SVENSK STANDARD
SS-ISO/IEC 27002:2014

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

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

Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013, IDT)

Standarder får världen att fungera

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

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

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

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

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

Standards make the world go round

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

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

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

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

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

Den internationella standarden ISO/IEC 27002:2013 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO/IEC 27002:2013 följd av den officiella engelska språkversionen.

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

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

This standard supersedes the Swedish Standard SS-ISO/IEC 27002:2005, edition 1.

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

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

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

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

Internationella standarder utarbetas i enlighet med ISO/IEC Directives, Part 2.

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

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

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

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

0 Orientering

0.1 Allmänt

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

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

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

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

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

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

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

0.2 Informationssäkerhetskrav

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

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

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

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

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

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

0.3 Val av säkerhetsåtgärder

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

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

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

0.4 Utveckla egna riktlinjer

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

0.5 Livscykelsöverväganden

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

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

0.6 Relaterade standarder

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

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

Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder

1 Omfattning

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

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

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

b) införa allmänt accepterade informationssäkerhetsåtgärder;

c) utveckla sina egna riktlinjer för hantering av informationssäkerhet.

2 Normativa hänvisningar

Följande dokument, hela eller delar av, är nödvändiga när det här dokumentet ska tillämpas. För daterade hänvisningar gäller endast den utgåva som anges. För odaterade hänvisningar gäller senaste utgåvan av dokumentet (inklusive alla tillägg).

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

3 Termer och definitioner

I detta dokument gäller de termer och definitioner som anges i SS-ISO/IEC 27000.

4 Denna standards struktur

4.1 Avsnitt

Denna standard innehåller 14 avsnitt som innehåller totalt 35 av de viktigaste säkerhetsområdena med 114 säkerhetsåtgärder.

Den inbördes ordningen på avsnitten i denna standard avspeglar inte deras betydelse. Beroende på omständigheterna kan säkerhetsåtgärder från några eller alla avsnitt vara viktiga. Därför bör varje organisation som tillämpar denna standard identifiera tillämpliga säkerhetsåtgärder för den egna organisationen. Den bör också avgöra hur viktiga dessa är samt deras tillämpning på specifika verksamhetsprocesser. Listorna i denna standard är inte heller i prioritetsordning.

4.2 Säkerhetskategorier

Varje huvudsaklig säkerhetskategori beskriver:

a) ett åtgärdsmål som anger vad som bör uppnås;

b) en eller flera säkerhetsåtgärder som kan användas för att uppnå detta mål.

Definitioner av säkerhetsåtgärder är uppbyggda på följande sätt:

Säkerhetsåtgärd

Definition av den specifika säkerhetsåtgärden i syfte att uppnå målet.

Vägledning för införande

Ger mer detaljerad information till stöd för införandet av säkerhetsåtgärden och för att uppnå målet. Det är inte givet att vägledningen är fullt lämplig eller tillräcklig i alla situationer eller att den uppfyller organisationens specifika krav.

Övrig information

Innehåller ytterligare information som kan behöva beaktas, exempelvis avseende rättsliga överväganden och hänvisningar till andra standarder. Om det inte finns övrig information att presentera utgår denna rubrik.

5 Informationssäkerhetspolicy

5.1 Ledningens inriktning för informationssäkerhet

Mål: Att delge ledningens inriktning och stöd för informationssäkerhet i enlighet med verksamhetens krav och relevanta författningar.

5.1.1 Informationssäkerhetspolicy

Säkerhetsåtgärd

Ett regelverk för informationssäkerhet, som inkluderar informationssäkerhetspolicyn, bör fastställas, godkännas av ledningen, publiceras och kommuniceras till medarbetare och relevanta externa parter.

Svensk ANM. Den engelska termen ”policys” översätts i den svenska texten med policy och vidhängande regelverk. Termen ”policy” används i översättningen enbart för organisationens övergripande informationssäkerhetspolicy. För övriga förekomster av termen ”policy” används de svenska termerna regler och regelverk. Detta överensstämmer med definitionen av policy i SS-ISO/IEC 27000 och med svenskt språkbruk.

Vägledning för införande

På den högsta nivån bör organisationerna definiera en informationssäkerhetspolicy som godkänts av högsta ledningen och som anger organisationens syn på sina mål för informationssäkerheten.

Informationssäkerhetspolicyn bör hantera de krav som härleds från:

a) verksamhetsstrategi;

b) författningar och avtal;

c) den nuvarande, och den förväntade, samlade hotbilden.

Informationssäkerhetspolicyn bör innehålla uppgifter om:

a) definition av informationssäkerhet samt mål och principer som styr all verksamhet som är relaterad till informationssäkerhet;

b) tilldelning, till definierade roller, av allmänna och särskilda ansvar för hantering av informationssäkerhet;

c) processer för att hantera avvikelser och undantag.

På en lägre nivå bör informationssäkerhetspolicyn stödjas av ämnesspecifika regler. Det ger ytterligare stöd vid införandet av informationssäkerhetsåtgärderna och de är vanligtvis uppbyggda för att tillgodose behoven hos vissa målgrupper inom en organisation eller för att täcka vissa områden.

Exempel på sådana detaljerade regelområden inkluderar:

a) styrning av åtkomst (se avsnitt 9);

b) informationsklassning (och -hantering) (se 8.2);

c) fysisk och miljörelaterad säkerhet (se avsnitt 11);

d) ämnen orienterade mot slutanvändare, såsom:

   1) tillåten användning av tillgångar (se 8.1.3);

   2) rent skrivbord och tom skärm (se 11.2.9);

   3) informationsöverföring (se 13.21);

   4) mobila enheter och distansarbete (se 6.2);

   5) begränsning av programinstallationer och användning (se 12.6.2);

e) säkerhetskopiering (se 12.3);

f) informationsöverföring (se 13.2);

g) skydd mot skadlig kod (se 12,2);

h) hantering av tekniska svagheter (se 12.6.1);

i) kryptografiska säkerhetsåtgärder (se avsnitt 10);

j) kommunikationssäkerhet (se avsnitt 13);

k) konfidentialitet och skydd av personlig information (se 18.1.4);

l) leverantörsrelationer (se avsnitt 15).

Dessa regler bör kommuniceras till medarbetare och relevanta externa parter i en form som är relevant, tillgänglig och begriplig för den avsedda läsaren, t.ex. i ett “informationssäkerhetsmedvetenhets-, utbildnings- och träningsprogram” (se 7.2.2).

Övrig information

Behovet av interna regler för informationssäkerhet varierar mellan organisationer. Interna regler är särskilt användbara för större och mer komplexa organisationer där de som definierar och godkänner de förväntade nivåerna av säkerhetsåtgärder är åtskilda från de som inför säkerhetsåtgärderna eller i situationer där en regel gäller för många olika personer eller funktioner i organisationen. Regler för informationssäkerhet kan utfärdas i en enda dokumenterad “informationssäkerhetspolicy”, eller som en uppsättning separata men relaterade dokument.

Om någon av reglerna för informationssäkerhet distribueras utanför organisationen bör försiktighet iakttas i syfte att inte lämna ut konfidentiell information.

Organisationer kan ha olika benämningar på dessa regeldokument, till exempel “normer”, “riktlinjer” eller “direktiv”.

5.1.2 Granskning av regelverk för informationssäkerhet

Säkerhetsåtgärd

Regelverket (inklusive informationssäkerhetspolicyn) för informationssäkerhet bör granskas med planerade intervall, eller om betydande förändringar sker, för att säkerställa deras fortsatta lämplighet, riktighet och verkan.

Vägledning för införande

Varje del av regelverket bör ha en ägare som har ett uttalat ansvar för utveckling, granskning och utvärdering av reglerna. Granskningen bör inkludera en bedömning av organisationens möjligheter till förbättringar av sitt regelverk och organisationens förhållningssätt till informationssäkerhet utifrån förändringar i organisationens omvärld, verksamhetsförutsättningar, legala krav och tekniska miljö.

Granskningen av informationssäkerhetspolicy och vidhängande regelverk bör ta hänsyn till utfallet av högsta ledningens genomgång.

Förändringar av informationssäkerhetspolicyn bör godkännas av högsta ledningen.

6 Organisation av informationssäkerhetsarbetet

6.1 Intern organisation

Mål: Att upprätta ett organisatoriskt ramverk för att initiera och styra införandet och driften av informationssäkerhetsarbetet inom organisationen.

6.1.1 Informationssäkerhetsroller och ansvar

Säkerhetsåtgärd

Allt ansvar för informationssäkerhet bör definieras och tilldelas.

Vägledning för införande

Tilldelningen av ansvar för informationssäkerheten bör göras i enlighet med informationssäkerhetspolicyn (se 5.1.1). Ansvar för att skydda enskilda tillgångar och för att utföra specifika informationssäkerhetsprocesser bör identifieras. Ansvar för hantering av informationssäkerhetsrisker, och i synnerhet för godkännande av kvarstående risker bör definieras. Dessa ansvarsområden bör, vid behov, kompletteras med mer detaljerade riktlinjer för specifika platser och informationsbehandlingsresurser. Lokalt ansvar för skydd av tillgångar och för att utföra särskilda processer bör definieras.

Medarbetare med tilldelat informationssäkerhetsansvar kan delegera säkerhetsuppgifter till andra. De förblir dock ändå de ytterst ansvariga och bör följa upp att alla delegerade uppgifter har utförts korrekt.

Vilka medarbetare som ansvarar för vilka områden bör förtecknas. I synnerhet bör följande ske:

a) tillgångar och informationssäkerhetsprocesser bör identifieras och definieras;

b) de enheter, eller medarbetare, som ansvarar för de aktuella tillgångarna eller informationssäkerhetsprocesserna bör fastställas. Detaljerna i detta ansvar bör vara dokumenterat (se 8.1.2);

c) behörighetsnivåer bör definieras och dokumenteras;

d) för att kunna fullgöra sitt ansvar inom informationssäkerhetsområdet bör de utsedda personerna ha kompetens inom området, samt kunna hålla sig à jour med utvecklingen;

e) koordinering och övergripande tillsyn av informationssäkerhetsaspekterna vid leverantörsrelationerna bör identifieras och dokumenteras.

Övrig information

Många organisationer utser en informationssäkerhetsansvarig som har det övergripande ansvaret för utveckling och införande av informationssäkerhet och som stöttar organisationen vid identifiering av säkerhetsåtgärder.

Ansvaret för resurser och för införandet av säkerhetsåtgärderna ligger oftast på verksamhetsansvariga. Ett vanligt tillvägagångssätt är att utse en ägare för varje tillgång som sedan blir ansvarig för det löpande skyddet.

6.1.2 Uppdelning av arbetsuppgifter

Säkerhetsåtgärd

Ansvar och ansvarsområden som står i konflikt med varandra bör åtskiljas för att minska möjligheterna för obehörig eller oavsiktlig ändring eller missbruk av organisationens tillgångar.

Vägledning för införande

Försiktighet bör iakttas så att ingen enskild person kan få tillgång till, ändra eller använda tillgångar utan tillstånd eller upptäckt. Initiering av en händelse bör skiljas från dess godkännande. Möjligheter till samverkan bör övervägas vid utformningen av säkerhetsåtgärderna.

Inom små organisationer kan det vara svårt att uppnå en korrekt fördelning av ansvar men principen bör tillämpas i den mån det är möjligt och praktiskt. När det är svårt att separera ansvaret för säkerhetsåtgärder, till exempel övervakning av aktiviteter, bör verifieringskedjor för revisionsändamål och tillsyn av ledningen övervägas.

Övrig information

Strikt uppdelning av arbetsuppgifter är en metod för att minska risken för oavsiktligt eller avsiktligt missbruk av organisationens tillgångar.

6.1.3 Kontakt med myndigheter

Säkerhetsåtgärd

Lämpliga kontakter med relevanta myndigheter bör upprätthållas.

Vägledning för införande

Organisationer bör ha rutiner som anger när och av vem myndigheter (t.ex. brottsbekämpande myndigheter, tillsynsorgan, tillsynsmyndigheter) bör kontaktas och hur identifierade informationssäkerhetsincidenter bör rapporteras vid lämplig tidpunkt (t.ex. om lagbrott misstänks).

Övrig information

Organisationer som attackeras via internet kan behöva stöd av myndigheter som vidtar åtgärder mot källan till attacken.

Att upprätthålla sådana kontakter kan vara ett krav som stöd för hanteringen av informationssäkerhetsincidenter (se avsnitt 16) eller processen för kontinuitetsplanering för verksamheten (se avsnitt 17). Kontakter med tillsynsorgan är också användbara för att förutse och förbereda sig för kommande förändringar i författningar som organisationen måste följa. Kontakt med andra organisationer inkluderar myndigheter för t.ex. räddningstjänst, sjukvård och säkerhet och brandkår (i samband med kontinuitet i verksamheten), samt leverantörer av el, vatten (i samband med kylningen av utrustning), andra tekniska försörjningssystem och teleoperatörer (i samband med linjedragning och tillgänglighet).

6.1.4 Kontakt med särskilda intressegrupper

Säkerhetsåtgärd

Lämpliga kontakter med särskilda intressegrupper eller andra forum för säkerhetsspecialister och branschorganisationer bör upprätthållas.

Vägledning för införande

Medlemskap i särskilda intressegrupper eller forum bör betraktas som ett medel för att:

a) förbättra kunskapen inom området och hålla sig uppdaterad med relevant säkerhetsinformation;

b) säkerställa att förståelsen för informationssäkerhetsmiljön är aktuell och fullständig;

c) få tidiga varningar om larm samt råd och uppdateringar avseende attacker och sårbarheter;

d) få tillgång till specialistråd avseende informationssäkerhetsfrågor;

e) dela och utbyta information om nya tekniker, produkter, hot eller sårbarheter;

f) tillhandahålla lämpliga kontaktpunkter när man behandlar informationssäkerhetsincidenter (se avsnitt16).

Övrig information

Avtal för informationsutbyte kan fastställas för att förbättra samarbete och samordning av säkerhetsfrågor. Sådana avtal bör innehålla krav för skydd av konfidentiell information.

6.1.5 Informationssäkerhet i projektledning

Säkerhetsåtgärd

Informationssäkerhet bör hanteras inom projektledning, oavsett typ av projekt.

Vägledning för införande

Informationssäkerhet bör integreras i organisationens metoder för projektledning för att säkerställa att informationssäkerhetsrisker identifieras och behandlas som delar av ett projekt. Detta gäller generellt för alla projekt oavsett deras karaktär, t.ex. projekt för verksamhetskritiska processer, IT, fastighetsförvaltning och andra stödjande processer. De metoder som projektledningen använder bör kräva att:

a) informationssäkerhetsmål ingår i projektets mål;

b) en bedömning av informationssäkerhetsrisker genomförs i ett tidigt skede av projektet för att identifiera nödvändiga säkerhetsåtgärder;

c) informationssäkerhet ingår i alla faser av den tillämpade projektmetodiken.

Informationssäkerhetsaspekter bör behandlas och ses över regelbundet i alla projekt. Ansvar för informationssäkerhet bör fastställas och tilldelas till angivna roller som är definierade i projektledningens projektmetod.

6.2 Mobila enheter och distansarbete

Mål: Att säkerställa säkerheten vid distansarbete och användning av mobila enheter.

6.2.1 Regler för mobila enheter

Säkerhetsåtgärd

Regler och stödjande säkerhetsåtgärder bör antas för att hantera de risker som användning av mobila enheter medför.

Vägledning för införande

Vid användning av mobila enheter bör särskild försiktighet iakttas för att säkerställa att verksamhetsinformation inte äventyras. Reglerna för mobila enheter bör beakta riskerna med att arbeta med mobila enheter i oskyddade miljöer.

Reglerna för mobila enheter bör hantera:

a) registrering av mobila enheter;

b) krav på fysiskt skydd;

c) begränsning av installation av program;

d) krav på programversioner för mobila enheter och på att göra uppdateringar;

e) begränsning av anslutning till informationstjänster;

f) styrning av åtkomst;

g) krypteringsteknik;

h) skydd mot skadlig kod;

i) avaktivering, radering eller låsning av konto på distans;

j) säkerhetskopiering;

k) användning av webbtjänster och webbtillämpningar.

Försiktighet bör iakttas vid användning av mobila enheter på offentliga platser, i mötesrum och på andra oskyddade områden. Skyddet bör vara på plats för att förhindra obehörig åtkomst till eller avslöjande av information som lagras och bearbetas av dessa enheter, t.ex. genom att använda krypteringsteknik (se avsnitt 10) och upprätthålla användningen av hemliga autentiseringsuppgifter (se 9.2.4).

Mobila enheter bör också vara fysiskt skyddade mot stöld särskilt när de lämnas obevakade, t.ex. i bilar och andra transportmedel, på hotellrum, i konferensanläggningar och på mötesplatser. En specifik rutin som beaktar rättsliga, försäkrings- och andra säkerhetskrav i organisationen bör fastställas vid fall av stöld eller förlust av mobila enheter. Enheter som innehåller viktig, känslig eller kritisk verksamhetsinformation bör inte lämnas utan uppsikt och om möjligt bör de vara fysiskt inlåsta eller säkrade med särskild låsanordning.

Utbildning bör ordnas för personal som använder mobila enheter för att öka deras medvetenhet om de ytterligare risker som följer av detta sätt att arbeta och vilka säkerhetsåtgärder som bör vara införda.

Om reglerna för mobila enheter tillåter användning av privatägda mobila enheter bör reglerna och de relaterade säkerhetsåtgärderna överväga:

a) separation av privat och yrkesmässig användning av enheter, inklusive användandet av program för att stödja sådan separation, samt skydda verksamhetsdata på en privat enhet;

b) att ge tillgång till verksamhetsinformation endast efter att användaren har tecknat ett avtal där slutanvändaren bekräftar sina skyldigheter (fysiskt skydd, uppdatering av program, etc.), avstår från ägandet av verksamhetsdata, tillåter radering av data på distans av organisationen i händelse av stöld eller förlust av enheten eller när användaren inte längre har rätt att använda tjänsten. Dessa regler måste ta hänsyn till lagstiftning gällande skydd av personuppgifter.

Övrig information

Mobila enheters trådlösa anslutningar liknar andra typer av nätverksanslutningar men har viktiga skillnader som bör beaktas vid identifiering av säkerhetsåtgärder. Typiska skillnader är:

a) vissa trådlösa säkerhetsprotokoll är omogna och har kända svagheter;

b) information som lagras på mobila enheter kanske inte kan säkerhetskopieras på grund av begränsad nätverksbandbredd eller på grund av att mobila enheter kanske inte kan vara anslutna på tider när säkerhetskopior är schemalagda.

Mobila enheter delar generellt vanliga funktioner, t.ex. nätverk, internet, e-post och filhantering, med fasta enheter.

6.2.2 Distansarbete

Säkerhetsåtgärd

Regler och stödjande säkerhetsåtgärder bör införas för att skydda information som nås, bearbetas eller lagras på distansarbetsplatser.

Vägledning för införande

Organisationer som tillåter distansarbete bör utfärda regler som definierar villkor och restriktioner för distansarbete. När det anses tillämpligt och tillåtet enligt lag bör följande övervägas:

a) den befintliga fysiska säkerheten för distansarbetsplatsen med beaktande av den fysiska säkerheten för byggnaden och den lokala miljön;

b) den föreslagna fysiska distansarbetsmiljön;

c) säkerhetskrav för kommunikation, med hänsyn tagen till behovet av fjärråtkomst till organisationens interna system, känsligheten avseende den information som kommer att nås och passera över kommunikationslänken och känslighet i det inre systemet;

d) tillhandahållande av virtuella skrivbord som förhindrar bearbetning och lagring av information med privatägd utrustning;

e) hotet för obehörig åtkomst till information eller resurser, från andra personer på distansarbetsplatsen, t.ex. familj och vänner;

f) användning av privata nätverk och kraven eller begränsningarna på konfigurationen av trådlösa nätverkstjänster;

g) regler och rutiner för att förebygga tvister om immateriella rättigheter för material som har utvecklats på privatägd utrustning;

h) tillgång till privatägd utrustning (för att styra säkerheten på maskinen eller vid en förundersökning), som ej medges av lagstiftning;

i) licensavtal för program som är av den naturen att organisationen kan bli ansvarig för licensiering för klientprogram på arbetsstationer som ägs privat av anställda eller extern part;

j) kravställningen på skydd mot skadlig kod samt brandvägg.

