the context of the organization. This information should be supplied by internal staff.

Organizations should consider that internal employees acting as internal auditors can be able to perform detailed audits considering the organization's context, but may not have enough knowledge about performing audits.

Organizations should then recognize characteristics and potential shortcomings of internal versus external auditors and establish suitable audit teams with the necessary knowledge and competence.

Performing the audit

When performing the audit, the audit team leader should prepare an audit plan considering results of previous audits and the need to follow up on previously reported nonconformities and unacceptable risks. The audit plan should be retained as documented information and should include criteria, scope and methods of the audit.

The audit team should review:

— adequacy and effectiveness of processes and determined controls;

— fulfilment of information security objectives;

— compliance with requirements defined in ISO/IEC 27001:2013, Clauses 4 to 10;

— compliance with the organization's own information security requirements;

— consistency of the Statement of Applicability against the outcome of the information security risk treatment process;

— consistency of the actual information security risk treatment plan with the identified assessed risks and the risk acceptance criteria;

— relevance (considering organization's size and complexity) of management review inputs and outputs; and

— impacts of management review outputs (including improvement needs) on the organization.

The extent and reliability of available monitoring over the effectiveness of controls as produced by the ISMS (see 9.1) may allow the auditors to reduce their own evaluation efforts, provided they have confirmed the effectiveness of the measurement methods.

If the outcome of the audit includes nonconformities, the auditee should prepare an action plan for each nonconformity to be agreed with the audit team leader. A follow-up action plan typically includes:

i) description of the detected nonconformity;

j) description of the cause(s) of nonconformity;

k) description of short term correction and longer term corrective action to eliminate a detected nonconformity within a defined timeframe; and

l) the persons responsible for implementing the plan.

Audit reports, with audit results, should be distributed to top management.

Results of the previous audits should be reviewed and the audit programme adjusted to better manage areas experiencing higher risks due to nonconformity.

Other information

Further information can be found in ISO 19011, which provides general guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits. It also provides guidance on the evaluation of competence of persons or group of people involved in the audit, including the person managing the audit programme, auditors and audit teams.

Also, in addition to the guidance contained in ISO 19011, further information can be found in:

a) ISO/IEC 27007[1)], which provides specific guidance on managing an ISMS audit programme, on conducting the audits, and on the competence of ISMS auditors; and

b) ISO/IEC 27008[1)], which provides guidance on assessing information security controls.

9.3 Management review

Required activity

Top management reviews the ISMS at planned intervals.

Explanation

The purpose of management review is to ensure the continuing suitability, adequacy and effectiveness of the ISMS. Suitability refers to continuing alignment with the organization's objectives. Adequacy and effectiveness refer to a suitable design and organizational embedding of the ISMS, as well as the effective implementation of processes and controls that are driven by the ISMS.

Overall, management review is a process carried out at various levels in the organization. These activities could vary from daily, weekly, or monthly organizational unit meetings to simple discussions of reports. Top management is ultimately responsible for management review, with inputs from all levels in the organization.

Guidance

Top management should require and regularly review reporting of the performance of the ISMS.

There are many ways in which management can review the ISMS, such as receiving and reviewing measurements and reports, electronic communication, verbal updates. Key inputs are the results of the information security measurements as described in 9.1 and the results of the internal audits described in 9.2 and risk assessment results and risk treatment plan status. When reviewing the results of information security risk assessment and status of the information security risk treatment plan, management should confirm that residual risks meet risk acceptance criteria, and that the risk treatment plan addresses all relevant risks and their risk treatment options.

All aspects of the ISMS should be reviewed by management at planned intervals, at least yearly, by setting up suitable schedules and agenda items in management meetings. New or less mature ISMSs should be reviewed more frequently by management to drive increased effectiveness.

The agenda of the management review should address the following topics:

a) status of actions from previous management reviews;

b) changes in external and internal issues (see 4.1) that are relevant to the ISMS;

c) feedback on the information security performance, including trends, in:

   1) nonconformities and corrective actions;

   2) monitoring and measurement results;

   3) audit results; and

   4) fulfilment of information security objectives.

d) feedback from interested parties, including suggestions for improvement, requests for change and complaints;

1) Second edition under preparation.

e) results of information security risk assessment(s) and status of information security risk treatment plan; and

f) opportunities for continual improvement, including efficiency improvements of both the ISMS and information security controls.

Inputs to the management review should be at the appropriate level of detail, according to the objectives established for the management involved in the review. For example, top management should evaluate only a summary of all items, according to the information security objectives or high level objectives.

The outputs from the management review process should include decisions related to continual improvement opportunities and any needs for changes to the ISMS. They can also include evidence of decisions regarding:

g) changes of the information security policy and objectives, e.g. driven by changes in external and internal issues and requirements of interested parties;

h) changes of the risk acceptance criteria and the criteria for performing information security risk assessments (see 6.1.2);

i) actions, if needed, following assessment of information security performance;

j) changes of resources or budget for the ISMS;

k) updated information security risk treatment plan or Statement of Applicability; and

l) necessary improvements of monitoring and measurement activities.

Documented information from management reviews is required. It should be retained to demonstrate that consideration has been given to (at least) all the areas listed in ISO/IEC 27001, even where it is decided that no action is necessary.

When several management reviews are done at different levels of the organization, then they should be linked to each other in an appropriate manner.

Other information

No other information.

10 Improvement

10.1 Nonconformity and corrective action

Required activity

The organization reacts to nonconformities, evaluates them and takes corrections as well as corrective actions if needed.

Explanation

A nonconformity is a non-fulfilment of a requirement of the ISMS. Requirements are needs or expectations that are stated, implied or obligatory. There are several types of nonconformities such as:

a) failure to fulfil a requirement (completely or partially) of ISO/IEC 27001 in the ISMS;

b) failure to correctly implement or conform to a requirement, rule or control stated by the ISMS; and

c) partial or total failure to comply with legal, contractual or agreed customer requirements.

Nonconformities can be for example:

d) persons not behaving as expected by procedures and policies;

e) suppliers not providing agreed products or services;

f) projects not delivering expected outcomes; and

g) controls not operating according to design.

Nonconformities can be recognised by:

h) deficiencies of activities performed in the scope of the management system;

i) ineffective controls that are not remediated appropriately;

j) analysis of information security incidents, showing the non-fulfilment of a requirement of the ISMS;

k) complaints from customers;

l) alerts from users or suppliers;

m) monitoring and measurement results not meeting acceptance criteria; and

n) objectives not achieved.

Corrections aim to address the nonconformity immediately and deal with its consequences (ISO/IEC 27001:2013, 10.1 a)).

Corrective actions aim to eliminate the cause of a nonconformity and to prevent recurrence (ISO/IEC 27001:2013, 10.1 b) to g)).

Note that as “as applicable” (ISO/IEC 27001:2013, 10.1 a)) means that if an action to control and correct a nonconformity can be taken, then it needs to be taken.

Guidance

Information security incidents do not necessarily imply that a nonconformity exists, but they can be an indicator of a nonconformity. Internal and external audit and customer complaints are other important sources that help in identifying nonconformities.

The reaction to the nonconformity should be based on a defined handling process. The process should include:

— identifying the extent and impact of the nonconformity;

— deciding on the corrections in order to limit the impact of the nonconformity. Corrections can include switching to previous, failsafe or other appropriate states. Care should be taken that corrections do not make the situation worse;

— communicating with relevant personnel to ensure that corrections are carried out;

— carrying out corrections as decided;

— monitoring the situation to ensure that corrections have had the intended effect and have not produced unintended side-effects;

— acting further to correct the nonconformity if it is still not remediated; and

— communicating with other relevant interested parties, as appropriate.

As an overall result, the handling process should lead to a managed status regarding the nonconformity and the associated consequences. However, corrections alone will not necessarily prevent recurrence of the nonconformity.

Corrective actions can occur after, or in parallel with, corrections. The following process steps should be taken:

1. decide if there is a need to carry out a corrective action, in accordance with established criteria (e.g. impact of the nonconformity, repetitiveness);
2. review of the nonconformity, considering:
   - if similar nonconformities have been recorded;
   - all the consequences and side-effects caused by the nonconformity; and
   - the corrections taken.
3. perform an in-depth cause analysis of the nonconformity, considering:
   - what went wrong, the specific trigger or situation which led to the nonconformity (e.g. mistakes determined by persons, methods, processes or procedures, hardware or software tools, wrong measurements, environment); and
   - patterns and criteria that may help to identify similar situations in the future.
4. perform an analysis of potential consequences on the ISMS, considering:
   - whether similar nonconformities exist in other areas, e.g. by using the patterns and criteria found during the cause analysis; and
   - whether other areas match the identified patterns or criteria, so that it is only a matter of time before a similar nonconformity occurs.
5. determine actions needed to correct the cause, evaluating if they are proportionate to the consequences and impact of the nonconformity, and checking they do not have side-effects which may lead to other nonconformities or significant new information security risks;
6. plan the corrective actions, giving priority, if possible, to areas where there are higher likelihood of recurrence and more significant consequences of the nonconformity. Planning should include a responsible person for a corrective action and a deadline for implementation;
7. implement the corrective actions according to the plan; and
8. assess the corrective actions to determine whether they have actually handled the cause of the nonconformity, and whether it has prevented related nonconformities from occurring. This assessment should be impartial, evidence-based and documented. It should also be communicated to the appropriate roles and interested parties.

As a result of corrections and corrective actions, it is possible that new opportunities for improvement are identified. These should be treated accordingly (see 10.2).

Sufficient documented information is required to be retained to demonstrate that the organization has acted appropriately to address the nonconformity and has dealt with the related consequences. All significant steps of nonconformity management (starting from discovery and corrections) and, if started, corrective action management (cause analysis, review, decision about the implementation of actions, review and change decisions made for the ISMS itself) should be documented. The documented information is also required to include evidence as to whether or not actions taken have achieved the intended effects.

Some organizations maintain registers for tracking nonconformities and corrective actions. There can be more than one register (for example, one for each functional area or process) and on different media (paper, file, application, etc.). If this is the case, then they should be established and controlled as documented information and they should allow a comprehensive review of all nonconformities and corrective actions for ensuring the correct evaluation of the need for actions.

Other information

ISO/IEC 27001 does not explicitly state any requirements for "preventive action". This is because one of the key purposes of a formal management system is to act as a preventive tool. Consequently, the common text used in ISO management system standards requires an assessment of the organization's "external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s)" in 4.1, and to "determine the risks and opportunities that need to be addressed to: assure the ISMS can achieve its intended outcome(s); prevent, or reduce, undesired effects; and achieve continual improvement." in 6.1. These two sets of requirements are considered to cover the concept of "preventive action", and also to take a wider view that looks at risks and opportunities.

10.2 Continual improvement

Required activity

The organization continually improves the suitability, adequacy and effectiveness of the ISMS.

Explanation

Organizations and their contexts are never static. In addition, the risks to information systems, and the ways in which they can be compromised, are evolving rapidly. Finally, no ISMS is perfect; there is always a way in which it can be improved, even if the organization and its context are not changing.

As an example of improvements not linked with nonconformities or risks, the assessment of an element of the ISMS (in terms of suitability, adequacy and effectiveness) can show that it exceeds ISMS requirements or lacks efficiency. If it does, then there can be an opportunity to improve the ISMS by changing the assessed element.