De riktlinjer och arrangemang som bör beaktas bör omfatta:

a) tillhandahållande av lämplig utrustning och förvaringsmöbler för distansarbete där användningen av privatägd utrustning som inte styrs av organisationen inte är tillåten;

b) en definition av tillåtet arbete, arbetstid, klassificeringen av information som kan lagras och de interna system och tjänster som distansarbetaren är auktoriserad att få tillgång till;

c) tillhandahållande av lämplig utrustning inbegripet metoder för att säkra fjärråtkomst;

d) fysisk säkerhet;

e) regler och vägledning om familj och besökares tillgång till utrustning;

f) tillhandahållande av hårdvara och program samt underhåll;

g) tillhandahållande av försäkring;

h) rutiner för säkerhetskopiering och för verksamhetens kontinuitet;

i) revision och säkerhetsövervakning;

j) återkallande av tillstånd och nyttjanderätt samt återlämnande av utrustningen när distansarbetet upphör.

Övrig information

Distansarbete avser alla former av arbete utanför kontoret, inklusive icke-traditionella arbetsmiljöer, benämnda “distansarbete”, “flexibel arbetsplats”, “distansarbete” och “virtuella arbetsmiljöer”.

7 Personalsäkerhet

7.1 Före anställning

Mål: Att säkerställa att anställda och leverantörer förstår sitt ansvar och är lämpliga för de roller de är tilltänkta för.

7.1.1 Bakgrundskontroll

Säkerhetsåtgärd

Bakgrundskontroll på alla sökande för anställning bör utföras i enlighet med relevanta författningar och etiska krav och bör stå i proportion till verksamhetskraven, klassificeringen av information som de ges behörighet till och de upplevda riskerna.

Vägledning för införande

Vid verifiering bör hänsyn tas till all relevant lagstiftning gällande integritet, skydd av personuppgifter och anställningar. Verifiering bör, där så är tillåtet, inkludera följande:

a) tillgång till fullgoda referenser, t.ex. en arbetsrelaterad och en personlig;

b) verifiering (för fullständighet och riktighet) av den sökandes meritförteckning;

c) bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer;

d) oberoende identitetsverifiering (pass, körkort, nationellt id-kort eller motsvarande);

e) förstärkt kontroll, t.ex. kreditupplysning eller kontroll i brottsregister.

När en person anställs för en specifik informationssäkerhetsroll, bör organisationer säkerställa att den ansökande:

a) har den nödvändiga kompetensen för att utföra säkerhetsrollen;

b) är betrodd att få rollen speciellt om rollen är avgörande för organisationen.

När ett arbete, antingen vid den ursprungliga tillsättningen eller vid befordran medför att personen får tillgång till informationsbehandlingsresurser, och i synnerhet om dessa hanterar konfidentiell information, t.ex. finansiell information eller strängt konfidentiell information, bör organisationen också överväga ytterligare, mer detaljerade kontroller.

Rutinerna bör definiera kriterier och begränsningar för kontroll, t.ex. vem som är kvalificerad att utföra bakgrundskontroll, samt hur, när och varför verifieringsåtgärder utförs.

Bakgrundskontroll bör också genomföras av leverantörer. I dessa fall bör avtalet mellan organisationen och leverantören ange ansvar för att genomföra bakgrundskontroll och den anmälningsrutin som måste följas om kontrollen inte har fullföljts eller om resultatet ger anledning till tvivel eller osäkerhet.

Information om alla sökande som övervägs för befattningar inom organisationen bör samlas in och hanteras i enlighet med tillämplig gällande lagstiftning i den aktuella jurisdiktionen. Beroende på tillämplig lagstiftning bör kandidaterna informeras i förväg om aktiviteterna för bakgrundskontroll.

7.1.2 Anställningsvillkor

Säkerhetsåtgärd

Avtal med anställda och leverantörer bör ange deras och organisationens ansvar för informationssäkerhet.

Vägledning för införande

Avtalsenliga skyldigheter för anställda eller leverantörer bör återspegla organisationens informationssäkerhetspolicy och tillhörande regelverk samt klargöra och fastställa:

a) att alla anställda och leverantörer som får tillgång till konfidentiell information undertecknar en överenskommelse om konfidentialitet eller om "tystnadsplikt" innan åtkomst beviljas till informationsbehandlingsresurser (se 13.2.4);

b) den anställdes eller leverantörens juridiska ansvar och rättigheter, t.ex. avseende upphovsrättslagar eller datalagar (18.1.4);

c) ansvar för klassificering av information och hantering av organisatoriska tillgångar som är relaterade till information, informationsbehandlingsresurser och informationstjänster som hanteras av den anställde eller leverantören (se avsnitt 8);

d) ansvar för den anställde eller leverantören för hantering av information från andra företag eller externa parter;

e) åtgärder som bör vidtas om den anställde eller leverantören inte uppfyller organisationens säkerhetskrav (se 7.2.3).

Roller och ansvar för informationssäkerhet bör kommuniceras till den sökande under anställningsprocessen.

Organisationen bör säkerställa att anställda och leverantörer godtar villkor och förhållanden avseende informationssäkerhet som är anpassade till den typ och omfattning av åtkomst de kommer att ha till de av organisationens tillgångar som är relaterade till informationssystem och -tjänster.

Där så är lämpligt bör ansvar som ingår i anställningsvillkoren fortsätta att gälla under en bestämd period efter anställningens slut (se 7.3).

Övrig information

En uppförandekod kan användas för att ange den anställdes eller en leverantörs ansvar i fråga om konfidentialitet, dataskydd, etik, godtagbar användning av organisationens utrustning och resurser såväl som det moraliska uppträdande som organisationen förväntar sig. Leverantören kan ha koppling till en extern organisation som i sin tur kan avkrävas att teckna avtal för den persons räkning som avtalet avser.

7.2 Under anställning

Mål: Att säkerställa att anställda och leverantörer är medvetna om och uppfyller sitt ansvar för informationssäkerhet.

7.2.1 Ledningens ansvar

Säkerhetsåtgärd

Ledningen bör kräva att alla anställda och leverantörer tillämpar informationssäkerhetskrav i enlighet med för organisationen fastställda regler och rutiner.

Vägledning för införande

Ledningens ansvar bör inkludera att se till att anställda och leverantörer:

a) är tillräckligt informerade om sina roller och ansvar ifråga om informationssäkerhet innan de ges åtkomst till känslig information eller informationssystem;

b) erhåller riktlinjer som anger förväntningarna för deras roll avseende informationssäkerheten inom organisationen;

c) är motiverade att uppfylla organisationens informationssäkerhetspolicy och tillhörande regelverk;

d) har en nivå av medvetenhet om informationssäkerhet som är relevant för deras roller och ansvar inom organisationen (se 7.2.2);

e) uppfyller anställningsvillkoren som omfattar organisationens informationssäkerhetspolicy samt lämpliga arbetsmetoder;

f) upprätthåller lämpliga kunskaper och kvalifikationer samt utbildas regelbundet;

g) tillhandahåller en anonym rapporteringskanal för att kunna rapportera överträdelser mot informationssäkerhetspolicyn, tillhörande regelverk eller rutiner (“whistle-blower”).

Ledningen bör visa sitt stöd för informationssäkerhetspolicyn och tillhörande regelverk, rutiner och säkerhetsåtgärder och fungera som en förebild.

Övrig information

Om anställda och leverantörer inte görs medvetna om sitt informationssäkerhetsansvar kan de orsaka avsevärd skada för en organisation. Motiverad personal är sannolikt mer pålitlig och orsakar färre informationssäkerhetsincidenter än omotiverad personal.

Bristfällig ledning av organisationen kan orsaka att personal känner sig undervärderad vilket kan ge en negativ inverkan på organisationens informationssäkerhet. Bristfällig ledning kan t.ex. leda till att informationssäkerheten försummas eller potentiellt missbruk av organisationens tillgångar.

7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet

Säkerhetsåtgärd

Alla organisationens anställda och i förekommande fall leverantörer bör erhålla lämplig utbildning och fortbildning för ökad medvetenhet och regelbundna uppdateringar vad gäller organisationens policy, regelverk och rutiner i den omfattning som är relevant för deras befattning.

Vägledning för införande

Ett program för medvetenhet avseende informationssäkerhet bör ha som målsättning att göra anställda och i tillämpliga fall leverantörer medvetna om sitt ansvar för informationssäkerhet och hur detta ansvar kan uppfyllas.

Ett utbildningsprogram bör fastställas i enlighet med organisationens informationssäkerhetspolicy, tillhörande regelverk och relevanta rutiner, med beaktande av att organisationens information bör skyddas och av de säkerhetsåtgärder som har införts för att skydda informationen. Utbildningsprogrammet bör omfatta ett antal kunskapshöjande aktiviteter såsom kampanjer (t.ex. en “Informationssäkerhetsdag”) och utfärdande av broschyrer eller nyhetsbrev.

Utbildningsprogrammet bör planeras med beaktande av de anställdas roller i organisationen och i tillämpliga fall organisationens förväntan på medvetenhet hos entreprenörer. Aktiviteterna i utbildningsprogrammet bör planeras över tid, helst regelbundet, så att programmet upprepas och täcker in nya medarbetare och entreprenörer. Utbildningsprogrammet bör också uppdateras regelbundet så att det förblir i linje med organisatoriska regler och rutiner och det bör byggas på lärdomarna från informationssäkerhetsincidenter.

Utbildning bör utföras i enlighet med organisationens program för medvetenhet avseende informationssäkerhetsfrågor. Utbildningen kan ges på olika sätt, såsom klassrumsbaserad, distansutbildning, webb-baserat och självstudier.

Informationssäkerhetsutbildningen bör också omfatta allmänna aspekter såsom:

a) ledningens engagemang för informationssäkerhet inom hela organisationen;

b) behovet av att bekanta sig med och följa gällande informationssäkerhetsregler och skyldigheter som är definierade i policy, standarder, författningar, avtal och överenskommelser;

c) personligt ansvar för sina egna handlingar och passivitet samt allmänna skyldigheter mot att säkra eller skydda information som tillhör organisationen och externa parter;

d) grundläggande informationssäkerhetsrutiner (t.ex. rapportering av informationssäkerhetsincidenter) och grundläggande säkerhetsåtgärder (såsom lösenordsskydd, skydd för skadliga program och renstädat skrivbord);

e) kontaktpunkter och resurser för ytterligare information och råd i frågor gällande informationssäkerhet, inbegripande ytterligare informationssäkerhetsutbildning och utbildningsmaterial.

Informationssäkerhetsutbildning bör ske regelbundet. Grundutbildningen riktar sig till dem som får nya positioner eller roller med väsentligt andra krav på informationssäkerhet, inte bara till nybörjare och utbildningen bör genomföras innan personen blir aktiv i sin nya roll.

Organisationen bör utveckla utbildningsprogrammet i syfte att genomföra utbildningen på ett verkningsfullt sätt. Programmet bör vara i linje med organisationens informationssäkerhetspolicy, tillhörande regelverk och relevanta rutiner, med hänsyn tagen till den information som organisationen bör skydda och de säkerhetsåtgärder som införts för att skydda informationen. Programmet bör överväga olika former av utbildning, t.ex. föreläsningar eller självstudier.

Övrig information

Vid skapandet av ett utbildningsprogram är det viktigt att inte bara fokusera på “vad” och “hur” men också “varför”. Det är viktigt att medarbetarna förstår syftet med informationssäkerhet och de potentiella konsekvenserna, positiva som negativa, på organisationen av sitt eget beteende.

Medvetenhetsutbildning kan vara en del av eller bedrivas i samband med andra utbildningsaktiviteter, exempelvis allmän IT eller säkerhetsutbildning. Medvetenhetsutbildningens aktiviteter bör vara lämpliga och relevanta för enskilda roller, ansvar och kompetenser (se 7.2.2).

En utvärdering av medarbetarnas förståelse kan genomföras i slutet av en medvetenhetsutbildning för att testa kunskapsöverföringen.

7.2.3 Disciplinär process

Säkerhetsåtgärd

Det bör finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsregler.

Vägledning för införande

Den disciplinära processen bör inte påbörjas utan att det är verifierat att någon har brutit mot informationssäkerhetskraven.

Den formella disciplinära processen bör säkerställa korrekt och rättvis behandling för anställda som misstänks ha brutit mot informationssäkerhetskrav. Den formella disciplinära processen bör innehålla en gradering av respons som, oavsett om detta är ett första eller återkommande brott, beaktar faktorer såsom typ av överträdelse, allvarlighetsgrad och inverkan på verksamheten samt relevant lagstiftning, affärsavtal, huruvida förövaren hade tillräcklig utbildning och andra relevanta faktorer.

Den disciplinära processen bör också användas för att förhindra anställa från överträdelser av informationssäkerhetspolicy och tillhörande regelverk eller informationssäkerhetsrutiner eller på annat sätt skada informationssäkerheten.

Avsiktliga överträdelser kan kräva omedelbara åtgärder.

Övrig information

Den disciplinära processen kan också bidra till motivation eller vara ett incitament om belöningar definieras för ett utmärkt beteende när det gäller informationssäkerhet.

7.3 Avslut eller ändring av anställning

Mål: Att skydda organisationens intressen som en del av processen för att ändra eller avsluta anställning.

7.3.1 Avslut eller ändring av anställds ansvar

Säkerhetsåtgärd

Ansvar för informationssäkerhet och skyldigheter som förblir gällande efter avslut eller ändring av anställning, bör definieras och kommuniceras till den anställde eller leverantören samt verkställas.

Svensk ANM: Svensk arbetsrätt är styrande vid uppsägning eller ändring av anställning.

Vägledning för införande

Kommunikationen avseende ansvar vid upphörande av anställning bör omfatta gällande krav avseende informationssäkerhet och rättsliga skyldigheter och, när så är lämpligt det ansvar som ingår i överenskommelse om konfidentialitet (se 13.2.4) och anställningsvillkor (se 7.1.2) för en definierad period som fortsätter efter utgången av den anställdes eller leverantörens avtal.

Ansvar och skyldigheter som fortfarande är giltiga efter upphörande av anställning bör ingå i den anställdes anställningsvillkor eller leverantörens avtalsvillkor (se 7.1.2).

Förändringar av ansvar eller anställning bör hanteras som avslutning av det nuvarande ansvaret eller anställningen i samband med inledandet av det nya ansvaret eller anställningen.

Övrig information

Personalfunktionen ansvarar vanligtvis för den övergripande anställningsprocessen och arbetar tillsammans med den närmaste chefen till den person som slutar för att hantera informationssäkerhetsaspekterna i de relevanta rutinerna. För det fallet att en entreprenör tillhandahålls via en extern part genomförs uppsägningsprocessen av den externa parten i enlighet med avtalet mellan organisationen och den externa parten.

Det kan vara nödvändigt att informera anställda, kunder eller leverantörer om förändringar avseende personal och drift.

8 Hantering av tillgångar

8.1 Ansvar för tillgångar

Mål: Att identifiera organisationens tillgångar och fastställa lämpligt ansvar för att skydda dem.

8.1.1 Inventering av tillgångar

Säkerhetsåtgärd

Tillgångar som är relaterade till information och informationsbehandlingsresurser bör identifieras och en förteckning över dessa tillgångar bör upprättas och underhållas.

Vägledning för införande

En organisation bör identifiera de tillgångar som är relevanta i livscykeln för information och dokumentera deras betydelse för organisationen. Livscykeln för information bör omfatta skapande, bearbetning, lagring, överföring, radering och förstörelse. Den dokumenterade informationen bör underhållas i särskilda eller befintliga register beroende på vad som är lämpligt.

Förteckningen över tillgångar bör vara korrekt, uppdaterad, konsistent och överensstämma med övriga register.

För varje identifierad tillgång bör ägare utses (se 8.1.2) och klassificering göras (se 8.2).

Övrig information

Inventering av tillgångar bidrar till att säkerställa ett verkningsfullt skydd och kan också krävas för andra ändamål såsom för hälsa och säkerhet, försäkringar eller finansiella (hantering av tillgångar) skäl.

SS-ISO/IEC 27005[11] ger exempel på tillgångar som kan behöva övervägas av organisationen vid identifiering av tillgångar. Processen att sammanställa ett register över tillgångar är en viktig förutsättning för riskhantering (se även SS-ISO/IEC 27000 och SS-ISO/IEC 27005[11]).

8.1.2 Ägarskap av tillgångar

Säkerhetsåtgärd

Tillgångar som återfinns i sammanställningen bör tilldelas ägare.

Vägledning för införande

Medarbetare såväl som andra organisationsenheter som har accepterat förvaltningsansvar för tillgångens livscykel har kvalificerat sig för att tilldelas ägarskap över tillgången.

En process för att säkerställa snabb överföring av tillgångar till ägare införs vanligtvis. Ägarskap bör tilldelas när tillgångar skapas eller när tillgångar överförs till organisationen. Tillgångens ägare bör ansvara för en korrekt förvaltning av en tillgång över dess livscykel.

Tillgångens ägare bör:

a) se till att tillgångarna är inventerade;

b) säkerställa att tillgångar på lämpligt sätt klassificeras och skyddas;

c) definiera och periodvis granska åtkomstbegränsningar och klassificeringar avseende viktiga tillgångar, med hänsyn tagen till gällande regler för åtkomststyrning;

d) säkerställa korrekt hantering när tillgången tas bort eller förstörs.

Övrig information

Identifierad ägare kan vara antingen en person eller en enhet som har accepterat förvaltningsansvar för att styra hela livscykeln för en tillgång. Identifierade ägare har inte nödvändigtvis någon äganderätt till tillgången.

Rutinuppgifter kan delegeras, t.ex. till någon som ansvarar för översyn av tillgångar på daglig basis, men ansvaret ligger hos ägaren.

I komplexa informationssystem kan det vara bra att fastställa grupper av tillgångar som tillsammans tillhandahåller en viss tjänst. I detta fall är ägaren av denna tjänst ansvarig för leverans av tjänsten, inklusive driften av dess tillgångar.

8.1.3 Tillåten användning av tillgångar

Säkerhetsåtgärd

Regler för tillåten användning av information och tillgångar som är relaterade till information och informationsbehandlingsresurser bör identifieras, dokumenteras och införas.

Vägledning för införande

Anställda och externa användare som använder eller har tillgång till organisationens tillgångar bör göras medvetna om de krav avseende informationssäkerhet som gäller för de av organisationens tillgångar som är förknippade med information och informationsbehandlingsresurser. De bör ansvara för sin användning av alla resurser för informationsbearbetning och all sådan användning som genomförs under deras ansvar.

8.1.4 Återlämnande av tillgångar

Säkerhetsåtgärd

Alla anställda och externa användare bör återlämna alla organisationens tillgångar som de förfogar över då deras anställning, uppdrag eller avtal upphör.

Vägledning för införande

Avslutningsprocessen bör formaliseras och inkludera återlämnande av alla tidigare utställda fysiska och elektroniska tillgångar som ägs av, eller har anförtrotts organisationen.

I de fall en anställd eller en extern användaren köper organisationens utrustning eller använder privat utrustning, bör rutiner finnas för att säkerställa att all relevant information överförs till organisationen och säkert raderas från utrustningen (se 11.2.7).

I fall där en anställd eller en extern användare har kunskap som är viktig för pågående verksamhet, bör informationen dokumenteras och överföras till organisationen.

Under uppsägningstiden bör organisationen skydda sig mot obehörig kopiering av relevant information (t.ex. som omfattas av immateriella rättigheter) av uppsagda anställda och entreprenörer.

8.2 Informationsklassning

Mål: Att säkerställa att information får en lämplig skyddsnivå i enlighet med dess betydelse för organisationen.

8.2.1 Klassning av information

Säkerhetsåtgärd

Information bör klassas i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering.

Vägledning för införande

Klassning och tillhörande säkerhetsåtgärder för informationen bör ta hänsyn till verksamhetens behov av spridning eller begränsning av informationen samt till de legala kraven. Andra tillgångar än information kan också klassas i överensstämmelse med klassningen av den information som är lagrad i, behandlas av eller på annat sätt hanteras eller skyddas av tillgången.

Ägare av informationstillgångar bör ansvara för deras klassning.

Modellen för informationsklassning bör omfatta regler för klassning samt kriterier för granskning av klassificering över tid. Skyddsnivån i modellen bör bedömas genom att analysera konfidentialitet, riktighet och tillgänglighet samt andra krav för den aktuella informationen. Modellen bör anpassas till regler för styrning av åtkomst (se 9.1.1).

Varje nivå bör ges ett namn som passar i det sammanhang där klassningsmodellen tillämpas.

Modellen bör vara gemensam för hela organisationen så att alla klassar information och relaterade tillgångar på samma sätt och därmed skapa en gemensam förståelse för krav på skydd och för tillämpningen av lämpliga skydd.