A systematic approach using continual improvement will lead to a more effective ISMS, which will improve the organization's information security. Information security management leads the organization's operational activities in order to avoid being too reactive, i.e. that most of the resources are used for finding problems and addressing these problems. The ISMS is working systematically through continual improvement so that the organization can have a more proactive approach. Top management can set objectives for continual improvement, e.g. through measurements of effectiveness, cost, or process maturity.

As a consequence, the organization treats its ISMS as an evolving, learning, living part of business operations. In order for the ISMS to keep up with changes, it is regularly evaluated with regard to its fitness for purpose, effectiveness, and alignment to the organization's objectives. Nothing is to be taken for granted, and nothing is to be considered as 'off limits' simply because it was good enough at the time it was implemented.

Guidance

Continual improvement of the ISMS should entail that the ISMS itself and all of its elements are assessed considering internal and external issues (4.1), requirements of the interested parties (4.2) and results of performance evaluation (Clause 9). The assessment should include an analysis of:

a) suitability of the ISMS, considering if the external and internal issues, requirements of the interested parties, established information security objectives and identified information security risks are properly addressed through planning and implementation of the ISMS and information security controls;

b) adequacy of the ISMS, considering if the ISMS processes and information security controls are compatible with the organization's overall purposes, activities and processes; and

c) effectiveness of the ISMS, considering if the intended outcome(s) of the ISMS are achieved, the requirements of the interested parties are met, information security risks are managed to meet information security objectives, nonconformities are managed, while resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS are commensurate with those results.

The assessment can also include an analysis of the efficiency of the ISMS and its elements, considering if their use of resources is appropriate, if there is a risk that the lack of efficiency can lead to loss of effectiveness or if there are opportunities for increasing efficiency.

Improvement opportunities can also be identified when managing nonconformities and corrective actions.

Once opportunities for improvement are identified, the organization should, according to 6.1.1:

d) evaluate them to establish whether they are worth pursuing;

e) determine the changes to the ISMS and its elements in order to achieve the improvement;

f) plan and implement the actions to address the opportunities ensuring that benefits are realised, and nonconformities do not occur; and

g) evaluate the effectiveness of the actions.

These actions should be considered as a subset of actions to address risks and opportunities described in 6.1.1.

Other information

No other information.

Annex A
(informative)

Policy framework

Annex A provides guidance on the structure of documentation that includes the information security policy.

In general, a policy is a statement of intentions and direction of an organization as formally expressed by its top management (see ISO/IEC 27000:2016, 2.84).

The content of a policy guides actions and decisions concerning the topic of the policy.

An organization can have a number of policies; one for each of the activity areas that is important to the organization. Some policies are independent of each other, while other policies have a hierarchical relationship.

Typically, an organization has a general policy, e.g. code of conduct, at the highest level of the policy hierarchy. The general policy is supported by other policies addressing different topics and can be applicable to specific areas or functions of the organization. The information security policy is one of these specific policies.

The information security policy is supported by a range of topic-specific policies related to aspects of information security. A number of these are discussed in ISO/IEC 27002, for example the information security policy can be supported by policies concerning access control, information classification (and handling), physical and environmental security, end user oriented topics, amongst others. Additional layers of policies may be added. This arrangement is shown in Figure A.1. Note that some organizations use other terms for topic-specific policy documents, such as "standards", "directives" or "rules".

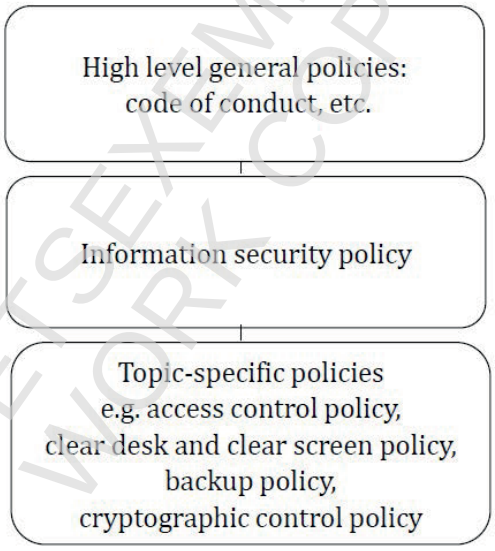


Figure A.1 — Policy hierarchy

ISO/IEC 27001 requires organizations to have an information security policy. It does not, however specify any particular relationship between this policy and other policies of the organization.

The content of policies is based on the context in which an organization operates. Specifically, the following should be considered when developing any policy within the policy framework:

1. the aims and objectives of the organization;
2. strategies adopted to achieve the organization's objectives;
3. the structure and processes adopted by the organization;
4. aims and objectives associated with the topic of the policy;
5. the requirements of related higher level policies; and
6. the target group to be directed by the policy.

This is shown in Figure A.2.

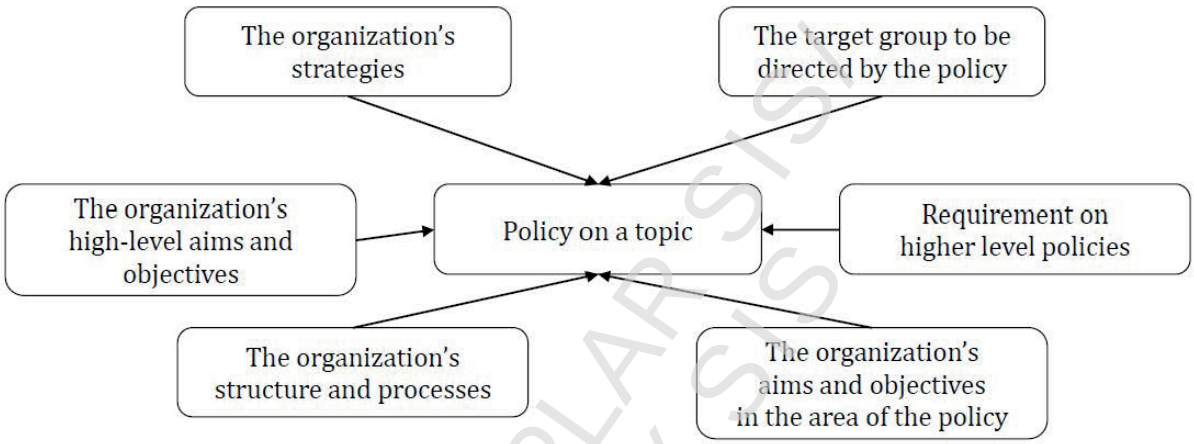


Figure A.2 — Inputs to the development of a policy

Policies can have the following structure:

a) Administrative – policy title, version, publication/validity dates, change history, owner(s) and approver(s), classification, intended audience etc.;

b) Policy summary – a one or two sentence overview. (This can sometimes be merged with the introduction.);

c) Introduction – a brief explanation of the topic of the policy;

d) Scope – describes those parts or activities of an organization that are affected by the policy. If relevant, the scope clause lists other policies that are supported by the policy;

e) Objectives – describes the intent of the policy;

f) Principles – describes the rules concerning actions and decisions for achieving the objectives. In some cases, it can be useful to identify the key processes associated with the topic of the policy and then the rules for operating the processes;

g) Responsibilities – describes who is responsible for actions to meet the requirements of the policy. In some cases, this can include a description of organizational arrangements as well as the responsibilities and authority of persons with designated roles;

h) Key outcomes – describes the business outcomes if the objectives are met. In some cases, this can be merged with the objectives;

i) Related policies – describes other policies relevant to the achievement of the objectives, usually by providing additional detail concerning specific topics; and

j) Policy requirements – describes the detailed requirements of the policy.

Policy content can be organized in a variety of ways. For example, organizations that place emphasis on roles and responsibilities may simplify the description of objectives, and apply the principles specifically to the description of responsibilities.

Bibliography

[1] ISO 19011, *Guidelines for auditing management systems*

[2] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[3] ISO/IEC 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[4] ISO/IEC 27004:2016, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[5] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[6] ISO/IEC 27007[2)], *Information technology — Security techniques — Guidelines for information security management systems auditing*

[7] ISO/IEC/TS 27008[2)], *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[8] ISO 30301, *Information and documentation — Management systems for records — Requirements*

[9] ISO 31000, *Risk management — Principles and guidelines*

2) Under preparation.

Ordlista

Här har vi samlat de förkortningar som oftast används i standardiseringssammanhang och förklarat dem kortfattat. Förkortningarna är sorterade i alfabetisk ordning.

CEN	European Committee for Standardization (Comité Européen de Normalisation). Utarbetar Europastandarder för områden som inte täcks av CENELEC.
CENELEC	European Committee for Electrotechnical Standardization (Comité Européen de Normalisation Electro-technique). Utarbetar Europastandarder inom el.
CWA	CEN/CENELEC Workshop Agreement. Tekniskt dokument utarbetat av CEN- och CENELEC-organiserad arbetsgrupp.
EN	Europastandard från CEN/CENELEC.
ETSI	European Telecommunications Standards Institute. De utarbetar Europastandarder inom telekommunikationsområdet.
FDIS	Final Draft International Standard. Slutligt förslag till global standard från IEC eller ISO.
ICS	International Classification for Standards. Ett internationellt klassificeringssystem för standarder.
IEC	International Electrotechnical Commission. Utarbetar internationell standard inom området el.
ISO	International Organization for Standardization. Utarbetar internationell standard inom alla områden utom telekommunikation och elteknik.
ITS	Informationstekniska standardiseringen. Utarbetar och bevakar standardisering inom informationsteknik. En av de svenska medlemmarna i ETSI, European Telecommunications Standards Institute.
ITU	International Telecommunication Union. Utarbetar internationella standarder inom radio och telekommunikation.
IWA	ISO Workshop Agreement. Tekniskt dokument utarbetad av ISO-organiserad arbetsgrupp.
Konsoliderad	En konsoliderad standard har sitt tillägg inarbetat och ersätter tidigare utgåva.
PAS	Publicly Available Specifications. Tekniska dokument inom IEC och ISO.
prEN	Förslag till Europastandard från CEN, CENELEC eller ETSI.
SEK	SEK Svensk Elstandard. Svarar för standardiseringen inom området el i Sverige. Svensk medlem i CENELEC och IEC.
SIS	SIS, Swedish Standards Institute. Svensk medlem i CEN och ISO.
SIS-TR	Technical Report. Teknisk rapport som beskriver resultat av undersökningar eller andra studier.
SIS-TS	Technical Specification. Teknisk specifikation som anger tekniska krav som ska uppfyllas av en produkt, process eller tjänst.
SIS-WA	SIS Workshop Agreement. Överenskommelse som ger regler, riktlinjer eller kännetecken för aktiviteter eller deras resultat.
SIS-WS	SIS Workshop. Standardiseringsprojekt med syfte att snabbt ta fram SIS Workshop Agreement.
SS	Svensk standard. Fastställs av SIS, SEK eller ITS. SS ingår som första led i beteckningen för svensk standard fastställd efter 1 januari 1978.
SS/T1	Tillägg 1 till svensk standard.
SS-EN	Europastandard fastställd som svensk standard.
SS-EN/AC	Rättelse till Europastandard fastställd som svensk standard.
SS-EN/A1	Tillägg 1 till Europastandard fastställd som svensk standard.
SS-EN ISO	Internationell standard från ISO som blivit Europastandard och fastställd som svensk standard.
SS-EN ISO/AC	Rättelse till standard från ISO som blivit Europastandard och fastställd som svensk standard.
SS-EN ISO/A1	Tillägg 1 till standard från ISO som blivit Europastandard och fastställd som svensk standard.
SS-EN ISO/IEC	Internationell standard från ISO/IEC som blivit Europastandard och fastställd som svensk standard.
SS-IEC	IEC-standard fastställd som svensk standard.
SS-ISO	ISO-standard fastställd som svensk standard.
SS-ISO Amd 1	ISO-standard fastställd som svensk standard. Tillägg 1.
SS-ISO/Cor 1	ISO-standard fastställd som svensk standard. Rättelse 1.
WD	Working Draft. Förslag till internationell standard eller Europastandard utarbetade i WG.
WG	Working Group. Arbetsgrupp tillsatt av t. ex. en internationell kommitté.
WI	Work Item. Ärende, en avgränsad arbetsuppgift som avser att resultera i en standard.