Klassningen bör ingå i organisationens processer och vara konsekvent och sammanhängande i organisationen. Resultatet av klassningen bör ange värdet av tillgångar beroende på deras känslighet och betydelse för organisationen, t.ex. när det gäller konfidentialitet, riktighet och tillgänglighet. Resultatet av klassningen bör uppdateras vid ändringar av tillgångens värde, känslighet och betydelse under dess livscykel.

Övrig information

Klassningen ger dem som arbetar med information en tydlig indikation på hur den bör hanteras och skyddas. Att skapa grupper av information med liknande behov av skydd och specificera informationssäkerhetsrutiner som gäller för all information i varje grupp underlättar detta. Detta tillvägagångssätt minskar behovet av att utföra en riskbedömning från fall till fall samt egendesign av säkerhetsåtgärderna.

Information kan upphöra att vara känslig eller kritisk efter en viss tidsperiod, t.ex. när information har offentliggjorts. Dessa aspekter bör beaktas eftersom överdriven klassning kan leda till införandet av onödiga säkerhetsåtgärder vilket resulterar i extra kostnader medan motsatsen kan äventyra uppnåendet av verksamhetsmålen.

Ett exempel på ett klassningsschema avseende konfidentialitet skulle kunna baseras på följande fyra nivåer:

a) utlämnande eller röjande orsakar ingen skada;

b) utlämnande eller röjande orsakar mindre problem eller mindre olägenheter för verksamheten;

c) utlämnande eller röjande har en betydande kortsiktig effekt på verksamheten eller taktiska mål;

d) utlämnande eller röjande har en allvarlig inverkan på långsiktiga strategiska mål eller äventyrar organisationens överlevnad.

8.2.2 Märkning av information

Säkerhetsåtgärd

En lämplig uppsättning rutiner för märkning av information bör utvecklas och införas i enlighet med den modell för informationsklassning som antagits av organisationen.

Vägledning för införande

Rutiner för märkning av information måste omfatta information och dess relaterade tillgångar i fysiska och elektroniska format. Märkningen bör återspegla den modell för klassning som fastställts i 8.2.1. Markeringen bör vara lätt att känna igen. Rutinerna bör ge vägledning om var och hur märkningen är kopplad med tanke på hur informationen nås eller hur tillgångar hanteras beroende på typ av media. Rutiner kan definiera fall där märkning utelämnas t.ex. märkning av icke-konfidentiell information för att minska arbetsbelastning. Anställda och leverantörer bör göras medvetna om rutiner för märkning.

Utdata från system som innehåller information som klassas som känslig eller kritisk bör bära en lämplig klassningsmärkning.

Övrig information

Märkning av klassad information är en viktig förutsättning för att upprätta informationsutbyte. Fysiska etiketter och metadata är vanliga former av märkning.

Märkning av information och dess relaterade tillgångar kan ibland ha negativa effekter. Konfidentiella tillgångar är lättare att identifiera och därmed att stjäla för insiders eller externa angripare.

8.2.3 Hantering av tillgångar

Säkerhetsåtgärd

Rutiner för hantering av tillgångar bör utvecklas och införas i enlighet med den modell för informationsklassning som antagits av organisationen.

Vägledning för införande

Rutiner som överensstämmer med informationens klassning bör upprättas för hantering, bearbetning, lagring och kommunikation av information (se 8.2.1).

Följande bör övervägas:

a) begränsningar av åtkomst för att stödja behovet av skydd för varje klassningsnivå;

b) underhåll av dokumenterad information avseende godkända mottagare av tillgångar;

c) skydd av tillfälliga eller permanenta kopior av information till en nivå som överensstämmer med skyddet av den ursprungliga informationen;

d) IT-tillgångar lagras i överensstämmelse med tillverkarens specifikationer;

e) tydlig märkning på alla kopior av media som information till den avsedda mottagaren.

Den modell för klassning som används inom organisationen kanske inte motsvarar de modeller som används av andra organisationer även om namnen för nivåer är likartade. Information som rör sig mellan organisationer kan dessutom variera avseende klassning beroende på dess sammanhang i varje organisation, även om deras modeller för klassning är identiska.

Överenskommelser med andra organisationer som omfattar informationsutbyte bör omfatta rutiner för att fastställa klassning av denna information och för att uttolka klassningsmarkeringar från andra organisationer.

8.3 Hantering av lagringsmedia

Mål: Att förhindra obehörigt röjande, modifiering, avlägsnande eller destruktion av information som lagras på media.

8.3.1 Hantering av flyttbara lagringsmedia

Säkerhetsåtgärd

Rutiner bör införas för hantering av flyttbara lagringsmedia i enlighet med den modell för informationsklassning som antagits av organisationen.

Vägledning för införande

Följande riktlinjer för hantering av flyttbara media bör övervägas:

a) innehållet i alla återanvändningsbara media som avses att avlägsnas från organisationen bör, när det inte längre behövs, göras omöjligt att återskapa;

b) där så krävs och är praktiskt bör tillstånd krävas för att avlägsna media från organisationen och avlägsnandet bör registreras för att upprätthålla en verifieringskedja;

c) alla medier bör lagras i en säker och skyddad miljö som överensstämmer med tillverkarens specifikationer;

d) om konfidentialitet och riktighet för data är viktigt att överväga bör krypteringsteknik användas för att skydda data på flyttbara media;

e) för att minska risken för att media försämras medan lagrade data fortfarande behövs bör data överföras till nytt media innan den blir oläslig;

f) värdefull data bör lagras i flera kopior på olika medier för att ytterligare minska risken för skada eller förlust av data orsakad av tillfälligheter;

g) registrering av flyttbara media bör övervägas för att begränsa risken för förlust av data;

h) flyttbara medieenheter bör endast aktiveras om det finns ett verksamhetsskäl för detta;

i) där det finns behov av att använda flyttbara media bör överföring av information till sådana medier övervakas.

Rutiner och behörighetsnivåer bör dokumenteras.

8.3.2 Avveckling av lagringsmedia

Säkerhetsåtgärd

Lagringsmedia bör avvecklas på ett säkert sätt när det inte längre behövs med stöd av formella rutiner.

Vägledning för införande

Formella rutiner för säker avveckling av lagringsmedia bör fastställas för att minimera risken för läckage av konfidentiell information till obehöriga personer. Rutiner för säker avveckling av lagringsmedia som innehåller konfidentiell information bör stå i proportion till känsligheten hos den informationen. Följande bör övervägas:

a) media som innehåller konfidentiell information bör lagras och avvecklas på ett säkert sätt, t.ex. genom förbränning eller fragmentering, eller så kan data raderas för användning av en annan tillämpning inom organisationen;

b) rutiner bör vara på plats för att identifiera de lagringsmedia som kan komma att kräva säker avveckling;

c) det kan vara lättare om alla lagringsmedia samlas och avvecklas på ett säkert sätt hellre än att försöka att skilja ut känsliga föremål;

d) många organisationer erbjuder insamling och avveckling av lagringsmedia som tjänst och val av en lämplig extern part med tillräckliga säkerhetsåtgärder och erfarenhet bör ske med omsorg;

e) avveckling av känsliga lagringsmedia bör loggas för att bibehålla en verifieringskedja.

När lagringsmedia för avveckling ackumuleras och sammanförs bör det övervägas huruvida denna aggregation kan orsaka att en stor mängd icke-känsliga uppgifter tillsammans blir känsliga.

Övrig information

Skadade lagringsmedia som innehåller känsliga data kan kräva en riskbedömning för att avgöra om enheterna bör förstöras fysiskt snarare än skickas för reparation eller kassation (se 11.2.7).

8.3.3 Transport av fysiska lagringsmedia

Säkerhetsåtgärd

Lagringsmedia som innehåller information bör skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport.

Vägledning för införande

Följande riktlinjer anses skydda media som innehåller information som transporteras:

a) användning av pålitlig transport eller bud;

b) en förteckning över auktoriserade bud, godkända av ledningen;

c) rutiner för identifiering av bud bör utvecklas;

d) för att skydda media från fysiska skador som kan uppstå under transporten bör lagringsmediet förpackas på ett lämpligt sätt för att skydda och i enlighet med tillverkarens rekommendationer. Det bör t.ex. skydda mot miljömässig påverkan som kan minska mediets lagringsförmåga såsom exponering för värme, fukt eller elektromagnetiska fält;

e) hålla loggar som specificera innehållet i lagringsmedia, tillämpat skydd samt registrering av tidpunkt för överlämnande till kurir och kvitton på mottagande vid överlämningen.

Övrig information

Information kan utsättas för obehörig åtkomst, missbruk eller korruption under fysisk transport, t.ex. när lagringsmedia skickas via post eller bud. I denna säkerhetsåtgärd inkluderar media pappersdokument.

När konfidentiell information på media inte är krypterad bör ytterligare fysiskt skydd av media övervägas.

9 Styrning av åtkomst

9.1 Verksamhetskrav för styrning av åtkomst

Mål: Att begränsa åtkomst till information och informationsbehandlingsresurser.

9.1.1 Regler för styrning av åtkomst

Säkerhetsåtgärd

Regler för styrning av åtkomst bör upprättas, dokumenteras och vara föremål för uppföljning utifrån verksamhets- och informationssäkerhetskrav.

Vägledning för införande

Tillgångens ägare bör fastställa lämpliga regler för styrning av åtkomst, rättigheter och begränsningar för specifika roller. Detaljrikedomen och hur stränga säkerhetsåtgärderna är bör avspegla de säkerhetsrisker som är förknippande med informationen.

Åtkomstkontroller är både logiska och fysiska (se avsnitt 11) och dessa bör beaktas tillsammans. Användare och tjänsteleverantörer bör ges ett tydligt besked om vilka verksamhetsmässiga krav som bör uppfyllas genom åtkomstkontroller.

Reglerna bör ta hänsyn till följande:

a) säkerhetskrav för verksamhetstillämpningar;

b) regler för informationsspridning och auktorisering, exempelvis utgående från principen om vad individen behöver veta, informationssäkerhetsnivåer och klassning av information (se 8.2);

c) överensstämmelse mellan åtkomsträttigheter och regler för informationsklassning för olika system och nätverk;

d) relevant lagstiftning och alla avtalsenliga skyldigheter när det gäller begränsning av tillgång till data eller tjänster (se 18.1);

e) förvaltning av åtkomsträttigheter i en distribuerad och nätverksansluten miljö som känner igen alla typer av tillgängliga anslutningar

f) uppdelning av roller för åtkomst, t.ex. begäran om åtkomst, tillstånd till åtkomst, behörighetsadministration;

g) krav för formellt godkännande av begäran om åtkomst (se 9.2.1);

h) krav för regelbunden översyn av åtkomsträttigheter (se 9.2.5);

i) borttagande av behörigheter (se 9.2.6);

j) arkivering av dokumenterad information över alla viktiga händelser rörande användning och hantering av användaridentiteter och hemlig autentiseringsinformation;

k) roller med privilegierad åtkomst (se 9.2.3).

Övrig information

Försiktighet bör iakttas vid angivande av regler för styrning av åtkomst med hänsyn tagen till:

a) att upprätta regler som baseras på förutsättningen “allt är generellt förbjudet om det inte uttryckligen tillåts” snarare än den svagare regeln “allt är generellt tillåtet såvida det inte är uttryckligen förbjudet”;

b) ändringar i klassningsmärkning (se 8.2.2) som initieras automatiskt av resurser för informationsbearbetning och de som initieras efter användares eget gottfinnande;

c) förändringar i användarbehörigheter som initieras automatiskt av systemet och de som initieras av en administratör;

d) regler som kräver särskilt godkännande innan tillämpning och sådana som inte gör det.

Regler för styrning av åtkomst bör ha stöd i formella rutiner (se 9.2, 9.3, 9.4) och definierade ansvarsområden (se 6.1.1, 9.2, 15,1).

Rollbaserad åtkomstkontroll är ett angreppsätt som används framgångsrikt av många organisationer för att länka åtkomsträttigheter med roller i verksamheten.

Två återkommande principer för styrning av åtkomst är:

a) Behöver veta (need-to-know): du beviljas bara tillgång till den information som du behöver för att utföra dina uppgifter (olika aktiviteter/roller innebär olika behöver-veta och därmed olika åtkomstprofil);

b) Behöver använda: du beviljas endast tillgång till de informationsbehandlingsresurser (IT-utrustning, program, rutiner, utrymmen) du behöver för att utföra din uppgift, ditt arbete eller din roll.

9.1.2 Tillgång till nätverk och nätverkstjänster

Säkerhetsåtgärd

Användare bör endast ges tillgång till nätverk och nätverkstjänster som de specifikt beviljats tillstånd för.

Vägledning för införande

Regler bör formuleras om användning av nät och tjänster. Dessa regler bör omfatta:

a) de nätverk och nätverkstjänster som får nås;

b) tillståndsrutiner för att bestämma vem som får tillgång till nätverk och nätverksanslutna tjänster;

c) hantering av säkerhetsåtgärder och rutiner för att skydda åtkomst till nätverksanslutningar och nättjänster;

d) de medel som används för åtkomst till nätverk och nätverkstjänster (t.ex. till VPN eller trådlösa nätverk);

e) autentiseringskrav för användare för åtkomst till olika nättjänster;

f) övervakning av användning av nättjänster.

Principer för användning av nättjänster bör vara förenliga med organisationens principer för styrning av åtkomst (se 9.1.1).

Övrig information

Otillåtna och osäkra anslutningar till nättjänster kan påverka hela organisationen. Denna säkerhetsåtgärd är särskilt viktigt för nätverksanslutningar till känsliga eller kritiska verksamhetsprogram eller användare på riskfyllda platser, exempelvis offentliga eller yttre områden som ligger utanför organisationens kontroll och informationssäkerhetsarbete.

9.2 Hantering av användaråtkomst

Mål: Att säkerställa behörig användaråtkomst och att förhindra obehörig åtkomst till system och tjänster.

9.2.1 Registrering och avregistrering av användare

Säkerhetsåtgärd

En formell process för registrering och avregistrering av användare bör införas för att möjliggöra tilldelning av åtkomsträttigheter.

Vägledning för införande

Processen för att hantera användarkonton bör omfatta:

a) unika användarkonton så att användarna kan vara kopplade till och hållas ansvariga för sina handlingar; användning av delade konton tillåtas endast när de är nödvändiga för verksamheten eller av operativa skäl och bör vara godkända och dokumenterade;

b) att omedelbart avaktivera eller ta bort användarkonton för användare som har lämnat organisationen (se 9.2.5);

c) att regelbundet identifiera och ta bort eller inaktivera överflödiga användaridentifikationer;

d) att säkerställa att redundanta användarkonton inte utfärdas.

Övrig information

Att ge eller återkalla åtkomst till information eller resurser för informationsbehandling är vanligtvis en tvåstegsrutin:

a) tilldela och aktivera eller återkalla ett användarkonto (denna åtgärd);

b) ge eller återkalla nyttjanderätt till sådant användarkonto (se 9.2.2).

9.2.2 Tilldelning av användaråtkomst

Säkerhetsåtgärd

En formell process för tilldelning av användaråtkomst bör införas för tilldelning och återkallande av åtkomsträttigheter för alla typer av användare till alla system och tjänster.

Vägledning för införande

Etableringsprocessen för att fördela eller återkalla åtkomsträttigheter till användarkonton bör omfatta att

a) erhålla tillstånd från ägaren av informationssystem eller tjänsten för användning av informationssystem eller tjänst (se säkerhetsåtgärd 8.1.2). Separat godkännande för rättigheter från ledningen kan också vara lämpliga;

b) verifiera att åtkomstnivån som beviljats är lämplig med hänsyn tagen till regler för styrning av åtkomst (se 9.1) och är förenlig med andra krav som uppdelning av roller (se 6.1.5);

c) se till att åtkomsträttigheter inte aktiveras (t.ex. genom tjänsteleverantörer) innan tillstånd är klara;

d) bibehålla ett centralt register över åtkomsträttigheter som beviljas till användarkonton för att få tillgång till information och tjänster;

e) anpassa åtkomsträttigheter för användare som har bytt roller eller jobb och omedelbart ta bort eller blockera åtkomsträttigheter för användare som har lämnat organisationen;

f) med jämna mellanrum granska åtkomsträttigheter med ägare till informationssystem eller tjänster (se 9.2.4).

Övrig information

Organisationen bör överväga att skapa användarroller för åtkomst baserat på verksamhetskrav som sammanfattar ett antal rättigheter i typiska användarprofiler för åtkomst. Förfrågningar om åtkomst och åtkomstgranskningar (se 9.2.4) är lättare att hantera för sådana användarroller än för roller som skapas baserat på särskilda rättigheter.

Organisationen bör överväga införande av bestämmelser i anställnings- och leverantörsavtal som beskriver sanktioner vid försök till obehörig åtkomst som görs av anställda eller av leverantörer (se 7.1.2, 7.2.3, 13.2.4,15.1.2).

9.2.3 Hantering av privilegierade åtkomsträttigheter

Säkerhetsåtgärd

Tilldelning och användning av privilegierade åtkomsträttigheter bör begränsas och styras.

Vägledning för införande

Fördelningen av privilegierade rättigheter bör styras genom ett formellt godkännande i enlighet med de relevanta principerna för styrning av åtkomst (se säkerhetsåtgärd 9.1.1). Följande åtgärder bör övervägas:

a) privilegierade åtkomsträttigheter för varje system eller process, t.ex. operativsystem, databashanteringssystem och varje tillämpning samt att användarna som dessa rättigheter behöver fördelas till bör identifieras;

b) användare bör tilldelas privilegierade åtkomsträttigheter på grundval av deras behov av åtkomst och anpassat till situationen i enlighet med regler för styrning av åtkomst (se 9.1.1), d.v.s. baserat på minimikravet för deras funktionella roller;

c) det bör finnas en godkännandeprocess och ett register över alla tilldelade privilegier. Privilegierade rättigheter bör inte beviljas förrän godkännandeprocessen är klar;

d) krav på giltighetstid för privilegierade åtkomsträttigheter bör definieras;

e) privilegierade åtkomsträttigheter bör tilldelas ett användarkonto som skiljer sig från de konton som används för ordinarie verksamhet. Ordinarie aktiviteter bör inte utföras från privilegierade konton;

f) kompetensen hos användare med privilegierade åtkomsträttigheter bör ses över regelbundet för att verifiera att den är i nivå med deras arbetsuppgifter;

g) särskilda rutiner bör införas och upprätthållas för att undvika obehörig användning av generella administratörskonton i enlighet med systemets konfiguration;

h) för generella administratörskonton bör hemlig autentiseringsinformation behållas konfidentiell när den delas (t.ex. täta byten av lösenord och så snart som möjligt när en privilegierad användare lämnar eller byter jobb, samt kommunicera den mellan privilegierade användare genom lämpliga mekanismer).

Övrig information

Otillbörlig användning av privilegier för systemadministration (någon funktion eller resurs inom ett informationssystem som gör att användaren kan åsidosätta säkerhetsåtgärder för system eller program) är en stor bidragande faktor till fel i eller missbruk av system.

9.2.4 Hantering av användares konfidentiella autentiseringsinformation

Säkerhetsåtgärd

Tilldelningen av konfidentiell autentiseringsinformation bör styras genom en formell hanteringsprocess.

Vägledning för införande

Processen bör innehålla följande krav:

a) användare bör vara skyldiga att underteckna en försäkran om att hålla konfidentiell personlig autentiseringsinformation konfidentiell och att hålla gruppens (vid delade användarkonton) hemliga autentiseringsinformation enbart inom gruppen. Denna skriftliga försäkran kan ingå i anställningsvillkoren (se 7.1.2);

b) när användare är skyldiga att skapa sin egen konfidentiella autentiseringsinformation bör de initialt få sig tilldelad säker tillfällig konfidentiell autentiseringsinformation som de är tvungna att ändra på vid första användningen;

c) rutiner bör fastställas för att säkerställa identiteten på en användare innan konfidentiell autentiseringsinformation tilldelas, oavsett om informationen är ny, förnyad eller tillfällig;

d) tillfällig konfidentiell autentiseringsinformation bör ges till användare på ett säkert sätt och användning av externa parter eller oskyddade (klartext) elektroniska meddelanden bör undvikas;

e) tillfällig konfidentiell autentiseringsinformation bör vara unik för en individ och bör inte gå att gissa;

f) användare bör bekräfta mottagandet av sin konfidentiella autentiseringsinformation;

g) konfidentiell autentiseringsinformation som är grundinstallerad av leverantören bör ändras efter installation av system eller program.

Övrig information

Lösenord är en vanligt förekommande typ av hemlig autentiseringsinformation och är ett vanligt sätt att verifiera en användares identitet. Exempel på andra typer av hemlig autentiseringsinformation är kryptografiska nycklar och andra data som lagras på maskinvarutoken eller smarta kort som producerar autentiseringskoder.