Glossary

Here are a number of the abbreviations/acronyms frequently used in standardisation contexts, with brief explanations. The abbreviations are in alphabetical order.

CEN	European Committee for Standardization (Comité Européen de Normalisation). Develops European standards for areas not covered by CENELEC.
CENELEC	European Committee for Electrotechnical Standardization (Comité Européen de Normalisation Electro-technique). Develops European standards in the electricity sector.
CWA	CEN/CENELEC Workshop Agreement. Technical document developed by CEN- and CENELEC-organised working group.
Consolidated	A consolidated standard incorporates its supplement and replaces previous editions.
EN	European standard from CEN/CENELEC.
ETSI	European Telecommunications Standards Institute. Develop European standards in the telecommunications field.
FDIS	Final Draft International Standard. Final proposal for global standard from IEC or ISO.
ICS	International Classification for Standards. An international classification system for standards.
IEC	International Electrotechnical Commission. Develops global standards in the electricity sector.
ISO	International Organization for Standardization. Develops global standards in all areas except telecommunications and electrical technology.
ITS	ITS Information Technology Standardisation. Develops and monitors standardisation in information technology. A Swedish member of the ETSI, European Telecommunications Standards Institute.
ITU	International Telecommunication Union. Develops global standards in radio and telecommunications.
IWA	ISO Workshop Agreement. Technical document developed by ISO-organised working group.
PAS	Publicly Available Specifications. Technical IEC and ISO documents.
prEN	Draft European standards from CEN, CENELEC or ETSI.
SEK	SEK Svensk Elstandard. Develops and monitors standardisation in the electrotechnical sector. Swedish member of the CENELEC and IEC.
SIS	SIS, Swedish Standards Institute. Swedish member of CEN and ISO.
SIS-TR	Technical Report. Technical report describing the results of investigations or other studies.
SIS-TS	Technical Specification. Technical specification describing what requirements a product, process or service must fulfil.
SIS-WA	SIS Workshop Agreement. An agreement setting out rules, guidelines or criteria for activities or their results.
SIS-WS	SIS Workshop. Standardisation project aimed at rapidly developing an SIS Workshop Agreement.
SS	Swedish standard. Established by SIS, SEK or ITS. SS is the first step in all standard classifications to emerge since 1 January 1978.
SS/T1	Supplement 1 to a Swedish standard.
SS-EN	European standard established as Swedish standard.
SS-EN/AC	Correction to the European standard established as Swedish standard.
SS-EN/A1	Supplement to the European standard established as Swedish standard.
SS-EN ISO	International and European standard established as Swedish standard.
SS-EN ISO/AC	Correction to the international and European standard established as Swedish standard.
SS-EN ISO/A1	Supplement to the international and European standard established as Swedish standard.
SS-EN ISO/IEC	International and European standard established as Swedish standard.
SS-IEC	IEC standard established as Swedish standard.
SS-ISO	ISO standard established as Swedish standard.
SS-ISO Amd 1	ISO standard established as Swedish standard, with Amendment 1.
SS-ISO/Cor 1	ISO standard established as Swedish standard, with Correction 1.
WD	Working Draft. Proposed international or European standard developed by the Working Group.
WG	Working Group. Appointed by an international committee or some other body.
WI	Work Item. A delimited task designed to result in a standard.

Slutanvändarlicens

VIKTIGT – LÄS NOGGRANNT IGENOM DESSA VILLKOR INNAN ANVÄNDNING SKER AV DE PRODUKTER SOM TILLHANDAHÅLLS MED DENNA LICENS. GENOM ATT ANVÄNDA PRODUKTERNA GODKÄNNER OCH ACCEPTERAR NI DÄRMED VILLKOREN I DETTA SLUTANVÄNDARLICENSAVTAL.

1. Parter
Detta slutanvändarlicensavtal (”Licensavtal”) är ingått mellan SIS och det företag och/eller den person som licensierar standarden som medföljer eller levereras under denna licens (”Kunden”).

2. Upphovsrätt till Produkten
Den produkt och dess eventuella metadata som medföljer eller levereras under detta Licensavtal (”Produkten”) är skyddad av svensk och internationell upphovsrättslagstiftning och tillhör den eller de upphovsrättsinnehavare som finns angivna på Produkten.

3. Upplåtelse av nyttjanderätt
SIS upplåter till Kunden en icke-exklusiv och icke-överlåtbar nyttjanderätt att använda Produkten enligt följande:
(a) Om Produkten levereras i pappersform har Kunden rätt att endast för internt bruk inom sin egen verksamhet att använda det exemplar av Produkten som levereras med detta Licensavtal.
(b) Om Produkten levereras i elektronisk form har Kunden rätt att endast för internt bruk inom sin egen verksamhet installera Produkten på endast en (1) dator, vilken ägs, hyrs eller kontrolleras av Kunden. Kunden har även rätt att flytta Produkten till en annan dator vilken ägs, hyrs eller kontrolleras av Kunden, under förutsättning att Produkten avinstalleras från den första datorn. Produkten får inte användas på två eller flera datorer samtidigt och inte heller i nätverk.

4. Begränsningar i nyttjanderätten
Kunden har inte rätt att under några omständigheter kopiera, anpassa, ändra, förändra, översätta, göra tillägg, uteslutningar och/eller bearbetningar i det material som utgör Produkten, hyra eller leasa ut, sälja, marknadsföra, underlicensiera eller på annat sätt distribuera, sprida eller överlåta Produkten på annat sätt än som uttryckligen anges i detta Licensavtal. Kunden får inte ta bort eller förändra någon upplysning om upphovsrätt, äganderätt och vattenmärkning som finns på Produkten och ansvarar vidare för att de upplysningar om upphovsrätt, äganderätt och vattenmärkning som finns på originalexemplaret av Produkten återges på samtliga kopior (om några) som Kunden har rätt att göra enligt detta Licensavtal. Kunden ansvarar även för att tillse att inte dess anställda (”Användare”, ”Användaren”, ”Användarna”) eller någon annan än Användarna får åtkomst till eller använder Produktens eller kopia av Produktens metadata.

5. SISs ansvar samt ansvarsbegränsning
SIS ansvarar för att innehållet i den textmassa som Produkten omfattar levereras till Kunden i det skick som den kommit SIS tillhanda. I övrigt levereras Produkten i ”befintligt skick” och SIS ansvarar inte för att den information som Produkten förmedlar är korrekt eller fullständig, eller för resultatet av användningen av Produkten.
SISs ansvar i enlighet med detta Licensavtal omfattar endast direkta skador och ej indirekta skador såsom exempelvis men inte uteslutande utebliven vinst, intäkt, besparing eller goodwill, förlust på grund av driftavbrott, förlust av data, Kundens eventuella ersättningsskyldighet gentemot tredje man eller indirekt skada eller annan följdskada av vad slag det än må vara. I inget fall ska SIS och SISs totala skadeståndsansvar enligt detta Licensavtal överstiga ett belopp motsvarande den avgift som Kunden betalat för nyttjanderätten enligt detta Licensavtal.
Kunden ska hålla SIS skadelösa för eventuella skadeståndsanspråk som påtalas av tredje man avseende Kunden och Användarens användning av Produkten. För den händelse SIS skulle tvingas utge ersättning och skadestånd med anledning av Kundens och Användarens användning av Produkten, skall Kunden omedelbart på anfordran ersätta SIS med ett belopp motsvarande det utgivna.

6. Immateriella rättigheter
Samtliga immateriella rättigheter till Produkterna och dess metadata tillkommer SIS, CEN och ISO och Kunden är medveten om att Kunden och/eller Användaren genom detta Licensavtal inte förvärvar någon som helst rätt till SIS:s, CEN:s och ISO:s upphovsskyddade Produkter och dess metadata, varumärke, domännamn, firmanamn, kännetecken, know-how, och andra immateriella rättigheter som tillhör SIS, CEN och ISO.
Kunden äger inte rätt att utan SISs skriftliga samtycke använda och marknadsföra SIS:s, CEN:s och ISO:s varumärken, logotyper, domännamn, produktbenämningar och firmanamn.
Kunden skall vidta alla de rättigheter som SIS rimligen kan kräva och vara SIS behjälplig för att SIS ska kunna upprätthålla giltigheten och genomförbarheten av SIS immateriella rättigheter under giltighetstiden för detta Licensavtal.

7. Intrång i immaterialrätt
Om det, enligt SIS föreligger risk för att krav avseende intrång i tredje mans immateriella rättigheter kan komma att ställas på grund av användningen av Produkterna, har SIS rätt att på egen bekostnad (i) utverka rätt för Kunden att fortsätta med användning av Produkten, (ii) förändra eller ersätta Produkten eller del därav med andra produkter i syfte att undvika sådant krav, eller (iii) stoppa Kundens användning av Produkten och återbetala de avgifter som erlagts för den tid då utnyttjande av Produkten inte kunnat ske.
SIS ansvarar inte gentemot Kunden för krav som kunde ha undvikits om Kunden accepterat ersättningsprodukt eller om användningen av Produkten stoppats.
Kunden skall utan dröjsmål informera SIS om intrång eller misstänkt intrång i SIS alla immateriella rättigheter som finns uppräknade i detta Licensavtal och som inte är begränsat till de marknader där Kunden är verksam på.