9.2.5 Granskning av användares åtkomsträttigheter

Säkerhetsåtgärd

Ägare av tillgångar bör med jämna mellanrum granska användarnas åtkomsträttigheter.

Vägledning för införande

Vid granskning av rättigheter bör hänsyn tas till följande:

a) användarnas rättigheter bör ses över med jämna mellanrum och efter ändringar, t.ex. befordran, degradering eller uppsägning (se avsnitt 7);

b) en användares behörigheter bör ses över och omfördelas när användaren byter från en roll till en annan inom samma organisation;

c) tillstånd för privilegierade åtkomsträttigheter bör ses över oftare;

d) tilldelning av privilegier bör granskas med jämna mellanrum för att säkerställa att obehöriga privilegier inte har tilldelats;

e) ändringar av konton med priviligierade rättigheter bör loggas och granskas regelbundet.

Övrig information

Denna säkerhetsåtgärd kompenserar för möjliga brister i genomförandet av säkerhetsåtgärderna 9.2.1, 9.2.2 och 9.2.6.

9.2.6 Borttagning eller justering av åtkomsträttigheter

Säkerhetsåtgärd

Åtkomsträttigheterna för alla anställda, och externa användare, till information och informationsbehandlingsresurser bör tas bort vid avslutande av deras anställning, avtal eller uppdrag eller justeras vid förändringar.

Vägledning för införande

Vid avslutande av anställning bör individens åtkomsträttigheter till information och tillgångar som är kopplade till informationsbehandlingsresurser och -tjänster avlägsnas eller avslutas. Detta avgör om det är nödvändigt att ta bort åtkomstbehörigheterna. Förändringar i anställningen bör återspeglas i avlägsnande av alla rättigheter som inte är godkända för den nya rollen. Rättigheter som bör tas bort eller justeras omfattar fysisk och logisk åtkomst. Borttagning eller justering kan göras genom borttagning, återkallande eller utbyte av nycklar, ID-kort, informationsbehandlingsresurser eller prenumerationer. Dokumenterad information som identifierar åtkomsträttigheter för anställda och entreprenörer bör återspegla avlägsnad eller justerad nyttjanderätt. Om en avgående medarbetares eller en extern parts användarkonto är aktivt bör lösenordet ändras vid uppsägning eller vid förändring av anställning, avtal eller överenskommelse.

Åtkomsträttigheter för information och tillgångar som är kopplade till informationsbehandlingsresurser bör reduceras eller tas bort innan anställningen upphör eller ändras, beroende på utvärdering av riskfaktorer såsom:

a) om avslutande eller ändring av anställning är initierad av den anställde, den externa parten eller av ledningen och orsaken till avslutande av anställningen;

b) medarbetarens, den externa partens eller annan användares nuvarande ansvar;

c) värdet av de tillgängliga tillgångarna.

Övrig information

Under vissa omständigheter kan åtkomsträttigheter vara fördelade på fler personer, t.ex. genom delade användarkonton. När en person slutar bör i dessa fall personen i fråga tas bort från gruppåtkomstlistor och åtgärder bör vidtas för att informera övriga anställda och externa parter att de inte längre bör dela denna information med den person som slutar.

I de fall ledningen initierar uppsägningar kan missnöjda anställda eller extern part avsiktligt förvränga information eller sabotera informationsbehandlingsresurser. När personer säger upp sig eller sägs upp kan de vara frestade att samla in information för framtida bruk.

9.3 Användaransvar

Mål: Att göra användare ansvariga för att skydda sin autentiseringsinformation.

9.3.1 Användning av konfidentiell autentiseringsinformation

Säkerhetsåtgärd

Användare bör åläggas att följa organisationens arbetssätt gällande användning av konfidentiell autentiseringsinformation.

Vägledning för införande

Alla användare bör rådas att:

a) hålla konfidentiell autentiseringsinformation konfidentiell och se till att det inte sprids till andra parter, inklusive personer inom organisationen;

b) undvika att notera (t.ex. på papper, fil eller handhållen utrustning) konfidentiell autentiseringsinformation, såvida inte detta kan lagras säkert och metoden för lagring har godkänts (t.ex. verktygsstöd för lösenordshantering);

c) ändra konfidentiell autentiseringsinformation närhelst det finns någon indikation på dess röjande;

d) när lösenord används som konfidentiell autentiseringsinformation, välja lösenord av hög kvalitet med tillräcklig längd som:

   1) är lätta att komma ihåg;

   2) inte är baserade på något en annan person lätt kan gissa eller få fram med personrelaterad information, t.ex. namn, telefonnummer och födelsedatum etc.;

   3) står emot ordlisteattacker (d.v.s. inte bestå av ord i ordböcker);

   4) inte bestå av identiska enbart numeriska eller enbart alfabetiska tecken;

   5) om de är tillfälliga, ändras vid den första inloggningen;

e) inte dela enskild användares konfidentiella autentiseringsinformation;

f) säkerställa korrekt skydd av lösenord när lösenord används och lagras som hemlig autentiseringsinformation i automatiska inloggningsrutiner;

g) inte använda samma konfidentiella autentiseringsinformationen för företag och icke-kommersiella syften.

Övrig information

Tillhandahållande av Single Sign On (SSO) eller andra hanteringsverktyg för hemlig autentiseringsinformation minskar mängden av hemlig autentiseringsinformation som användare behöver skydda och kan därmed öka verkan av denna säkerhetsåtgärd. Dessa verktyg kan också öka konsekvenserna av att hemlig autentiseringsinformation utlämnas eller röjs.

9.4 Styrning av åtkomst till system och tillämpningar

Mål: Att förhindra obehörig åtkomst till system och tillämpningar

9.4.1 Begränsning av åtkomst till information

Säkerhetsåtgärd

Tillgång till information och systemfunktioner bör begränsas i enlighet med regler förstyrning av åtkomst.

Vägledning för införande

Begränsningar i åtkomst bör baseras på specifika verksamhetskrav och på de definierade åtkomstkontrollprinciperna.

Följande bör övervägas för att stödja kraven på begränsning av åtkomst:

a) tillhandahålla menyer för att styra åtkomsten till systemfunktioner i tillämpningssystem;

b) styra vilka data som kan nås av en viss användare;

c) styra åtkomsträttigheter för användare, t.ex. läsa, skriva, radera och exekvera;

d) styra åtkomsträttigheter för andra tillämpningar;

e) begränsa informationen i utdata;

f) ge fysiska eller logiska åtkomstkontroller för isolering av känsliga tillämpningar, tillämpningsdata eller system.

9.4.2 Säkra inloggningsrutiner

Säkerhetsåtgärd

Där regler för styrning av åtkomst så kräver, bör tillgång till system och tillämpningar styras genom säkra inloggningsrutiner.

Vägledning för införande

En lämplig autentiseringsteknik bör väljas för att styrka den påstådda identiteten hos en användare.

Om stark autentisering och identitetsverifiering krävs bör metoder för autentisering som alternativ till lösenord, exempelvis kryptografiska hjälpmedel, smarta kort, token eller biometriska metoder, användas.

Rutiner för att logga in i ett system eller program bör utformas för att minimera möjligheten för obehörig åtkomst. Inloggningsrutiner bör därför avslöja så lite som möjligt om systemet eller tillämpningen för att undvika att ge en obehörig användare hjälp. En bra inloggningsrutin bör:

a) inte visa system- eller programidentitet förrän inloggningsprocessen har slutförts;

b) visa ett allmänt varningsmeddelande att datorn endast får användas av behöriga användare;

c) inte tillhandahålla hjälpmeddelanden under inloggning som skulle kunna hjälpa en obehörig användare;

d) validera inloggningsinformation endast när alla data matats in. Vid fel bör systemet inte ange vilken del av informationen som är rätt eller fel;

e) skydda mot ”Brute Force”-inloggningsförsök;

f) logga misslyckade inloggningsförsök och lyckade inloggningar;

g) registrera en informationssäkerhetshändelse när potentiella obehöriga försök till inloggning eller lyckade obehöriga inloggningar upptäcks;

h) visa följande information vid slutförandet av en lyckad inloggning:

   1) datum och tid för föregående lyckade inloggning;

   2) detaljer för misslyckade inloggningsförsök sedan föregående lyckade inloggning;

i) inte visa lösenord i klartext;

j) inte överföra lösenord i klartext över ett nätverk;

k) avsluta inaktiva sessioner efter en definierad tidsperiod av inaktivitet, särskilt på högriskmiljöer som offentliga platser eller områden utanför organisationens säkerhetshantering eller i mobila enheter;

l) begränsa uppkopplingstid till högrisktillämpningar och därigenom uppnå ökad säkerhet och minska möjligheterna till obehörig åtkomst.

Övrig information

Lösenord är ett vanligt sätt för identifiering och autentisering baserat på en hemlighet som bara användaren vet. Samma effekt kan uppnås med kryptografiska hjälpmedel och autentiseringsprotokoll. Styrkan på användarautentiseringen bör motsvara klassningsnivån som informationen har.

Om lösenord skickas i klartext vid inloggningssessionen över ett nätverk kan de fångas upp av ett spionprogram.

9.4.3 System för lösenordshantering

Säkerhetsåtgärd

System för lösenordshantering bör vara interaktiva och bör säkerställa kvalitativa lösenord.

Vägledning för införande

Ett system för lösenordshantering bör:

a) framtvinga användning av individuella användarkonton och lösenord så att individuellt ansvar kan utkrävas;

b) låta användare välja och ändra sina egna lösenord och innehålla en rutin som ger meddelande om inmatningsfel;

c) säkerställa att lösenord av hög kvalitet väljs;

d) tvinga användarna att ändra sina lösenord vid den första inloggningen;

e) kräva ändring av lösenord regelbundet samt vid behov;

f) upprätthålla ett register över tidigare använda lösenord och förhindra användning av tidigare lösenord;

g) inte visa lösenord på skärmen vid inmatning;

h) lagra lösenordsfiler åtskilt från data för tillämpningssystem;

i) lagra och överföra lösenorden på ett säkert sätt.

Övrig information

Vissa tillämpningar kräver att lösenord tilldelas av en oberoende funktion. I sådana fall gäller inte punkt b), d) och e) av den ovanstående vägledningen. I de flesta fall väljs och underhålls lösenord av användare.

9.4.4 Användning av privilegierade verktygsprogram

Säkerhetsåtgärd

Användning av verktygsprogram som kan ha förmåga att kringgå säkerhetsåtgärder i system och tillämpningar bör begränsas och styras strikt.

Vägledning för införande

Följande riktlinjer för användning av verktygsprogram som kan ha förmåga att kringgå säkerhetsåtgärder för system och program bör övervägas:

a) användning av rutiner för identifiering, autentisering och auktorisering för verktygsprogram;

b) segregering av verktygsprogram från tillämpningar;

c) begränsa användningen av verktygsprogram till minsta möjliga antal betrodda och godkända användare (se 9.2.2);

d) tillstånd för ad hoc-användning av verktygsprogram;

e) begränsning av tillgången till program, t.ex. av tiden för auktoriserad ändring;

f) loggning av all användning av verktygsprogram;

g) definiera och dokumentera åtkomstnivåer för verktygsprogram;

h) borttagning eller avaktivering av alla onödiga program;

i) inte göra verktygsprogram tillgängliga för användare som har åtkomst till tillämpningar i system där separering av ansvar krävs.

Övrig information

De flesta datorinstallationer har ett eller flera program som kan ha förmåga att åsidosätta säkerhetsåtgärder för system och tillämpningar.

9.4.5 Åtkomstkontroll till källkod för program

Säkerhetsåtgärd

Tillgång till källkod för program bör begränsas.

Vägledning för införande

Tillgång till källkod och relaterade objekt (t.ex. designspecifikationer, kravspecifikationer, planer för verifiering och validering) bör styras noggrant för att förhindra införandet av obehörig funktionalitet och undvika oavsiktliga ändringar. De bör även granskas för att upprätthålla konfidentialitet gällande värdefulla immateriella rättigheter. För källkod till program kan detta uppnås genom styrd central lagring av sådan kod, helst i särskilda källkodsbibliotek. Följande riktlinjer bör övervägas för att styra tillgången till sådana källkodsbibliotek i syfte att minska risken för korrupt kod:

a) om möjligt bör källkodsbibliotek inte förekomma i produktionssystem;

b) källkod och källkodsbibiliotek bör förvaltas enligt fastställda rutiner;

c) supportpersonalens tillgång till källkodsbibliotek bör begränsas;

d) uppdatering av bibliotek för källkod och relaterade objekt samt utlämning av källkod till programmerare bör endast göras efter korrekt godkännande;

e) förteckningar över program bör förvaras i en säker miljö;

f) en granskningslogg för all åtkomst till källkodsbibliotek bör upprätthållas;

g) underhåll och kopiering av källkodsbibliotek bör styras genom formell ändringshantering (se 14.2.2).

Om källkoden för program är avsedd att offentliggöras bör ytterligare säkerhetsåtgärder övervägas för att säkerställa dess riktighet (t.ex. digital signatur).

10 Kryptering

10.1 Kryptografiska säkerhetsåtgärder

Mål: Att säkerställa korrekt och verkningsfull användning av kryptering för att skydda informationens konfidentialitet, äkthet och riktighet.

10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder

Säkerhetsåtgärd

Regler för användning av kryptografiska säkerhetsåtgärder för skydd av information bör utvecklas och införas.

Vägledning för införande

Vid utveckling av regler för kryptografi bör följande övervägas:

a) en ledningsstrategi för användning av kryptografiska säkerhetsåtgärder bör finnas för hela organisationen inklusive allmänna principer enligt vilka verksamhetsinformation skyddas;

b) den skyddsnivå som krävs bör fastställas baserat på riskbedömning och med hänsyn tagen till typ, styrka och kvalitet på den krypteringsalgoritm som krävs;

c) användning av kryptering för skydd av information som överförs på mobila eller flyttbara medieenheter eller över kommunikationslinjer;

d) en strategi för nyckelhantering, inklusive metoder för att hantera skyddet av kryptografiska nycklar och återvinning av krypterad information om nycklar förloras, äventyras eller skadas;

e) roller och ansvarsområden, t.ex. vem som ansvarar för:

   1) införande av reglerna;

   2) central förvaltning inklusive nyckelgenerering (se 10.1.2);

f) vilka standarder som bör införas för verkningsfullt genomförande i hela organisationen (vilken lösning som används för vilka verksamhetsprocesser);

g) effekten av att använda krypterad information på säkerhetsåtgärder som är beroende av att innehållet inspekteras (t.ex. upptäckt av skadlig kod).

Vid införande av principer för kryptering bör hänsyn tas till regelverk, nationella restriktioner som kan tillämpas på användningen av krypteringsteknik i olika delar av världen och frågor avseende gränsöverskridande flöde av krypterad information (se 18.1.5).

Säkerhetsåtgärder baserade på kryptering kan användas för att uppnå olika informationssäkerhetsmål, t.ex.:

a) konfidentialitet: användning av kryptering av information för att skydda känslig eller kritisk information, som antingen lagras eller överförs;

b) riktighet/äkthet: användning av digitala signaturer eller ”autentiseringskoder för meddelanden” för att verifiera äktheten eller riktigheten hos lagrad eller vidarebefordrad känslig eller kritisk information;

c) oavvislighet: användning av kryptografiska tekniker för att ge belägg för förekomst eller avsaknad av en händelse eller handling;

d) autentisering: användning av kryptografiska tekniker för att autentisera användare och andra systemenheter som begär åtkomst till eller verksamhetsförbindelser med systemets användare, enheter och resurser.

Övrig information

Ett beslut om huruvida en krypteringslösning är lämplig bör ses som en del av den bredare processen för riskbedömning och val av säkerhetsåtgärder. Denna bedömning kan sedan användas för att avgöra huruvida en säkerhetsåtgärd baserad på kryptering är lämplig, vilken typ av säkerhetsåtgärd som bör tillämpas och för vilket syfte och för vilka verksamhetsprocesser.

Regler för användning av säkerhetsåtgärder baserade på kryptering är nödvändiga för att maximera nytta och minimera riskerna med att använda krypteringsteknik och att undvika olämplig eller felaktig användning.

För att uppfylla målen i informationssäkerhetspolicyn och tillhörande regelverk bör specialistråd inhämtas inför val av lämpliga säkerhetsåtgärder som baserar sig på kryptering.

10.1.2 Nyckelhantering

Säkerhetsåtgärd

Regler för användning, skydd och gilltighetstid för kryptografiska nycklar för deras hela livscykel bör utvecklas och införas.

Vägledning för införande

Reglerna bör omfatta krav för hantering av krypteringsnycklar för deras hela livscykel inklusive generering, lagring, arkivering, hämtning, distribution, återkallande och destruering av nycklar.

Kryptografiska algoritmer, nyckellängder och praktisk användning bör väljas enligt praxis. Lämplig nyckelhantering kräver säkra processer för att generera, lagra, arkivera, hämta, distribuera, återkalla och förstöra kryptografiska nycklar.

Alla krypteringsnycklar bör skyddas mot förändring och förlust. Hemliga och privata nycklar måste dessutom skyddas mot obehörig användning och utlämnande. Utrustning som används för att skapa, lagra och arkivera nycklar bör skyddas fysiskt.

Ett system för nyckelhantering bör baseras på en överenskommen uppsättning standarder, rutiner och säkra metoder för att:

a) generera nycklar för olika kryptografiska system och olika tillämpningar;

b) utfärda och erhålla certifikat för offentlig nyckel;

c) distribuera nycklarna till avsedda enheter, inklusive hur nycklar bör aktiveras vid mottagande;

d) lagra nycklar, inklusive hur behöriga användare får tillgång till nycklar;

e) ändra eller uppdatera nyckel inklusive regler om när nycklar bör ändras och hur detta kommer att ske;

f) hantera kompromitterade nycklar;

g) återkalla nycklar inklusive hur nycklarna bör återkallas eller avaktiveras, t ex. när nycklar har kompromitterats eller när en användare lämnar en organisation (i vilket fall nycklar också bör arkiveras);

h) återställa nycklar som förlorats eller skadats;

i) säkerhetskopiera eller arkivera nycklar;

j) förstöra nycklar;

k) loggning och revision av till nyckelhanteringen relaterade aktiviteter.

För att minska risken för felaktig användning bör datum för aktivering och avaktivering definieras så att nyckeln endast kan användas under angiven tidsperiod i de aktuella reglerna för nyckelhantering.

Förutom att säkert hantera hemliga och privata nycklar bör även äktheten hos offentliga nycklar bedömas. Detta kan göras genom att använda certifikat för offentliga nycklar som normalt utfärdas av en certifikatutfärdare, som bör vara en betrodd organisation med lämpliga säkerhetsåtgärder och rutiner som ger den nödvändiga graden av förtroende.

Innehåll i överenskommelser om tjänsteleverans eller avtal med externa leverantörer av kryptografiska tjänster, t.ex. med en certifikatutfärdare, bör omfatta frågor om ansvar, tillförlitlighet och svarstider för tillhandahållande av tjänster (se 15.2).

Övrig information

Hantering av krypteringsnycklar är avgörande för en verkningsfull användning av krypteringsteknik. ISO/IEC 11770[2] [3] [4] ger ytterligare information om nyckelhantering.

Krypteringsteknik kan också användas för att skydda kryptografiska nycklar. Rutiner kan behöva övervägas för hantering av förelägganden från myndigheter om åtkomst till kryptografiska nycklar, t.ex. om krypterad information behöver göras tillgänglig i okrypterad form som bevis vid rättegång.

11 Fysisk och miljörelaterad säkerhet

11.1 Säkra områden

Mål: Att förhindra otillåten fysisk åtkomst till, skador på och störningar i tillgången till organisationens information och informationsbehandlingsresurser.

11.1.1 Fysiska säkerhetsavgränsningar

Säkerhetsåtgärd

Fysiska avgränsningar bör definieras och användas för att skydda områden som innehåller antingen känslig eller kritisk information och informationsbehandlingsresurser.