8. Personuppgiftsbehandling
SIS lagrar och behandlar Användarnas persondata i elektronisk form och i pappersform. Detta gör SIS för fullgörande av detta Licensavtal, för att fullgöra SISs skyldighet enligt lag eller annan författning, för fakturerings-, betalnings- och bokföringsändamål, för marknadsföringsändamål, för reklamations-hantering, för kundservice, säkerhets, sekretess- och administrationsfrågor, kvalitetsarbete, affärsutveckling för bl.a. kund- och marknadsanalyser samt för statistiska ändamål. SIS kan komma att överföra personuppgifter som härrör till Kunden och Användarna utanför SIS och till ett annat land för fullgörande av detta Licensavtal. SIS säkerställer att en adekvat skyddsnivå enligt gällande personuppgifts-regelverket uppfylls vid en sådan överföring av personuppgifterna utanför SIS och till ett annat land. Behandling av personuppgifterna kommer att ske så länge personuppgifterna behövs för de aktuella ändamålen. Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet räknas enligt Personuppgiftslagen som personuppgifter. Även bilder och ljudupptagnin**gar på i**ndivider som behandlas i dator kan vara personuppgifter även om inga namn nämns.
Kunden och dess Användare har rätt att kostnadsfritt en gång per kalenderår, efter skriftligt undertecknad ansökan av behörig Användare hos Kunden ställd till SIS, Box 45443 SE-104 31 Stockholm få besked om vilka personuppgifter som SIS behandlar som kan härledas till den behöriga Användaren ifråga, vad syftet med personuppgiftsbehandlingen är och hur SIS behandlar dennes personsdata. Behörig Användare hos Kunden har också rätt att begära rättelse i fråga om dennes personuppgifter eller kräva att SIS skall radera dennes personuppgifter. Behörig Användare hos Kunden har också rätt att få sina personuppgifter överförda till ett annat företag eller organisation (sk. dataportabilitet). Behörig Användare hos Kunden har också rätt att invända mot SISs behandling av dennes person-uppgifter och inge klagomål till Datainspektionen.

9. Export
Kunden äger inte rätt att exportera eller reexportera Produkten eller del därav, tillhörande information eller teknologi i strid med gällande svensk och annan tillämplig exportlagstiftning.

10. Avtalstid och uppsägning
Detta Licensavtal gäller tills vidare. Kunden har rätt att säga upp Licensavtalet när som helst. SIS har rätt att kan säga upp Licensavtalet till omedelbart upphörande om Kunden bryter mot bestämmelse i Licensavtalet. Då Licensavtalet upphör ska Kunden omedelbart upphöra med användningen av Produkten och förstöra samtliga kopior av denna.

11. Tillämplig lag
Svensk lag gäller för detta Licensavtal och tvister ska avgöras genom förfarande vid svensk domstol.

12. Övriga bestämmelser
Detta Licensavtal utgör en fullständig reglering av vad som avtalats mellan parterna avseende användningen av Produkten och ersätter samtliga tidigare skriftliga eller muntliga avtal, utfästelser eller överenskommelser parterna emellan.
Ändring i Licensavtalet kan endast ske genom skriftligen upprättad handling vilken undertecknats av SIS. Om en bestämmelse i Licensavtalet skulle förklaras ogiltig av någon anledning, ska Licensavtalet revideras endast i sådan omfattning som är nödvändigt för att göra Licensavtalet giltigt, och sådan revidering ska (i) inte påverka giltigheten av den ogiltigförklarande delen under andra omständigheter, eller (ii) påverka övriga delar av Licensavtalet.
SIS äger rätt att fritt överlåta samtliga sina rättigheter och skyldigheter enligt detta Avtal till moderföreningen SIS Ideell Förening.

End user license

IMPORTANT - READ CAREFULLY THROUGH THESE TERMS AND CONDITIONS BEFORE USING THE PRODUCTS PROVIDED UNDER THIS LICENSE. BY USING THE PRODUCTS, YOU APPROVE AND ACCEPT THE TERMS AND CONDITIONS OF THIS END USER LICENCE AGREEMENT.

1. The Parties
This end user licence agreement ("the License Agreement") has been entered into between SIS and the company and/or the person who licenses the standard that is included or delivered under this License Agreement ("the Customer").

2. Copyright to the Product
The product and any associated metadata that is included or delivered under this License Agreement ("the Product") is protected by Swedish and international copyright law and belongs to the copyright holder(s) stated for the Product.

3. Granting of right of use
SIS grants the Customer a non-exclusive and non-transferable right to utilise the Product as follows:
(a) If the Product is delivered in paper format, the Customer is entitled to use the copy of the Product provided within this License Agreement solely for internal use within his/her own business.
(b) If the Product is delivered in electronic format, the Customer is entitled to install the Product provided within this License Agreement on one (1) computer, which is owned, leased or controlled by the Customer, solely for internal use within his/her own business. The Customer also has the right to move the Product to another computer that is owned, leased or controlled by the Customer, provided that the Product is uninstalled from the first computer. The Product may not be used on two or more computers at the same time, nor in a network.

4. Limitations to the right of use
The Customer may not, in any event, copy, adapt, modify, alter, translate, make additions to, exclusions and/or process the material contained in the Product and/or copies of the Product, rent or lease, sell, market, sublicense or otherwise distribute, disseminate or transfer the Product and/or copies of the Product produced in any other way than as explicitly stated in this License Agreement. The Customer may not remove or change any information on copyright, proprietary rights and watermarks contained in the Product and the Customer is also responsible for ensuring that the copyright, proprietary rights and watermarks contained in the original copy of the Product are reproduced on all copies (if any) that the Customer is entitled to make under this License Agreement. The Customer is also responsible for ensuring that his/her employees ("User", "the User", "the Users") or anyone other than the Users do not have access to or use the metadata of the Product or copy of the Product.

5. Limitation of liability
SIS is only liable for ensuring that the content of the text included in the Product is delivered to the Customer in the condition in which it was received by SIS. Otherwise, the Product is delivered "as is" and SIS is not responsible for the accuracy or completeness of the information provided in the Product or for the result of the use of the Product.
SIS's liability in accordance with this Agreement includes only direct damages and not indirect damage such as loss of profit, revenue, savings or goodwill, loss due to operational disruptions, loss of data, any liability for compensation on the part of the Customer in relation to third parties or indirect damage or other consequential loss of any kind. Under no circumstances shall SIS total liability for damages under this License Agreement exceed an amount corresponding to the fee paid by the Customer for the right of use under this License Agreement.
The Customer shall indemnify SIS for any damages claimed by third parties in regard to the Customer and the User's use of the Product. In the event that SIS would have to pay compensation and damages due to the Customer's and the User's use of the Product, the Customer shall on request immediately reimburse the amount in question to SIS.