Vägledning för införande

Följande riktlinjer bör beaktas och införas där så är lämpligt för fysisk säkerhet:

a) skalskydd bör definieras och placering och styrka av varje avgränsning bör bestämmas beroende på säkerhetskraven för tillgångarna inom avgränsningen och resultaten av en riskbedömning;

b) inneslutningen av en byggnad eller en plats som innehåller informationsbehandlingsresurser bör vara fysiskt stark (dvs. det bör inte finnas några brister i avgränsningen eller några områden där ett inbrott lätt kan genomföras). Yttre tak, väggar och golv bör vara av solid konstruktion och alla yttre dörrar bör skyddas på lämpligt sätt mot obehörig passage med säkerhetsmekanismer (t.ex. bommar, larm, lås). Dörrar och fönster bör vara låsta när de är obevakade och yttre skydd bör övervägas för fönster, särskilt på marknivå;

c) en bemannad reception eller andra metoder för att styra fysiskt tillträde till webbplatsen eller byggnaden bör vara på plats. Tillträde till platser och byggnader bör begränsas till behörig personal;

d) fysiska hinder bör i tillämpliga fall byggas för att förhindra otillåten fysiskt åtkomst och negativ påverkan på miljön;

e) alla branddörrar, tillsammans med väggarna i skalskyddet, bör vara larmade, övervakas och testas för att uppnå den skyddsnivå som krävs i enlighet med lämpliga regionala, nationella och internationella standarder. De bör fungera på ett säkert sätt och enligt lokala brandföreskrifter;

f) lämpliga detektionssystem bör installeras enligt nationella, regionala eller internationella standarder. Detektionssystem bör testas regelbundet för att omfatta alla ytterdörrar och tillgängliga fönster. Obemannade utrymmen bör vara larmade hela tiden och även omfatta andra utrymmen, t.ex. datahall eller kommunikationsutrymmen;

g) informationsbehandlingsresurser som förvaltas av organisationen bör fysiskt åtskiljas från de som förvaltas av externa parter.

Övrig information

Fysiskt skydd kan uppnås genom att skapa en eller flera fysiska säkerhetszoner inom och runt organisationens lokaler och informationsbehandlingsresurser. Användning av flera säkerhetszoner ger ytterligare skydd, innebärande att fel på ett enda skydd inte gör att säkerheten omedelbart äventyras.

En säkerhetszon kan vara ett låsbart kontor eller flera utrymmen omgivna av en kontinuerlig intern fysisk säkerhetsbarriär. Ytterligare hinder och skalskydd för att styra fysiskt tillträde kan behövas mellan områden med olika säkerhetskrav inom det yttre skalskyddet. Särskild uppmärksamhet avseende fysiskt tillträde bör ägnas åt byggnader som innehar tillgångar för flera organisationer.

Tillämpningen av fysiska säkerhetsåtgärder, särskilt för säkra områden, bör anpassas till de tekniska och ekonomiska förutsättningar för organisationen som anges i riskbedömningen.

11.1.2 Fysiska tillträdesbegränsningar

Säkerhetsåtgärd

Säkra områden bör skyddas genom lämpliga säkerhetsåtgärder för att säkerställa att endast behörig personal får tillträde.

Vägledning för införande

Följande riktlinjer bör övervägas:

a) datum och tid för besökares ankomst och utgång bör registreras och alla besökare bör övervakas om inte deras tillträde har godkänts tidigare. De bör endast beviljas tillträde för specifika, godkända syften och besökarna bör delges instruktioner avseende områdets säkerhetskrav och rutiner vid nödsituationer. Besökarnas identitet bör säkerställas på lämpligt sätt;

b) tillträde till områden där konfidentiell information bearbetas eller lagras bör begränsas endast till behöriga personer genom att införa lämpliga åtkomstkontroller, t.ex. genom att införa tvåfaktorsautentisering med mekanismer som passerkort eller hemliga PIN-koder;

c) en fysisk loggbok eller en elektronisk verifieringskedja över alla tillträden bör underhållas och bevaras säkert;

d) alla anställda, leverantörer och externa parter bör åläggas att bära någon form av synlig identifiering och de bör omedelbart underrätta säkerhetspersonalen om de möter besökare utan ledsagare eller någon som inte bär synlig identifiering;

e) extern servicepersonal bör beviljas begränsat tillträde till säkra områden eller områden där konfidentiell information bearbetas endast när det behövs. Detta tillträde bör godkännas och övervakas;

f) tillträdesrätt till säkra områden bör regelbundet granskas och uppdateras, och återkallas vid behov (se 9.2.4 och 9.2.5).

11.1.3 Säkerställande av kontor, rum och anläggningar

Säkerhetsåtgärd

Fysisk säkerhet för kontor, utrymmen och anläggningar bör utformas och tillämpas.

Vägledning för införande

Följande riktlinjer bör övervägas för att säkra kontor, utrymmen och anläggningar:

a) viktiga anläggningar bör placeras så att allmänheten inte får tillträde till dem;

b) i förekommande fall bör byggnader vara diskreta och utan minsta antydan om deras syfte och utan uppenbara tecken, utanför eller inne i byggnaden, som kan indikera att informationsbehandling sker där;

c) utrymmen bör utformas för att förhindra att konfidentiell information eller verksamhet är synlig eller avlyssningsbar från utsidan. Elektromagnetisk avskärmning bör övervägas;

d) kataloger och interna telefonlistor som identifierar utrymmen där konfidentiell informationsbehandling bedrivs bör inte vara lätt åtkomliga för obehöriga.

11.1.4 Skydd mot yttre och miljörelaterade hot

Säkerhetsåtgärd

Fysiskt skydd mot naturkatastrofer, illvilliga angrepp eller olyckor bör utformas och tillämpas.

Vägledning för införande

Specialistråd bör inhämtas om hur skador från brand, översvämning, jordbävning, explosion, oroligheter och andra former av naturkatastrofer eller olyckor kan undvikas.

11.1.5 Arbeta i säkra utrymmen

Säkerhetsåtgärd

Rutiner för att arbeta i säkra utrymmen bör utformas och tillämpas.

Vägledning för införande

Följande riktlinjer bör övervägas:

a) personal bör endast känna till förekomsten av eller aktiviteter inom ett skyddat utrymme baserat på vad de behöver känna till;

b) oövervakat arbete i säkra områden bör undvikas både av säkerhetsskäl och för att förhindra skadliga aktiviteter;

c) säkra utrymmen som inte används bör vara låsta och granskas regelbundet;

d) fotografisk, video, ljud eller annan inspelningsutrustning såsom kameror i mobila enheter bör inte tillåtas, såvida inte detta är godkänt.

För arbete i säkra utrymmet bör säkerhetsåtgärderna omfatta anställda och extern part som arbetar i det säkra utrymmet och omfatta alla aktiviteter som äger rum där.

11.1.6 Leverans- och lastningsområden

Säkerhetsåtgärd

Åtkomstpunkter såsom leverans- och lastningsområden och andra punkter där obehöriga personer kan komma in i lokalerna bör styras och om möjligt isoleras från informationsbehandlingsresurser för att undvika obehörig åtkomst.

Vägledning för införande

Följande riktlinjer bör övervägas:

a) tillträde till ett leverans- och lastningsområde utifrån bör begränsas till identifierad och godkänd personal;

b) leverans- och lastningsområde bör utformas så att leveranser kan lastas och lossas utan att leveranspersonal kan få tillgång till andra delar av byggnaden;

c) yttre dörrar till ett leverans- och lastningsområde bör säkras när de inre dörrarna öppnas

d) inkommande material bör inspekteras och undersökas för förekomst av explosiva ämnen, kemikalier eller annat farligt material, innan det flyttas från leverans- och lastningsområdet;

e) inkommande material bör registreras vid leverans enligt rutiner för hantering av tillgångar (se avsnitt 8);

f) inkommande och utgående leveranser bör hållas fysiskt åtskilda där så är möjligt;

g) inkommande material bör granskas avseende synlig åverkan under transport. Om sådan åverkan upptäcks bör det omedelbart rapporteras till säkerhetspersonalen.

11.2 Utrustning

Mål: Att förhindra förlust, skada, stöld eller påverkan på tillgångar, och avbrott i organisationens verksamhet.

11.2.1 Placering av utrustning och skydd

Säkerhetsåtgärd

Utrustning bör placeras och skyddas för att minska riskerna för miljörelaterade hot och faror och möjligheter för obehörig åtkomst.

Vägledning för införande

Följande riktlinjer bör övervägas för att skydda utrustning:

a) utrustning bör placeras så att onödigt tillträde till arbetsutrymmen minimeras;

b) anläggningar för informationsbehandling som hanterar känsliga uppgifter bör placeras noggrant för att minska risken för att informationen visas för obehöriga vid användning;

c) lagerutrymmen bör säkras för att undvika obehörigt tillträde;

d) objekt med särskilda skyddsbehov bör ges anpassat skydd för att minska den allmänna skyddsnivån som krävs;

e) säkerhetsåtgärder bör vidtas för att minimera risken för potentiella fysiska och miljömässiga hot, t.ex. stöld, brand, explosiva ämnen, rök, vatten (eller avbrott i vattenförsörjning), damm, vibrationer, kemiska skador, elförsörjningsproblem, kommunikationsstörning, elektromagnetisk strålning och vandalism;

f) riktlinjer gällande intag av mat och dryck samt gällande rökning i närheten av informationsbehandlingsresurser bör fastställas;

g) miljöförhållanden som temperatur och fuktighet bör övervakas för att upptäcka förhållanden som kan leda till negativ påverkan på driften av informationsbehandlingsresurser;

h) åskskydd bör finnas på alla byggnader och åskskyddsfilter bör monteras på alla inkommande strömförsörjnings- och kommunikationsvägar;

i) användning av särskilda skydd, såsom tangentbordsmembran, bör övervägas för utrustning i industriella miljöer;

j) utrustning för bearbetning av konfidentiell information bör skyddas för att minimera risken för informationsläckage på grund av röjande strålning.

11.2.2 Tekniska försörjningssystem

Säkerhetsåtgärd

Utrustning bör skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.

Vägledning för införande

Tekniska försörjningssystem (t.ex. el, telekommunikation, vatten, gas, avlopp, ventilation och luftkonditionering) bör:

a) överensstämma med tillverkarens specifikationer för utrustningen och rättsliga krav;

b) bedömas regelbundet avseende deras förmåga att uppfylla organisationens kapacitetsbehov och beroenden av andra försörjningssystem;

c) inspekteras och provas regelbundet för att säkerställa deras funktion;

d) om det behövs, ha larm för att upptäcka störningar;

e) om det behövs, ha alternativa flöden med olika fysiska vägar.

Nödbelysning och nödkommunikation bör tillhandahållas. Konsoler och ventiler för att stänga av el, vatten, gas eller andra försörjningssystem bör vara placerade nära nödutgångar eller utrustningsrum.

Övrig information

Utökad redundans för uppkoppling mot nätverk kan erhållas genom alternativa vägval från mer än en tjänsteleverantör.

11.2.3 Kablagesäkerhet

Säkerhetsåtgärd

Kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada.

Vägledning för införande

Följande riktlinjer för kablagesäkerhet bör övervägas:

a) kablage för ström och telekommunikationer till informationsbehandlingsresurser bör om möjligt vara lagda i marken eller ges annat lämpligt skydd;

b) kablage för strömförsörjning bör hållas åtskilda från kommunikationskablage för att förhindra störningar;

c) för känsliga eller kritiska system bör följande ytterligare säkerhetsåtgärder övervägas:

   1) installationen av fysiskt skyddat kablage och låsta utrymmen och skåp för inspektioner och slutpunkter;

   2) användning av elektromagnetisk avskärmning för kabelskydd;

   3) användning av tekniska granskningar och fysiska säkerhetsåtgärder för att identifiera obehöriga anslutningar till kablage;

   4) styrd tillgång till kontrollpaneler för konfigurering av nätverk och till utrymmen för kablage.

11.2.4 Underhåll av utrustning

Säkerhetsåtgärd

Utrustning bör underhållas korrekt för att säkerställa fortsatt tillgänglighet och riktighet.

Vägledning för införande

Följande riktlinjer för underhåll av utrustning bör övervägas:

a) utrustning bör underhållas i enlighet med leverantörens rekommenderade serviceintervall och specifikationer;

b) endast auktoriserad servicepersonal bör genomföra reparationer och service på utrustning;

c) alla misstänkta eller faktiska fel och allt förebyggande och avhjälpande underhåll bör registreras;

d) lämpliga säkerhetsåtgärder bör införas när utrustning är schemalagt för underhåll, med hänsyn till huruvida detta underhåll utförs av personal på plats eller utanför organisationen. Om nödvändigt, bör konfidentiell information avlägsnas från utrustningen, alternativt bör underhållspersonalen vara granskad och godkänd;

e) alla underhållskrav som följer av försäkringar bör följas;

f) innan utrustning är tillbaka i drift efter underhåll bör den inspekteras för att säkerställa att utrustningen inte har manipulerats och att den fungerar.

11.2.5 Utförsel av tillgångar

Säkerhetsåtgärd

Utrustning, information eller program bör inte avlägsnas utanför organisationens lokaler utan tillstånd.

Vägledning för införande

Följande riktlinjer bör övervägas:

a) vilka anställda och externa parter som har befogenhet att tillåta avlägsnande av tillgångar bör fastställas;

b) tidsfrister för avlägsnande av tillgångar bör fastställas och återlämningstidpunkten verifieras;

c) där nödvändigt och lämpligt så är bör tillgångar som avlägsnas registreras och registreras vid återlämning;

d) identitet, roll och tillhörighet för alla som hanterar eller använder tillgångar bör dokumenteras och sådan dokumenterad information bör återlämnas tillsammans med utrustningen, information eller program.

Övrig information

Stickprovskontroller, genomförda för att upptäcka obehörigt avlägsnande av tillgångar, kan också utföras för att upptäcka obehöriga inspelningsenheter, vapen, etc., och för att förhindra deras införande till och borttagande från platsen. Sådana granskningar bör utföras i enlighet med gällande författningar. Alla individer bör göras medvetna om att stickprovskontroller utförs och granskningarna bör endast utföras med tillstånd baserade på tillämpliga rättsliga krav.

11.2.6 Säkerhet för utrustning och tillgångar utanför organisationens lokaler

Säkerhetsåtgärd

Säkerhet bör tillämpas på tillgångar utanför organisationens lokaler med hänsyn till de särskilda risker som finns förknippade med att arbeta utanför organisationens lokaler.

Vägledning för införande

Användning av eventuell lagrings- och informationsbehandlingsutrustning utanför organisationens lokaler bör godkännas av ledningen. Detta gäller för utrustning som ägs av organisationen och för privat utrustning som används av organisationen.

Följande riktlinjer bör övervägas för skydd av portabel utrustning:

a) utrustning och media som används utanför organisationens lokaler bör inte lämnas obevakad på offentliga platser;

b) tillverkarens instruktioner för att skydda utrustningen bör alltid iakttas, exempelvis skydd mot exponering för starka elektromagnetiska fält;

c) säkerhetsåtgärder för externa arbetsplatser, som arbetsplats i hemmet, distansarbete och tillfälliga platser, bör beslutas baserat på en riskbedömning och tillämpas. Säkerhetsåtgärderna kan t.ex. bestå av låsbart arkivskåp, städat skrivbord, åtkomststyrning av datorer och säker kommunikation med kontoret (se även ISO/IEC 27033[15] [16] [17] [18] [19]);

d) när utrustning överförs mellan olika individer eller externa parter utanför fasta driftställen bör ett register upprätthållas för spårbarhet av utrustningen. Dokumenterad information bör innehålla namn på de individer och organisationer som är ansvariga för utrustningen.

Risker, t.ex. för skador, stöld eller avlyssning, kan variera avsevärt mellan platser och bör beaktas vid fastställandet av de mest lämpliga säkerhetsåtgärderna.

Övrig information

Informationsbehandlingsresurser och resurser för lagring av information omfattar alla former av persondatorer, planeringskalendrar, mobiltelefoner, smarta kort, papper eller annan form, som används i samband med distansarbete eller som avlägsnats från den ordinarie arbetsplatsen.

Mer information om andra aspekter av skydda mobil utrustning finns i 6.2.

Det kan vara lämpligt att undvika risken genom att avråda viss personal från distansarbete eller genom att begränsa deras användning av portabel utrustning.

11.2.7 Säker kassering eller återanvändning av utrustning

Säkerhetsåtgärd

All utrustning som innehåller lagringsmedia bör granskas för att säkerställa att all känslig data och licensierade program har avlägsnats eller säkert överskrivits före kassering eller återanvändning.

Vägledning för införande

Före kassering eller återanvändning bör utrustning kontrolleras för att säkerställa om den innehåller lagringsmedia eller inte.

Istället för att använda standardfunktionen radera eller formatera bör lagringsmedia som innehåller konfidentiell eller upphovsrättsskyddad information förstöras fysiskt eller informationen bör förstöras, tas bort eller överskrivas med särskilda program för att göra den ursprungliga informationen omöjlig att återskapa.

Övrig information

Skadade enheter som innehåller känsliga data kan kräva en riskbedömning för att avgöra om enheterna bör förstöras fysiskt snarare än skickas för reparation eller kassation (se 11.2.7). Information kan äventyras genom oförsiktigt kassering eller återanvändning av utrustning.

Förutom säker diskförstöring, kan kryptering av hela disken minska risken för avslöjande av konfidentiell information när utrustning avyttras eller omplaceras, under förutsättning att:

a) krypteringsprocessen är tillräckligt stark och täcker hela disken (inklusive tomma ytor, swap-filer, etc.);

b) krypteringsnycklarna är tillräckligt långa för att motstå ”brute force-attacker”;

c) krypteringsnycklarna hålls konfidentiella (t.ex. aldrig lagras på samma disk).

För ytterligare råd om kryptering, se avsnitt 10.

Tekniker för säker överskrivning av lagringsmedia varierar beroende på typen av medialagring. Verktyg för överskrift bör ses över för att säkerställa att de är tillämpliga på den använda typen av lagringsmedia.

11.2.8 Obevakad utrustning som hanteras av användare

Säkerhetsåtgärd

Användare bör säkerställa att obevakad utrustning har lämpligt skydd.

Vägledning för införande

Alla användare bör göras medvetna om de säkerhetskrav och rutiner som gäller för att skydda obevakad utrustning, liksom deras ansvar för användning av sådant skydd. Alla användare bör rådas att:

a) avsluta aktiva sessioner när de är klara om de inte kan säkras genom en lämplig låsmekanism, t.ex. en lösenordskyddad skärmsläckare;

b) logga ut från program eller nätverkstjänster när de inte längre behövs;

c) skydda datorer eller mobila enheter från obehörig åtkomst genom användning av lås eller motsvarande säkerhetsåtgärd, t.ex. lösenordsskydd, när de inte används.

11.2.9 Regel om rent skrivbord och tom skärm

Säkerhetsåtgärd

En regel bör antas för rent skrivbord avseende papper och flyttbara lagringsmedia, och för tom skärm på informationsbehandlingsresurser.

Vägledning för införande

Regeln för rent skrivbord och tom skärm bör beakta informationsklassningar (se 8.2), rättsliga och avtalsmässiga krav (se 18.1) och motsvarande risker och kulturella aspekter av organisationen. Följande riktlinjer bör övervägas:

a) känslig eller kritisk verksamhetsinformation, t.ex. på papper eller på elektroniska lagringsmedia, bör vara inlåst (helst i kassaskåp eller dokumentskåp eller andra former av säkerhetsskåp) när den inte används, särskilt när lokalerna är obemannade;

b) datorer och terminaler bör lämnas utloggade eller skyddade med skärm- och tangentbordslåsmekanism som skyddas av ett lösenord, dongel eller liknande användarautentiseringsmetod när de är obevakad och bör skyddas genom centralt lås, lösenord eller andra säkerhetsåtgärder när de inte används;

c) otillåten användning av kopiatorer och annan reproduktionsteknik (skannrar, digitala kameror) bör förhindras;

d) media som innehåller känslig eller konfidentiell information bör tas bort från skrivare omedelbart.

Övrig information

En tydlig regel för rent skrivbord och tom skärm minskar risken för obehörig åtkomst, förlust av och skadad information under och utanför arbetstid. Kassaskåp eller andra former av säkra förvaringsutrymmen kan också skydda information mot katastrofer som brand, jordbävning, översvämning eller explosion.

Överväg att använda skrivare med pinkod-funktion, så att endast den som begärt utskriften kan få ut den och detta kan endast göras vid skrivaren.

12 Driftsäkerhet

12.1 Driftsrutiner och ansvar

Mål: Att säkerställa korrekt och säker drift av informationsbehandlingsresurser.

12.1.1 Dokumenterade driftsrutiner

Säkerhetsåtgärd

Driftrutiner bör dokumenteras och göras tillgängliga för alla användare som behöver dem.

Vägledning för införande

Dokumenterade rutiner bör finnas för drift av informationsbehandlings- och kommunikationsresurser, såsom uppstarts- och nedtagningsrutin, säkerhetskopiering, underhåll av utrustning, hantering av media, datahall samt hantering av e-post och säkerhet.

Driftsrutiner bör innefatta specifika instruktioner för:

a) installation och konfiguration av system;

b) automatisk och manuell bearbetning och hantering av information;

c) säkerhetskopiering (se 12.3);

d) fastställd schemaläggning, inklusive beroenden till andra system, tidigaste start för körningar och senaste tidpunkt för slutförande av körningar;

e) instruktioner för hantering av fel eller andra exceptionella omständigheter som kan uppstå under drift, inklusive begränsningar för användningen av systemverktyg (se 9.4.4);

f) support- och eskaleringskontakter inklusive kontakter för externt stöd vid oväntade funktionella eller tekniska problem;

g) särskilda instruktioner för hantering av utdata och media, användning av särskilda medel eller hantering av konfidentiell utdata inklusive rutiner för säker kassering av utdata från misslyckade körningar (se 8.3 och 11.2.7);

h) rutiner för återstart och återställande av systemet i händelse av systemfel;

i) hantering av information i transaktionsloggning och systemlogg (se 12.4);

j) rutiner för övervakning (se 12.4).

Driftsrutiner och de dokumenterade rutinerna för systemaktiviteter bör behandlas som formella dokument och ändringar bör godkännas av ledningen. Där så är tekniskt möjligt, bör informationssystem hanteras konsekvent med samma rutiner, verktyg och hjälpmedel.

12.1.2 Ändringshantering

Säkerhetsåtgärd

Förändringar i organisation, verksamhetsprocesser eller informationsbehandlingsresurser och system som påverkar informationssäkerheten bör styras.

Vägledning för införande

Följande bör övervägas:

a) identifiering och registrering av betydande förändringar;

b) planering och tester av förändringar;

c) bedömning av den potentiella påverkan, inbegripande påverkan på informationssäkerhet, avseende sådana förändringar;

d) formella rutiner för godkännande av föreslagna förändringar;

e) verifiering av att informationssäkerhetskrav är uppfyllda;

f) kommunicera detaljer avseende ändring till alla relevanta personer;

g) fall-back rutiner, inklusive rutiner och ansvar för att avbryta och återställa vid misslyckade ändringar och oförutsedda händelser;

h) tillhandahållande av en ändringsprocess för nödsituationer för att möjliggöra ett snabbt och kontrollerat införande av förändringar som behövs för att hantera en incident (se 16.1).

Formellt ledningsansvar och rutiner bör vara på plats för att säkerställa tillfredsställande styrning av alla ändringar. När ändringar görs bör en granskningslogg som innehåller all relevant information föras.

Övrig information

Otillräcklig styrning av förändringar av informationsbehandlingsresurser och system är en vanlig orsak till systemfel eller säkerhetsbrister. Ändringar i driftsmiljön, särskilt när ett system överförs från utveckling till drift, kan påverka tillförlitligheten för aktuella program (se 14.2.2).

12.1.3 Kapacitetshantering

Säkerhetsåtgärd

Användningen av resurser bör övervakas samt justeras och prognoser av framtida kapacitetskrav bör göras för att säkerställa nödvändig systemprestanda.

Vägledning för införande

Kapacitetskrav bör identifieras med hänsyn tagen till verksamhetsbetydelse för berörda system. Optimering och övervakning av system bör säkerställa och förbättra, där så är nödvändigt, tillgången till, och effektiviteten i systemen. Upptäckande åtgärder bör införas för att indikera problem i god tid. Prognoser för framtida kapacitetskrav bör ta hänsyn till ny verksamhet och systemkrav samt nuvarande och förutspådda trender i organisationens kapacitet för informationsbehandling.

Särskild uppmärksamhet bör ägnas åt resurser med långa ledtider för upphandling eller höga kostnader. Ledningen bör därför övervaka användningen av viktiga systemresurser. De bör identifiera trender i användning, särskilt när det gäller verksamhetsprogram eller systemverktyg.

Ledningen bör använda denna information för att identifiera och undvika potentiella flaskhalsar och beroendet av nyckelpersoner som kan utgöra ett hot mot säkerheten i systemet eller tjänster och planera lämpliga åtgärder.

Att tillhandahålla tillräcklig kapacitet kan uppnås genom att öka kapaciteten eller genom att minska efterfrågan. Exempel på åtgärder för hantering av efterfrågan på kapacitet:

a) borttagning av föråldrade data (diskutrymme);

b) avvecklingen av tillämpningar, system, databaser eller miljöer;

c) optimera batchprocesser och scheman;

d) optimera logiken i tillämpningar eller databasfrågor;

e) att neka eller begränsa bandbredd för resurskrävande tjänster om dessa inte är verksamhetskritiska (t.ex. strömmande video).

En dokumenterad kapacitetsplan bör övervägas för verksamhetskritiska system.

Övrig information

Denna säkerhetsåtgärd avser också kapacitetsbehov avseende personal, samt kontorslokaler och anläggningar.

12.1.4 Separation av utvecklings-, test- och driftmiljöer

Säkerhetsåtgärd

Utvecklings-, test- och driftmiljöer bör vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

Vägledning för införande

Den grad av separation mellan drift, test och utvecklingsmiljöer som är nödvändig för att förhindra driftproblem bör identifieras och införas.

Följande bör övervägas:

a) regler för överföring av program från utveckling till driftstatus bör definieras och dokumenteras;

b) utvecklingssystem bör hanteras i system eller datorprocessorer och i domäner eller kataloger som inte hanterar produktionssystem;

c) ändringar av produktionssystem och program bör testas i en test- eller mellanstationsmiljö innan överföring till driftsmiljön;

d) annat än i undantagsfall, bör testning inte göras i produktionssystem;

e) kompilatorer, editorer, och andra utvecklingsverktyg eller systemverktyg, bör inte vara tillgängliga från produktionssystem när det inte behövs;

f) användare bör använda olika användarprofiler för produktions- och testsystem och menyer bör visa ett lämpligt identifieringsmeddelande för att minska risken för fel;

g) känslig information bör inte kopieras till testmiljön om inte motsvarande säkerhetsåtgärder som för produktionsmiljön finns för testsystemet (se 14.3).

Övrig information

Utvecklings- och testaktiviteter kan orsaka allvarliga problem, t.ex. oönskade ändringar av filer eller systemmiljön eller systemfel. Det finns ett behov av att upprätthålla en känd och stabil miljö för att utföra meningsfulla tester och för att förhindra att utvecklare får olämplig åtkomst till produktionsmiljön.

Där utvecklings- och testpersonal har tillgång till produktionssystem och information i den, skulle de kunna införa obehörig och otestad kod eller förändra produktionsdata. På vissa system kan denna förmåga missbrukas för att begå bedrägeri eller införa otestade eller skadlig kod som kan vålla allvarliga driftsproblem.

Utvecklare och testare kan också utgöra ett hot mot konfidentialiteten för driftsinformation. Utvecklings- och testverksamhet kan orsaka oavsiktliga ändringar i program eller information om de delar samma miljö. Att separera utvecklings-, test- och produktionsmiljöer är därför önskvärt för att minska risken för oavsiktlig förändring eller obehörig åtkomst till produktionssystem och verksamhetsdata (se 14.3 för skydd av testdata).

12.2 Skydd mot skadlig kod

Mål: Att säkerställa att information och informationsbehandlingsresurser skyddas mot skadlig kod.

12.2.1 Säkerhetsåtgärder mot skadlig kod

Säkerhetsåtgärd

Upptäckande, förebyggande och återställande säkerhetsåtgärder för att skydda mot skadlig kod bör införas i kombination med säkerställande av en lämplig nivå av medvetenhet hos användarna.

Vägledning för införande

Skydd mot skadliga program bör baseras på program för upptäckande av skadlig kod och återställning, informationssäkerhetsmedvetenhet och korrekt åtkomst till system och förändringshantering. Följande riktlinjer bör övervägas:

a) att upprätta en formell regel som förbjuder användningen av icke-auktoriserade program (se 12.6.2 och 14.2.);

b) införa säkerhetsåtgärder som förhindrar eller upptäcker obehöriga program (t.ex. sammanställning över godkända tillämpningar);

c) införa säkerhetsåtgärder som förhindrar eller upptäcker användning av kända eller misstänkta skadliga webbplatser (t.ex. ”svartlistning”);

d) att upprätta en formell regel för att skydda mot risker i samband med erhållande av filer och program från eller via externa nätverk eller annat medium som anger vilka skyddsåtgärder som bör vidtas;

e) att minska sårbarheter som kan utnyttjas av skadlig kod, exempelvis genom hantering av tekniska sårbarheter (se 12.6);

f) genomföra regelbundna översyner av program och datainnehåll för system som stöder verksamhetskritiska processer. Förekomst av icke godkända filer eller obehöriga ändringar bör utredas särskilt;

g) installation och regelbunden uppdatering av program för upptäckt av skadlig kod och återställning som skannar datorer och media som en förebyggande säkerhetsåtgärd eller rutinmässigt. Sökningen som utförs bör omfatta:

   1) alla filer som tas emot via nätverk, eller via någon form av media, avseende förekomst av skadlig kod innan användning;

   2) bifogade filer till e-post och nedladdningar avseende förekomst av skadlig kod innan användning. Genomsökningen bör utföras på flera ställen, som t.ex. e-postservrar, bärbara datorer och vid anslutning till organisationens nätverk;

   3) webbsidor avseende förekomst av skadlig kod;

h) definiera rutiner och ansvar för hantering av system för skydd mot skadlig kod, användarutbildning, rapportering och återhämtning från attacker orsakade av skadlig kod;

i) förbereda lämpliga kontinuitetsplaner för återhämtning från attacker orsakade av skadlig kod, inklusive alla nödvändiga uppgifter och program för säkerhetskopiering och återställning (se 12.3);

j) genomföra rutiner för att regelbundet samla in information, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod;

k) genomförande av rutiner för att granska information om skadlig kod och säkerställa att varningsinformation är korrekt och informativ. Verksamhetsansvariga bör se till att kvalificerade källor, t.ex. välrenommerade tidskrifter, tillförlitliga webbplatser eller leverantörer som producerar program till skydd mot skadlig kod används, för att skilja mellan ryktesspridning och verklig skadlig kod. Alla användare bör göras medvetna om problemet med ryktesspridning och lämpliga åtgärder om det inträffar;

l) isolera miljöer där påverkan kan vara katastrofal.

Övrig information

Användning av två eller flera program som skydd mot skadliga program i hela informationsbehandlingsmiljön från olika leverantörer och med olika teknik kan förbättra verkan av skyddet mot skadlig kod.

Försiktighet bör iakttas för att skydda sig mot införandet av skadlig kod vid underhåll och vid akuta åtgärder, då normala säkerhetsåtgärder mot skadlig kod kan kringgås.

Under vissa förutsättningar kan säkerhetsåtgärder mot skadlig kod orsaka störningar inom verksamheten.

Användning av program för upptäckt av skadlig kod och återställning som enda säkerhetsåtgärd mot skadlig kod är oftast inte tillräckligt och måste ofta åtföljas av driftsrutiner som hindrar införandet av skadlig kod.

12.3 Säkerhetskopiering

Mål: Att skydda mot förlust av data.

12.3.1 Säkerhetskopiering av information

Säkerhetsåtgärd

Säkerhetskopior av information, program och speglingar av system bör tas och testas regelbundet i enlighet med överenskomna regler för säkerhetskopiering.

Vägledning för införande

Regler för säkerhetskopiering bör fastställas för att definiera organisationens krav på säkerhetskopiering av information, program och system.

Principen för säkerhetskopiering bör definiera krav på lagring och skydd.

Det bör finnas lämplig utrustning för säkerhetskopiering för att se till att all nödvändig information och alla program kan återställas efter en katastrof eller fel på media.

Vid utformning av en plan för säkerhetskopiering, bör följande beaktas:

a) korrekta och fullständiga register över säkerhetskopior och dokumenterade återställanderutiner utarbetas;

b) omfattning (t.ex. fullständig eller begränsad säkerhetskopiering) och frekvensen av säkerhetskopior bör återspegla kraven i organisationen, säkerhetskraven avseende den aktuella informationen och betydelsen av informationen för den fortsatta driften av organisationen;

c) säkerhetskopiorna bör förvaras på annan plats och på tillräckligt avstånd för att inte utsättas för eventuella skador vid katastrof på det ordinarie driftstället;

d) säkerhetskopierad information bör ges en lämplig nivå av fysiskt och miljömässigt skydd (se avsnitt 11) som överensstämmer med kraven för det ordinarie driftstället;

e) säkerhetskopior bör testas regelbundet för att säkerställa att de kan användas för nödsituationer vid behov. Detta bör kombineras med ett test av återställanderutiner och granskas avseende tidsåtgång för återställning. Test av återställning av säkerhetskopierad data bör utföras på dedikerat media och inte genom att skriva över den ursprungliga lagringsmedian, i de fall då säkerhetskopieringen eller återställningen misslyckas och orsakar irreparabel skada på, eller förlust av, data;

f) i situationer där konfidentialitet är av betydelse, bör säkerhetskopior skyddas genom kryptering.

Driftsrutiner bör inbegripa övervakning av säkerhetskopiering, hantera fel vid schemalagda säkerhetskopieringar, samt att säkerställa att säkerhetskopieringen är fullständig enligt reglerna för säkerhetskopiering.

Säkerhetskopiering för enskilda system och tjänster bör testas regelbundet för att säkerställa att de uppfyller kraven i kontinuitetsplaner. För kritiska system och tjänster bör säkerhetskopiering omfatta all information, alla program och all data som krävs för att återställa hela systemet i händelse av en katastrof.

Lagringstid för viktig verksamhetsinformation bör fastställas med hänsyn till eventuella krav på arkivkopior som behålls permanent.

12.4 Loggning och övervakning

Mål: Att logga händelser och skapa bevis.

12.4.1 Loggning av händelser

Säkerhetsåtgärd

Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser bör skapas, bevaras och granskas regelbundet.

Vägledning för införande

Händelseloggar bör innehålla, när det är relevant:

a) användarkonto;

b) systemaktiviteter;

c) datum, tider och uppgifter om viktiga händelser, t.ex. inloggning och utloggning;

d) enhetens identitet eller plats, om möjligt, och systemidentifierare;

e) register över lyckade och misslyckade åtkomstförsök till system;

f) poster av lyckade och misslyckade åtkomstförsök till data och andra resurser;

g) förändringar i systemkonfiguration;

h) användning av privilegierad åtkomst;

i) användning av systemverktyg och tillämpningar;

j) åtkomst till filer och typ av åtkomst;

k) nätverksadresser och protokoll;

l) alarm från systemet för åtkomstkontroll;

m) aktivering och inaktivering av säkerhetsverktyg, som anti-virussystem och intrångsdetekteringssystem;

n) register över transaktioner som utförs av användare i tillämpningar.

Loggning av händelser utgör grunden för automatiserade övervakningssystem som är kapabla att skapa konsoliderade rapporter och varningar avseende säkerhet i system och tillämpningar.

Övrig information

Händelseloggar kan innehålla känsliga data och personinformation. Lämpliga säkerhetsåtgärder för konfidentialitet bör vidtas (se 18.1.4).

Om möjligt bör inte systemadministratörer ha behörighet att radera eller inaktivera loggar som innefattar egna aktiviteter (se 12.4.3).

12.4.2 Skydd av logginformation

Säkerhetsåtgärd

Loggningsverktyg och logginformation bör skyddas mot manipulation och obehörig åtkomst.

Vägledning för införande

Säkerhetsåtgärder bör syfta till att skydda mot obehöriga ändringar i logginformation och operativa problem med loggningsverktyg inklusive:

a) ändringar av de meddelandetyper som registreras;

b) loggfiler som redigeras eller tas bort;

c) kapaciteteten för lagring av loggdata överskrids, vilket resulterar i antingen att registreringen av händelser upphör eller att tidigare registrerade händelser skrivs över.

Vissa granskningsloggar bör arkiveras utifrån regler för dokumenterad information eller utifrån krav på insamling och bevarande av bevis (se 16.1.7).

Övrig information

Systemloggar innehåller ofta en stor mängd information varav mycket är ovidkommande för övervakning av informationssäkerheten. Identifieringen av viktiga händelser för övervakning av informationssäkerhet underlättas genom att relevanta meddelandetyper kopieras automatiskt till en andra logg, eller genom användningen av lämpliga verktyg för att analysera filer.

Systemloggar måste skyddas. Om data kan ändras eller tas bort i dem kan deras existens skapa en falsk känsla av säkerhet. Realtidskopiering av loggar till ett system utan åtkomsträtt från systemadministratör eller operatör kan skydda loggar.

12.4.3 Administratörs- och operatörsloggar

Säkerhetsåtgärd

Systemadministratörers och systemoperatörers aktiviteter bör loggas och loggarna bör skyddas och granskas regelbundet.

Vägledning för införande

Användare med privilegierade användarkonton kan eventuellt manipulera loggarna på informationsbehandlingsresurser. Därför är det nödvändigt att skydda och granska loggarna för att säkerställa ansvarsskyldighet för privilegierade användare.

Övrig information

Ett intrångsdetekteringssystem utan åtkomsträtt från system- och nätverksadministratörer kan användas för att övervaka efterlevnad i system och nätverk.

12.4.4 Synkronisering av tid

Säkerhetsåtgärd

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller säkerhetsdomän bör synkroniseras mot en och samma referenskälla för tid.

Vägledning för införande

Krav på redovisning av tidsuppgifter, synkronisering och noggrannhet bör dokumenteras. Sådana krav kan hänföras till författningar, avtal, standarder, eller krav på intern övervakning. En standardiserad referenstid bör användas inom organisationen.

Organisationen bör implementera och dokumentera en tillförlitlig teknisk lösning för att tidssynkronisera interna klockor mot en extern referenstid.

Övrig information

Korrekt inställning av tid är viktig för att säkerställa riktigheten av granskningsloggar, som kan krävas för undersökningar eller som bevis i rättsliga eller disciplinära ärenden. Felaktiga granskningsloggar kan försvåra sådana utredningar och skada trovärdigheten i bevis. En klocka som länkas till en tid från ett nationellt atomur kan användas som tid för loggsystemet. Ett protokoll för nätverkstid kan användas för att tidssynkronisera alla servrar.

12.5 Styrning av driftsystem

Mål: Att säkerställa riktigheten hos driftsystem.

12.5.1 Installation av program på driftsystem

Säkerhetsåtgärd

Rutiner bör införas för att styra installation av program på driftsystem.

Vägledning för införande

Följande riktlinjer bör övervägas för att styra ändringar av program på driftsystem:

a) uppdatering av operativsystem, tillämpningar och programbibliotek bör endast utföras av utbildade administratörer efter tillstånd från rätt ledningsfunktion (se 9.4.5);

b) driftsystem bör endast innehålla godkänd exekverbar kod och inte utvecklingskod eller kompilatorer;

c) tillämpningar och operativsystem bör endast införas efter omfattande och lyckade tester. Testerna bör täcka användbarhet, säkerhet, effekter på andra system och användarvänlighet och bör utföras på separata system (se 12.1.4). Det bör säkerställas att alla motsvarande programs källkodsbibliotek har uppdaterats;

d) ett system för konfigurationsstyrning bör användas för att styra alla införda program och systemdokumentationen;

e) en plan för återställning bör finnas innan förändringar genomförs;

f) en granskningslogg bör upprätthållas för alla uppdateringar i bibliotek för driftsystems;

g) tidigare versioner av program bör bibehållas som en kompletterande åtgärd;

h) gamla versioner av program bör arkiveras, tillsammans med all information och de parametrar som krävs, rutiner, konfigurationsinformation och supportprogram så länge data lagras i arkivet.

Program från leverantör som används i driftsystem bör underhållas på en nivå som stöds av leverantören. Över tid kan programleverantörer upphöra att stödja äldre versioner av program. Organisationen bör överväga riskerna med att förlita sig på program som inte stöds.

Beslut om att uppgradera till en ny version bör väga in verksamhetskraven för ändringen och säkerheten i den nya versionen. Det kan t.ex. innefatta nya funktioner för informationssäkerhet som har tillkommit, och hur många informationssäkerhetsproblem den nya versionen uppvisar samt hur allvarliga de är. Uppdateringar bör installeras när de kan ta bort eller minska sårbarheter(se 12.6).

Fysisk eller logisk tillgång bör endast ges till leverantörer vid behov av underhåll och med ledningens godkännande. Leverantörens aktiviteter bör övervakas (se 15.2.1).

Program kan vara beroende av externt levererade program och moduler. De bör övervakas och styras för att undvika obehöriga ändringar som skulle kunna innebära att sårbarheter införs.

12.6 Hantering av tekniska sårbarheter

Mål: Att förhindra utnyttjande av tekniska sårbarheter.