6. Intellectual property rights
All intellectual property rights to the Products and their metadata belong to SIS, CEN and ISO, and the Customer is aware that the Customer and/or the User do not acquire any right through this License Agreement to copyright protected products belonging to SIS, CEN and ISO nor to their metadata, trademark, domain name, company name, characteristics, know-how, or to other intellectual property rights of SIS, CEN and ISO.
The Customer is not entitled to use and market trademarks, logos, domain names, product names and company names belonging to SIS, CEN and ISO without the written consent of SIS.

7. Infringement of intellectual property rights
If, in the view of SIS, there is a risk that claims for infringement of third party intellectual property rights may be made as a result of the use of the Products, SIS has the right at its own expense (i) to exercise the right for the Customer to continue using the Product, (ii) change or replace the Product or part thereof with other products in order to avoid such a claim, or (iii) stop the Customer's use of the Product and refund the fees paid for the time when utilisation of the Product could not be made.
SIS are not liable to the Customer for any claims that could have been avoided if the Customer had accepted a replacement product or if the use of the Product was terminated.
The Customer shall notify SIS without delay of any infringement or suspected infringement of all intellectual property rights belonging to SIS listed in this License Agreement, and which are not limited to the markets in which the Customer operates.

8. Personal data processing
SIS process and store the User's personal data in electronic and in paper format. SIS does this for fulfillment of the terms of this License Agreement, to fulfil SIS's obligations by law and other mandatory obligations, for the purposes of billing, payment and accounting, for the purposes of marketing, for the handling of claims, for customer services, for matters relating to confidentiality and administration, quality management, business development - including for customer and market analyses, and for statistical purposes. SIS may transfer personal data belonging to the Customer and Users outside SIS and to other organizations and countries. SIS ensures that an adequate level of security in accordance with prevailing personal data legislation is met in cases of the transfer of data to other countries. Personal data will be processed as long as the personal data is required for the purpose in question. Personal data, according the Swedish Personal Data Act, refers to all types of information that can directly or indirectly be related to a living being. Even images and audio recordings of individuals processed on computers may be regarded as personal data regardless whether or not names are mentioned.
The Customer and its Users are entitled to, once a calendar year and free of charge, upon written request from the authorized User at the Customer to SIS, Box 45443 SE-104 31 Stockholm, to obtain information on what personal data SIS processes that may be related to the authorized User in question, the purpose of processing this personal data, and how the User's personal data is treated by SIS. Authorized Users at the Customer are also entitled to request corrections to their personal data, or demand that SIS delete their personal data. Authorized Users at the Customer are also entitled to have their personal data transferred to another company or organization (so-called data portability). Authorized Users at the Customer are also entitled to object to SIS's treatment of their personal data and submit a complaint to the Swedish Data Protection Authority.

9. Export
The Customer does not have the right to export or re-export the Product or part thereof, related information or technology in breach of applicable Swedish and other applicable export legislation.

10. Agreement term and termination
This Licence Agreement applies until further notice. The Customer has the right to terminate the Licence Agreement at any time. SIS has the right to terminate the License Agreement with immediate effect if the Customer is in breach of any provision in the License Agreement. Upon termination of the License Agreement, the Customer shall immediately cease the use of the Product and destroy all copies thereof.

11. Applicable law
Swedish law applies to this License Agreement and any disputes shall be settled in a Swedish court in Stockholm.

12. Other provisions
This License Agreement constitutes full regulation of that which has been agreed between the Parties regarding the use of the Product and supersedes all previous written or verbal contracts, declarations or agreements between the Parties. Changes to the License Agreement can only be made by written document signed by SIS. If a provision in the License Agreement should be declared invalid for any reason, the License Agreement shall be revised only to the extent necessary to make the License Agreement valid and such revision shall (i) not affect the validity of the part declared invalid in other circumstances, or (ii) affect other parts of the License Agreement.
SIS is entitled to freely transfer all of its rights and obligations under this Agreement to the parent association SIS Ideell Förening.

SIS, Swedish Standards Institute och SEK Svensk Elstandard leder arbetet med standardisering i Sverige. Tillsammans med företag och organisationer jobbar vi med att förenkla, förbättra, kvalitetssäkra och skapa gemensamma standarder. SIS kunder har inflytande i internationell standardisering genom CEN i Europa och ISO globalt. SEK samordnar svensk medverkan i CENELEC i Europa och IEC globalt.

Du kan få dina standarder i olika format och media, detta är ett av dem. SIS är störst i Norden på att leverera standarder och allt som rör dess tillämpning. En tryckt standard från SIS är alltid tryckt på miljövänligt papper.

Vill du veta mer om vårt utbud och tjänster? Ring oss på 08-555 523 10
eller besök oss på www.sis.se

The Swedish Standards Institute (SIS) and SEK Svensk Elstandard share principal responsibility for standardisation in Sweden. Working with various agencies, enterprises and organisations, we seek to simplify, to introduce improvements, to secure quality and to establish common standards. SIS customers influence today's international standardisation work via CEN in Europe and ISO globally. SEK coordinates Swedish participation in CENELEC in Europe and in the IEC at the global level.

You can obtain your standards in different formats and in different media – this is just one of them. SIS is the leading supplier in the Nordic area of standards and all related applications. Printed standards from SIS are always printed on eco-friendly paper.

Would you like to know more about our range of products and services?
Phone us at +46 8 555 523 10 or visit us at www.sis.se

SIS Box 45443, SE-104 31 Stockholm, Sweden
Telephone +46 8 555 523 10. Fax +46 8 555 523 11
E-post sis.sales@sis.se **www.sis.se**

SWEDISH STANDARDS INSTITUTE