12.6.1 Hantering av tekniska sårbarheter

Säkerhetsåtgärd

Information om tekniska sårbarheter i de informationssystem som används bör erhållas i tid, organisationens exponering för sådana sårbarheter analyseras och lämpliga åtgärder vidtas för att behandla den tillhörande risken.

Vägledning för införande

En aktuell och fullständig inventering av tillgångar (se paragraf 8) är en förutsättning för en verkningsfull hantering av tekniska sårbarheter. Specifik information som behövs för att stödja hantering av tekniska sårbarheter inkluderar programleverantör, versionsnummer, driftsättning (t.ex. vilket program som är installerat på vilka system) och den, eller de, personer inom organisationen som ansvarar för programmet.

Lämpliga, snabba åtgärder bör vidtas vid identifiering av potentiella tekniska sårbarheter. Följande riktlinjer bör följas för att upprätta en verkningsfull process för hantering av tekniska sårbarheter:

a) organisationen bör fastställa roller och ansvar för hantering av tekniska sårbarheter, inkluderande övervakning av sårbarheter, riskbedömning av sårbarheter, uppdateringar av system och övervakning av tillgångar samt för den samordning som krävs;

b) informationsresurser som används för att identifiera relevanta tekniska sårbarheter och upprätthålla medvetenheten om dem, bör identifieras för program och annan teknik (baserat på inventering av tillgångar, se 8.1.1). Dessa informationsresurser bör uppdateras när inventering av tillgångar förändras eller när andra nya eller användbara resurser identifieras;

c) en tidsgräns bör definieras för agerande på information om potentiellt relevanta tekniska sårbarheter;

d) när en potentiell teknisk sårbarhet har upptäckts bör organisationen analysera riskerna och identifiera åtgärder som bör vidtas. Sådana åtgärder kan inkludera uppdateringar av sårbara system eller vidtagande av andra säkerhetsåtgärder;

e) beroende på hur snabbt en teknisk sårbarhet behöver åtgärdas bör de åtgärder som vidtas utföras i enlighet med de säkerhetsåtgärder som avser förändringshantering (se 12.1.2) eller genom att följa rutiner för incidenthantering (se 16.1.5);

f) om det finns en uppdatering från en legitim källa bör risker i samband med installation av uppdateringen bedömas (riskerna med sårbarheten bör jämföras med risken för installation av uppdateringen);

g) uppdateringar bör testas och utvärderas innan de installeras för att säkerställa att de är verkningsfulla och inte leder till effekter som inte kan tolereras. Om ingen uppdatering är tillgänglig, bör andra säkerhetsåtgärder övervägas, såsom att:

   1) stänga av tjänster eller funktioner relaterade till sårbarheten;

   2) anpassa eller lägga till säkerhetsåtgärder för åtkomst, exempelvis i brandväggar eller vid gräns för nätverk (se 13.1);

   3) öka övervakningen för att upptäcka verkliga attacker;

   4) öka medvetenheten om sårbarheten;

h) en logg bör hållas för alla vidtagna åtgärder;

i) processen för hantering av tekniska sårbarheter bör regelbundet övervakas och utvärderas för att säkerställa dess effektivitet och verkan;

j) system med hög risk bör åtgärdas först;

k) en verkningsfull process för hantering av tekniska sårbarheter bör samordnas med incidenthantering när det gäller att ge underlag om sårbarheter till funktionen för incidenthantering och för att ta fram tekniska åtgärder som kan användas om en incident inträffar;

l) definiera en rutin för att hantera situationen då sårbarheter har upptäckts men det saknas lämplig motåtgärd. I denna situation bör organisationen utvärdera risker avseende känd sårbarhet och definiera lämpliga upptäckande och korrigerande åtgärder.

Övrig information

Hantering av tekniska sårbarheter kan ses som en delprocess inom ändringshantering och nyttja processer och rutiner för ändringshantering (se 12.1.2 och 14.2.2).

Leverantörer är ofta under stor press att släppa uppdateringar så snart som möjligt. Därför finns det en möjlighet att en uppdatering inte löser problemet och har negativa effekter. I vissa fall kan det vara svårt att återställa en införd uppdatering.

Om test av uppdateringar inte är möjligt, t.ex. på grund av kostnader eller bristen på andra resurser kan organisationen överväga att avvakta införandet av uppdateringen för att utvärdera riskerna baserat på de erfarenheter som rapporterats av andra användare. Användning av ISO/IEC 27031[14] kan vara till nytta.

12.6.2 Restriktioner för installation av program

Säkerhetsåtgärd

Regler för programinstallationer som utförs av användare bör upprättas och införas.

Vägledning för införande

Organisationen bör definiera och verkställa regler för vilka typer av program en användare kan installera.

Principen om minsta privilegium bör tillämpas. Om vissa privilegier tilldelas kan användare ha möjlighet att installera program. Organisationen bör identifiera vilka typer av programinstallationer som tillåts (t.ex. uppdateringar och säkerhetskorrigeringar till befintliga program) och vilka typer av installationer som är förbjudna (t.ex. program som är endast för personligt bruk och program vars ursprung när det gäller att vara potentiellt skadliga är okänt eller misstänkt). Dessa privilegier bör beviljas med hänsyn till berörda användarroller.

Övrig information

Okontrollerad installation av program kan leda till införande av sårbarheter och leda till obehörig åtkomst till information, förlust av riktighet, andra informationssäkerhetsincidenter eller överträdelse av immateriella rättigheter.

12.7 Överväganden gällande revision av informationssystem

Mål: Att minimera revisionsverksamhetens påverkan på driftsystem.

12.7.1 Revisionskontroller för informationssystem

Säkerhetsåtgärd

Revisionskrav och revisionsaktiviteter som omfattar verifiering av status på driftsystem bör planeras noggrant och godkännas för att minimera störningar i verksamhetsprocesser.

Vägledning för införande

Följande riktlinjer bör övervägas:

a) krav på åtkomst till system och data bör avtalas med lämplig ledningsfunktion;

b) omfattningen av tekniska revisionsaktiviteter bör överenskommas och styras;

c) revisionsaktiviteter bör begränsas till skrivskyddad åtkomst av program och data;

d) annan åtkomst än skrivskyddad bör endast tillåtas på kopior av systemfiler som bör raderas när granskningen är klar eller ges lämpligt skydd om det finns en skyldighet att spara sådana filer som dokumenterad information;

e) krav för särskild eller ytterligare bearbetning bör identifieras och avtalas;

f) revisionstester som kan påverka tillgänglighet bör köras utanför kontorstid;

g) all åtkomst bör övervakas och loggas för att producera en spårbarhetskedja.

13 Kommunikationssäkerhet

13.1 Hantering av nätverkssäkerhet

Mål: Att säkerställa skyddet av information i nätverk och dess stödjande informationsbehandlingsresurser.

13.1.1 Säkerhetsåtgärder för nätverk

Säkerhetsåtgärd

Nätverk bör hanteras och styras för att skydda information i system och tillämpningar.

Vägledning för införande

Säkerhetsåtgärder bör införas för att säkerställa säkerheten för information i nätverk och skyddet av anslutna tjänster från obehörig åtkomst. Följande bör övervägas:

a) ansvar och rutiner för förvaltning av nätverksutrustning bör fastställas;

b) operativt ansvar för nätverk bör skiljas från datadrift där så är lämpligt (se 6.1.5);

c) särskilda säkerhetsåtgärder bör fastställas att garantera konfidentialitet och riktighet för data som passerar via offentliga nätverk eller trådlösa nätverk och för att skydda anslutna system och tillämpningar (se avsnitt 10 och 13.2). Särskilda säkerhetsåtgärder kan också krävas för att upprätthålla tillgängligheten av nätverkstjänster och anslutna enheter;

d) lämplig loggning och övervakning bör tillämpas för att möjliggöra registrering och upptäckt av åtgärder som kan påverka eller vara relevanta för informationssäkerheten;

e) förvaltning bör vara nära samordnad både att optimera tjänsten till organisationen och för att säkerställa att säkerhetsåtgärderna tillämpas konsekvent över hela infrastrukturen för informationsbehandling;

f) system i nätverket bör autentiseras;

g) systemanslutningar till nätverket bör begränsas.

Övrig information

Ytterligare information om nätverkssäkerhet kan hittas i ISO/IEC 27033[15][16][17][18][19].

13.1.2 Säkerhet hos nätverkstjänster

Säkerhetsåtgärd

Säkerhetsmekanismer, tjänstenivåer och ledningskrav vad gäller alla nätverkstjänster bör identifieras och inkluderas i avtal för nätverkstjänster, oavsett om dessa tjänster tillhandahålls internt eller som outsourcade tjänster.

Vägledning för införande

Leverantörens förmåga att hantera avtalade tjänster på ett säkert sätt bör fastställas och regelbundet övervakas och rätt till revision bör vara avtalad.

Säkerhetsarrangemang som är nödvändiga för särskilda tjänster, som säkerhetsfunktioner, tjänstenivåer och verksamhetskrav, bör identifieras. Organisationen bör se till att leverantörer av nätverkstjänster genomför dessa åtgärder.

Övrig information

Nätverkstjänster omfattar tillhandahållande av anslutningar, privata nättjänster och nät med värdeskapande tjänster, samt nätverkssäkerhetslösningar som brandväggar och intrångsdetekteringssystem. Dessa tjänster kan variera från enkla bredbandsanslutningar till komplexa värdeskapande lösningar.

Säkerhetsfunktionerna i nätverkstjänster kan vara:

a) teknik för säkerhet inom nätverkstjänster som autentisering, kryptering och uppkoppling av nätverk;

b) tekniska parametrar som krävs för skyddad anslutning till nätverkstjänster i överensstämmelse med reglerna för säkerhet och nätverkanslutning;

c) rutiner för användning av nätverkstjänster som vid behov begränsar åtkomsten till nätverkstjänster eller tillämpningar.

13.1.3 Separation av nätverk

Säkerhetsåtgärd

Grupper av informationstjänster, användare och informationssystem bör separeras i nätverk.

Vägledning för införande

En metod för att hantera säkerheten för stora nätverk är att dela in dem i separata nätverksdomäner. Domäner kan väljas utifrån förtroendenivåer (t.ex. domän med publik tillgång, pc-domän, server-domän), efter organisationsenheter (t.ex. personal, ekonomi, marknadsföring) eller en kombination (t.ex. server-domän som ansluter till flera organisationsenheter). Separation kan genomföras antingen fysiskt mellan olika nätverk eller genom olika logiska nätverk (t.ex. virtuella privata nätverk).

Avgränsningen för varje domän bör vara väldefinierad. Åtkomst mellan nätverksdomäner är tillåten, men bör styras i dess yttre avgränsning via särskild närverksnod (t.ex. brandvägg, router-filtrering). Kriterierna för separation av nätverksdomäner och åtkomst via nätverksnoder, bör baseras på en bedömning av säkerhetskraven för varje domän. Bedömningen bör göras enligt principerna för styrning av åtkomst (se 9.1.1), samt kraven på, värdet av och klassningen av den information som behandlas. Bedömningen bör också ta hänsyn till den relativa effekten gällande kostnad och prestanda av att införa lämplig teknik för nätverksnoder.

Trådlösa nätverk kräver särskild behandling på grund av att dess yttre avgränsningar är diffusa. För känsliga miljöer bör organisationen överväga att hantera all trådlös åtkomst som externa anslutningar (se 9.4.2). Organisationen bör avskilja denna åtkomst från interna nät tills det att åtkomst sker via en nätverksnod som följer åtkomstregler för nätverk (se 13.1.1) innan åtkomst till interna system beviljas.

Autentisering, kryptering och skyddsåtgärder för åtkomst till nätverk på användarnivå i trådlösa nätverk som bygger på moderna protokoll, kan vara tillräckligt för direkt anslutning till organisationens interna nätverk när de införts på ett korrekt sätt.

Övrig information

Nätverk sträcker sig ofta utöver organisatoriska gränser. Samarbeten som kräver sammankoppling eller delning av informationsbehandlingsresurser och nätverksresurser upprättas mellan organisationer. Sådana utökningar av nätverk kan öka risken för obehörig åtkomst till organisationens informationssystem. Vissa av dessa system kan behöva skyddas från andra nätverksanvändare på grund av systemens känslighet eller avgörande betydelse.

13.2 Informationsöverföring

Mål: Att upprätthålla säkerheten hos information som överförs inom en organisation eller till en extern enhet.

13.2.1 Regler och rutiner för informationsöverföring

Säkerhetsåtgärd

Formella regler, rutiner och säkerhetsåtgärder bör vara införda för att skydda överföring av information genom användning av alla typer av kommunikationsmedel.

Vägledning för införande

När kommunikationsmedel för informationsöverföring används bör följande rutiner och säkerhetsåtgärder övervägas:

a) rutiner för att skydda överförd informationen från avlyssning, kopiering, ändring, oönskad nätverksstyrning och förstörelse;

b) rutiner för identifiering av och skydd mot skadlig kod som kan överföras med hjälp av elektronisk kommunikation (se 12.2.1);

c) rutiner för att skydda kommunicerad känslig elektronisk information som är i form av en bifogad fil;

d) regel eller riktlinjer som beskriver acceptabel användning av kommunikationsmöjligheter (se 8.1.3);

e) anställdas, externa parters, eller andra användares ansvar att inte kompromettera organisationen, exempelvis genom förtal, trakasserier, personifiering, vidarebefordran av kedjebrev, obehöriga köp, etc.

f) användning av krypteringsteknik t.ex. att skydda konfidentialitet, riktighet och autenticitet avseende information (se avsnitt 10);

g) riktlinjer för lagring och hantering av all verksamhetskorrespondens, inklusive meddelanden, i enlighet med relevanta nationella och lokala lagar och förordningar;

h) säkerhetsåtgärder och begränsningar vid användning av vissa kommunikationsmedel såsom t.ex. automatisk vidarebefordran av e-post till externa e-postadresser;

i) rådgivande information till personal att iaktta lämpliga försiktighetsåtgärder för att inte avslöja konfidentiell information;

j) inte lämna meddelanden som innehåller konfidentiell information på telefonsvarare eftersom dessa kan spelas upp av obehöriga, lagras på gemensamma system eller lagras felaktigt till följd av felslagning av nummer;

k) rådgivande information till personal om risker vid användning av telefaxapparater eller tjänster, som t.ex:

   1) obehörig åtkomst till lagrade meddelanden;

   2) avsiktlig eller oavsiktlig programmering av särskilda nummer för att skicka meddelanden;

   3) skickande av dokument och meddelanden till fel mottagare genom felaktig inmatning av nummer eller fel i programmerade nummer.

Personal bör dessutom påminnas om att de inte bör genomföra samtal som berör konfidentiell information på offentliga platser, över osäkra kommunikationskanaler, i öppna kontor eller vid öppna mötesplatser.

Tjänster för överföring av information bör uppfylla alla relevanta legala krav (se 18.1).

Övrig information

Information kan överföras med hjälp av ett antal olika typer av kommunikationsmedel, inklusive e-post, tal, telefax och video.

Program kan överföras genom olika medier, inklusive nedladdning från Internet och genom köp av hyllvaruprodukter.

De verksamhetsrelaterade, rättsliga och säkerhetsmässiga konsekvenserna av elektroniskt datautbyte, elektronisk handel och elektronisk kommunikation och kraven för säkerhetsåtgärder bör övervägas.

13.2.2 Överenskommelser om informationsöverföring

Säkerhetsåtgärd

Säker överföring av verksamhetsinformation mellan organisationen och externa parter bör vara reglerad i överenskommelser.

Vägledning för införande

Överenskommelser om informationsöverföring bör innehålla följande:

a) ledningsansvar för att styra och anmäla överföring, sändning och mottagande;

b) rutiner för att säkerställa spårbarhet och oavvislighet;

c) tekniska minimistandarder för paketering och överföring;

d) depositionsavtal;

e) rutiner för identifiering av bud;

f) ansvarsförhållanden och skadeståndsskyldighet i händelse av informationssäkerhetsincident, såsom förlust av data;

g) användning av överenskommen märkning för känslig eller kritisk information, som säkerställer att innebörden av märkningen förstås omedelbart och att informationen skyddas på lämpligt sätt (se 8.2);

h) tekniska standarder för registrering och att läsa information och program;

i) särskilda säkerhetsåtgärder som krävs för att skydda känsliga tillgångar och objekt, till exempel kryptografi (se avsnitt 10);

j) att upprätthålla en ansvarskedja för information under överföring;

k) acceptabla nivåer av åtkomststyrning.

Regler, rutiner och standarder bör fastställas och bibehållas för att skydda information och fysiska medier under transport (se 8.3.3), och bör refereras till i avtal om överföring.

Innehåll i avtal som rör informationssäkerhet bör återspegla den berörda informationens känslighet.

Övrig information

Överenskommelser kan vara elektroniska eller skriftliga, och de kan utgöras av formella avtal. För konfidentiell information bör de specifika mekanismer som används för överföring av sådan information följas konsekvent, för alla organisationer och för alla typer av avtal.

13.2.3 Elektronisk meddelandehantering

Säkerhetsåtgärd

Information som hanteras genom elektronisk meddelandehantering bör ha tillräckligt skydd.

Vägledning för införande

Överväganden avseende informationssäkerhet för elektroniska meddelanden bör innehålla följande:

a) skydd av meddelanden från obehörig åtkomst, från ändring eller från avbrott i tjänsten, och som står i proportion till det klassningssystem som har antagits av organisationen;

b) att säkerställa korrekt adressering och överföring av meddelandet;

c) tillförlitlighet och tillgänglighet för tjänsten;

d) legala överväganden, t.ex. krav på elektroniska signaturer;

e) att erhålla godkännande innan användning av externa offentliga tjänster som meddelandetjänster, sociala nätverk eller fildelning;

f) starkare nivåer av autentisering för kontroll av åtkomst från publika nät.

Övrig information

Det finns många typer av elektroniska meddelanden som e-post, elektroniskt datautbyte och sociala nätverk som spelar en roll i verksamhetens kommunikation.

13.2.4 Konfidentialitet och förbindelser om konfidentialitet

Säkerhetsåtgärd

Krav på konfidentialitet eller förbindelser rörande konfidentialitet som återspeglar organisationens behov av skydd av information bör identifieras, regelbundet granskas och dokumenteras.

Vägledning för införande

Avtal rörande konfidentialitet eller tystnadsplikt bör omfatta krav för att skydda konfidentiell information med hjälp av juridiskt bindande villkor. Avtal rörande sekretess eller tystnadsplikt är tillämpliga på externa parter eller anställda i organisationen. Avtalstext bör läggas till med hänsyn till typ av part, dess tillåtna åtkomst eller hantering av konfidentiell information. För att identifiera krav på konfidentialitet eller tystnadsplikt, bör följande övervägas:

a) en definition av vilka uppgifter som behöver skyddas (t.ex. konfidentiell information);

b) förväntad varaktighet av avtal, inklusive fall där konfidentialitet kan gälla på obestämd tid;

c) åtgärder som krävs när ett avtal upphör;

d) ansvar och åtgärder för undertecknande parter att undvika obehörigt avslöjande av information;

e) ägande av information, affärshemligheter, immateriell äganderätt och hur detta relaterar till skydd av konfidentiell information;

f) tillåten användning av konfidentiell information och nyttjanderätter för undertecknande parter till information;

g) rätten att granska och övervaka aktiviteter som involverar konfidentiell information;

h) skyldighet att anmäla och rapportera obehörigt röjande eller läckage av konfidentiell information;

i) villkor för hur information returneras eller förstörs vid avtalets upphörande;

j) åtgärder vid avtalsbrott.

Baserat på en organisations säkerhetskrav kan andra villkor behövas i ett avtal rörande konfidentialitet eller tystnadsplikt.

Avtal rörande konfidentialitet och tystnadsplikt bör uppfylla alla tillämpliga författningar för det område som de avses att tillämpas inom (se 18.1).

Avtalskrav rörande konfidentialitet och tystnadsplikt bör ses över med jämna mellanrum och när förändringar inträffar som påverkar dessa avtalskrav.

Övrig information

Avtal rörande konfidentialitet och tystnadsplikt skyddar organisationens information och upplyser de som undertecknar avtal om deras ansvar för att skydda, använda och tillgängligöra information på ett ansvarsfullt och godkänt sätt.

Det kan finnas ett behov för en organisation att använda olika former av avtal för konfidentialitet eller tystnadsplikt under olika omständigheter.

14 Anskaffning, utveckling och underhåll av system

14.1 Säkerhetskrav på informationssystem

Mål: Att säkerställa att informationssäkerhet är en integrerad del av informationssystem över hela livscykeln. Detta inkluderar krav på informationssystem som tillhandahåller tjänster via publika nätverk.

14.1.1 Analys och specifikation av informationssäkerhetskrav

Säkerhetsåtgärd

Krav som rör informationssäkerhet bör inkluderas i kraven för nya informationssystem eller förbättringar av befintliga informationssystem.

Vägledning för införande

Informationssäkerhetskraven bör identifieras med hjälp av olika metoder som t.ex. härledning från författningar och interna regelverk, riskanalyser, analys av incidenter eller användning av sårbarhetsnivåer. Resultaten av identifieringen bör dokumenteras och granskas av alla berörda parter.

Informationssäkerhetskrav och säkerhetsåtgärder bör återspegla värdet av den berörda informationen (se 8.2) och den potentiella negativa påverkan på verksamheten som brist på tillräcklig säkerhet kan leda till.

Identifiering och hantering av informationssäkerhetskrav och associerade processer bör integreras i tidiga projektfaser för informationssystem. Tidig inkludering av informationssäkerhetskrav, t.ex. på projekteringsstadiet kan leda till mer verkningsfulla och kostnadseffektiva lösningar.

Informationssäkerhetskraven bör också:

a) inkludera nivå på förtroende som krävs mot den påstådda identiteten hos användare för att identifiera krav på autentisering;

b) inkludera tilldelning av åtkomst och godkännandeprocesser för användare såväl som för privilegierade eller tekniska användare;

c) informera användare och operatörer om deras skyldigheter och ansvar;

d) inkludera behov av skydd för de tillgångar som berörs, särskilt när det gäller tillgänglighet, konfidentialitet och riktighet;

e) inkludera krav som härrör från verksamhetsprocesser som transaktionsloggning, övervakning och krav på oavvislighet;

f) inkludera krav härledda från andra säkerhetsåtgärder, t.ex. gränssnitt för loggning och övervakning eller system för upptäckt av informationsläckage.

För program som tillhandahåller tjänster via publika nätverk eller som genomför transaktioner bör de särskilt avsedda säkerhetsåtgärderna 14.1.2 och 14.1.3 övervägas.

En formell process för testning och anskaffning bör följas när produkter anskaffas. Avtal med leverantören bör behandla de identifierade säkerhetskraven. Då säkerhetsfunktionen i en föreslagen produkt inte uppfyller angivna krav bör den tillkommande risken och säkerhetsåtgärder som är relaterade till den analyseras innan produkten anskaffas.

Tillgänglig vägledning för säkerhetskonfiguration av produkten, i linje med den slutliga installationen av program eller tjänster i systemet, bör utvärderas och tillämpas.

Godkännandekriterier för produkter bör fastställas t.ex. när det gäller deras funktionalitet som kommer att bekräfta om identifierade säkerhetskrav uppfylls. Produkter bör utvärderas mot dessa kriterier innan anskaffning. Tillkommande funktionalitet bör utvärderas för att säkerställa att det inte medför nya oacceptabla risker.

Övrig information

SS-ISO/IEC 27005[11] och SS-ISO 31000[27] ger vägledning om användningen av riskhanteringsprocessen för att identifiera säkerhetsåtgärder för att uppfylla kraven på informationssäkerhet.

14.1.2 Säkerställande av programtjänster på publika nätverk

Säkerhetsåtgärd

Information i programtjänster på publika nätverk bör skyddas från bedräglig aktivitet, avtalstvist och obehörigt röjande och modifiering.

Vägledning för införande

Säkerhetsöverväganden för programtjänster som passerar över publika nätverk bör innehålla följande information:

a) det förtroende parterna kräver för att lita på varandras påstådda identitet, exempelvis genom autentisering;

b) processer för auktorisation inkluderande vem som kan godkänna innehållet i, utfärda eller signera viktiga transaktioner;

c) säkerställa att kommunicerande parter är fullständigt informerade om auktorisation för tillhandahållande eller användning av tjänsten;

d) fastställa och uppfylla krav på konfidentialitet, riktighet, intyg för sändning eller mottagning av viktiga dokument och oavvislighet av avtal, t.ex. genom upphandlingskrav och avtalsprocesser;

e) krav på tillitsnivå för riktigheten i viktiga dokument;

f) behovet av skydd av konfidentiell information;

g) konfidentialitet och riktighet för ordertransaktioner, betalningsinformation, leveransadresser och kvittenser;

h) kravnivå för verifiering av betalningsinformation från kund;

i) val av mest lämplig form av betalning för skydd mot bedrägerier;

j) skyddsnivå som krävs för att upprätthålla konfidentialitet och riktighet för information;

k) undvikande av förlust eller kopiering av information om transaktioner;

l) ansvar förknippat med bedrägliga transaktioner;

m) försäkringskrav.

Många av ovanstående punkter kan lösas genom användning av kryptografiska säkerhetsåtgärder (se avsnitt 10) med beaktande av legala krav (se avsnitt 18, se särskilt 18.1.5 för legala krav rörande användningen av kryptografi).

Användningen av programtjänster mellan parter bör stödjas av avtal som förpliktar överenskomna villkor för parterna, inklusive detaljer rörande auktorisation (se punkt b) ovan).

Krav på motståndskraft mot attacker bör övervägas, vilket kan inkludera krav för att skydda inblandade servrar eller säkerställa tillgänglighet till de nätverkskomponenter som krävs för att leverera tjänsten.

Övrig information

Tillämpningar som är tillgängliga via publika nätverk är föremål för ett antal nätverksrelaterade hot, t.ex. bedrägerier, avtalstvister eller röjande av information till obehöriga. Därför är detaljerade riskbedömningar och korrekta val av säkerhetsåtgärder nödvändiga. Normalt omfattar dessa säkerhetsåtgärder bland annat kryptografiska metoder för autentisering och säker överföring av data.

Tillämpningstjänster kan använda metoder för autentisering, t.ex. med hjälp av kryptering med publika och privata nycklar samt digitala signaturer (se avsnitt 10) för att minska riskerna. Betrodda tredjeparter kan också användas där sådana tjänster behövs.

14.1.3 Skydd av transaktioner i tillämpningstjänster

Säkerhetsåtgärd

Information hanterad som del i programtjänsters transaktioner bör skyddas för att förhindra ofullständig överföring, felaktig styrning av nätverkstrafik, obehörig ändring av meddelanden, obehörigt röjande, obehörig duplicering av meddelanden eller återuppspelning.

Vägledning för införande

Överväganden avseende informationssäkerhet för programtjänster bör innehålla följande:

a) användningen av elektroniska signaturer mellan inblandade parter i transaktionen;

b) säkerställa att:

   1) användarens konfidentiella autentiseringsinformation för inblandade parter är giltig och verifierad;

   2) transaktionen förblir konfidentiell;

   3) konfidentialiteten för alla berörda parter upprätthålls;

c) kommunikationsvägar mellan alla inblandade parter är krypterade;

d) protokoll som används för kommunikation mellan alla inblandade parter är säkra;

e) att lagringen av transaktionsinformation ej genomförs på allmänt tillgängliga miljöer, t.ex. på en lagringsplattform på organisationens intranät eller behålls och exponeras på lagringsmedia som är direkt åtkomlig från Internet;

f) om en betrodd utfärdare används (t.ex. för att utfärda och underhålla digitala signaturer eller digitala certifikat), att säkerheten upprätthålls i hela processen för hantering av certifikat/signatur från början till slut.

Övrig information

Omfattningen på valda säkerhetsåtgärder bör överensstämma med risknivån på varje form av programtjänsttransaktion.

Transaktioner kan behöva uppfylla legala krav i de jurisdiktioner som transaktionen genereras från, bearbetas i, färdigställs eller lagras i.

14.2 Säkerhet i utvecklings- och supportprocesser

Mål: Att säkerställa att informationssäkerhet designas och införs inom utvecklingscykeln för informationssystem.

14.2.1 Regler för säker utveckling

Säkerhetsåtgärd

Regler för utveckling av program och system bör upprättas och tillämpas vid systemutveckling inom organisationen.

Vägledning för införande

Säker utveckling är en förutsättning för att bygga upp säkra tjänster, arkitekturer, program och system.

Följande aspekter bör övervägas i regler för säker utveckling:

a) säkerhet i utvecklingsmiljön;

b) vägledning om säkerheten i utvecklingscykeln för program:

   1) säkerhet i utvecklingsmetodik för program;

   2) riktlinjer för skapande av säker kod för varje programmeringsspråk som används;

c) säkerhetskraven i designfasen;

d) kontrollpunkter för säkerhet i samband med milstolpar inom projektet;

e) säkerhet i system för versionshantering och lagring av kod;

f) säkerhet i versionskontroll;

g) nödvändig kunskap om säkerhet för tillämpningar;

h) utvecklarnas förmåga att undvika, söka efter och korrigera sårbarheter.

Säker teknik för programmering bör användas både för utveckling och för återanvändning av kod där normerna som tillämpats för utveckling kanske inte är kända eller inte var förenliga med gällande praxis. Standarder för säker kodning bör beaktas och användas i relevanta uppdrag. Utvecklare bör utbildas i skapande av säker kod. Tester och kodgranskning bör styra utvecklingen av säker kod.

Om utveckling läggs ut bör organisationen försäkra sig om att den externa parten uppfyller riktlinjer för säker utveckling (se 14.2.7).

Övrig information

Utveckling kan också äga rum i tillämpningar som Office-program, skript, webbläsare och databaser.

14.2.2 Rutiner för hantering av systemändringar

Säkerhetsåtgärd

Systemförändringar inom utvecklingscykeln bör styras genom användning av formella riktlinjer för ändringshantering.

Vägledning för införande

Riktlinjer för ändringshantering bör finnas som dokumenterad information och efterlevas för att säkerställa riktigheten under hela livscykeln för system, tillämpningar och produkter. Införandet av nya system och större ändringar till befintliga system bör följa en formell process innehållande dokumenterad information, specificering av krav, testning, kvalitetskontroll och styrt införande i verksamheten.

Denna process bör omfatta en riskbedömning, analys av konsekvenser av ändringar och specificering av säkerhetsåtgärder som behövs. Denna process bör också se till att befintliga rutiner för säkerhet och styrning inte äventyras, att supportpersonal endast får tillgång till de delar av systemet som är nödvändigt för deras arbete och att formell överenskommelse och godkännande för varje förändring erhålls.

Där så är praktiskt möjligt bör riktlinjer för ändringshantering av program och driftsättning integreras (se 12.1.2). Riktlinjer för ändringshantering bör inkludera men inte begränsas till att:

a) upprätthålla dokumenterad information rörande överenskomna åtkomstnivåer;

b) se till att ändringar initieras av auktoriserade användare;

c) kontroll av att säkerhetsåtgärder och rutiner för att säkerställa riktighet inte äventyras av ändringarna;

d) identifiera alla program, information, databaser och maskinvara som kräver ändring;

e) identifiera och styra kod som är kritisk för säkerheten för att minimera risken att kända sårbarheter skapas;

f) detaljerade förslag formellt godkänts innan arbetet påbörjas;

g) se till att behöriga användare godkänner ändringar innan de införs;

h) säkerställa att dokumenterad information om system är uppdaterad vid avslutningen av varje förändring och att gammal dokumenterad information arkiveras eller gallras;

i) upprätthålla en versionskontroll för samtliga uppdateringar;

j) säkerställa spårbarhet i hanteringen av alla beställningar om ändringar;

k) säkerställa att användardokumentation (se 12.1.1) och rutiner för användning uppdateras;

l) se till att införande av ändringar sker vid en tidpunkt som inte stör inblandade verksamhetsprocesser.

Övrig information

Förändringar av program kan påverka driftsmiljön och vice versa.

Normalt testas nya program i en miljö som är åtskild från både drifts- och utvecklingsmiljö (se 12.1.4). Detta ger en möjlighet att ha kontroll över nya program och skyddar verksamhetsinformation som används för teständamål. Detta bör omfatta rättningar av program och uppdateringar.

Om automatiska uppdateringar övervägs bör risk för förlust av riktighet och tillgänglighet vägas mot förmån för snabb distribution av uppdateringar. Automatiska uppdateringar bör inte användas på kritiska system då vissa uppdateringar kan orsaka att kritiska program upphör att fungera.

14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö

Säkerhetsåtgärd

När driftsmiljön ändras bör verksamhetskritiska tillämpningar granskas och testas för att säkerställa att det inte innebär negativ påverkan på verksamheten eller säkerheten.

Vägledning för införande

Denna process bör omfatta:

a) kontroll av tillämpningar och rutiner för säkerställande av riktighet för att säkerställa att de inte har äventyrats på grund av förändringar i driftsmiljön;

b) att se till att förändringar i driftsmiljön planeras i tid för att möjliggöra lämpliga tester och granskningar före genomförandet;

c) att säkerställa att lämpliga ändringar införs i kontinuitetsplaner (se avsnitt 17).

Övrig information

Driftsmiljön omfattar operativsystem, databaser och mellanprogram. Säkerhetsåtgärden bör också tillämpas för ändringar av program.

14.2.4 Restriktioner för ändringar av programpaket

Säkerhetsåtgärd

Ändringar av programpaket bör förhindras eller begränsas till nödvändiga ändringar och alla ändringar bör styras noggrant.

Vägledning för införande

Så långt som möjligt och praktiskt genomförbart, bör leverantörens programpaket användas utan modifiering.

Där ett programpaket måste ändras bör följande övervägas:

a) risken för att inbyggda säkerhetsåtgärder och processer för riktighet kompromitteras;

b) om samtycke från leverantören bör inhämtas;

c) möjligheten att få ändringar införda från leverantören som uppdateringar av standardprogram;

d) konsekvenser om organisationen blir ansvarig för framtida underhåll av program till följd av förändringar;

e) kompatibilitet med andra program som används.

Om ändringar är nödvändiga bör det ursprungliga programmet bibehållas och ändringarna genomföras på en kopia. Riktlinjer för uppdateringar av godkända program bör införas för att säkerställa att den senaste godkända versionen inklusive eventuella rättningar är installerad (se 12.6.1). Alla ändringar bör vara testade och dokumenterade så att de kan återanvändas vid framtida uppdateringar. Vid behov kan ändringarna testas och valideras av ett oberoende evalueringsorgan.

14.2.5 Principer för utveckling av säkra system

Säkerhetsåtgärd

Riktlinjer för utveckling av säkra system bör upprättas, dokumenteras, underhållas och tillämpas vid alla införanden av informationssystem.

Vägledning för införande

Riktlinjer för säker systemutveckling som grundas på tekniska säkerhetsprinciper bör inrättas, dokumenteras och tillämpas på intern systemutveckling. Säkerhet bör utformas i alla arkitekturlager (verksamhet, data, program och teknik) genom att balansera behovet av informationssäkerhet med verksamhetens behov av tillgänglighet. Ny teknik bör analyseras avseende säkerhetsrisker och design bör granskas mot kända angreppsmetoder.

Riktlinjer för utveckling av säkra system bör ses över regelbundet för att säkerställa att de verkningsfullt bidrar till förbättrad säkerhet inom utvecklingsprocessen. De bör också ses över regelbundet för att säkerställa att de förblir aktuella när det gäller att motstå eventuella nya potentiella hot och fortsätter vara tillämpliga vid framsteg inom teknik och lösningar.

Riktlinjerna för säker systemutveckling bör tillämpas, där så behövs, på outsourcade informationssystem genom bindande avtal mellan organisationen och leverantören till vilken outsourcing har skett. Organisationen bör säkerställa att leverantörens tillämpning av säkerhet är i nivå med den egna nivån.

Övrig information

Riktlinjer för utveckling av program bör tillämpa tekniker för säker systemutveckling i utvecklingen av program som har gränssnitt för in- och utdata. Säker systemutveckling ger vägledning om användningen av tekniker för autentisering av användare, sessionsstyrning, validering av data och eliminering av kod för felsökning.

14.2.6 Säker utvecklingsmiljö

Säkerhetsåtgärd

För systemutvecklings- och integrationsåtgärder bör organisationen upprätta och på lämpligt sätt skydda säkra utvecklingsmiljöer som sträcker sig över systemets hela livscykel.

Vägledning för införande

En säker utvecklingsmiljö inkluderar människor, processer och teknik som är involverad i systemutveckling och integration.

Organisationer bör bedöma riskerna med utvecklingsarbete för enskilda system och upprätta säkra utvecklingsmiljöer för specifika system avseende:

a) känslighet för data som bearbetas, lagras och överförs genom systemet;

b) tillämpliga externa och interna krav, t.ex. från författningar eller interna regelverk;

c) säkerhetsåtgärder som redan införts i organisationen som berör systemutveckling;

d) pålitlighet hos personal som arbetar i miljön (se 7.1.1);

e) graden av outsourcad systemutveckling

f) behovet av segregering mellan olika utvecklingsmiljöer;

g) styrning av åtkomst till utvecklingsmiljön;

h) övervakning av förändringar av miljön och kod lagrad däri;

i) att säkerhetskopior lagras på säkra alternativa platser;

j) styrning av flödet av data från och till miljön.

När behovet av skydd bestäms för en specifik utvecklingsmiljö, bör organisationer dokumentera information om motsvarande processer i riktlinjer för säker utveckling och ge dessa till alla personer som behöver dem.

14.2.7 Outsourcad utveckling

Säkerhetsåtgärd

Organisationen bör övervaka och styra outsoursad systemutveckling.

Vägledning för införande

Om systemutveckling outsourcas, bör följande punkter tas i beaktande genom organisationens hela externa försörjningskedja:

a) licenser, äganderätt till kod och immateriella rättigheter relaterade till outsourcingen (se 18.1.2);

b) avtalskrav för säker design, kodning och testning (se 14.2.1);

c) tillhandahållande av godkänd hotmodell till den externa utvecklaren;

d) acceptanstest för kvalitet och korrekthet avseende leverabler;

e) tillhandahållande av bevis på att tröskelvärden för säkerhet används för att etablera lägsta acceptabla nivåer av säkerhet och integritet;

f) bevis för att tillräcklig testning har genomförts för skydd mot att skadlig kod, avsiktlig eller oavsiktligt, förs in vid leverans;

Svensk ANM. Den engelska texten anger att skydd bör finnas för frånvaro av skadlig kod. Detta har vid översättningen tolkats som ett fel och är korrigerat i den svenska översättningen.

g) bevis för att tillräcklig testning har genomförts för att skydda mot förekomsten av kända sårbarheter;

h) deposition av kod, t.ex. i händelse av att källkoden inte längre är tillgänglig;

i) avtalad rättighet att genomföra revision av utvecklingsprocesser och säkerhetsåtgärder;

j) giltig dokumenterad information rörande sammansättningen och uppsättning av miljön som används för att skapa leverabler;

k) att organisationen förblir ansvarig för efterlevnad av tillämpliga lagar och verifiering av säkerhetsåtgärdernas verkan.

Övrig information

Ytterligare information om leverantörsrelationer kan hittas i ISO/IEC 27036[21][22][23]

14.2.8 Säkerhetstestning

Säkerhetsåtgärd

Säkerhetsfunktionalitet bör testas vid utveckling.

Vägledning för införande

Nya och uppdaterade system kräver grundlig testning och verifiering under utvecklingsprocessen, inklusive utarbetandet av en detaljerad aktivitetsplan samt testning av indata och förväntad utdata under en rad villkor. Vid intern utveckling, bör sådana tester först utföras av utvecklingsteamet. Oberoende acceptanstest bör sedan göras (både för intern och outsourcad utveckling) för att säkerställa att systemet fungerar som förväntat (se 14.1.1 och 14.1.2). Omfattningen av testerna bör stå i proportion till systemets betydelse.

14.2.9 Acceptanstestning av system

Säkerhetsåtgärd

Program för acceptanstester och relaterade kriterier bör fastställas för nya informationssystem, uppgraderingar och nya versioner.

Vägledning för införande

Systemets acceptanstest bör inkludera testning gentemot ställda säkerhetskrav (se 14.1.1 och 14.1.2) och i enlighet med riktlinjer för säker utveckling (se 14.2.1). Testning bör också genomföras på mottagna komponenter och integrerade system. Organisationer kan dra nytta av automatiserade verktyg, t.ex. verktyg för kodgranskning eller för skanning av sårbarheter, och bör styra hanteringen av upptäckta säkerhetsrelaterade fel.

Testning bör utföras i en realistisk testmiljö för att säkerställa att systemet inte kommer att införa sårbarheter i organisationens miljö och att testerna är tillförlitliga.

14.3 Testdata

Mål: Att säkerställa skyddet av data som används för tester.

14.3.1 Skydd av testdata

Säkerhetsåtgärd

Testdata bör noggrant väljas ut, skyddas och styras.

Vägledning för införande

Verksamhetsinformation som innehåller personinformation eller annan konfidentiell information bör inte användas för teständamål. Om personinformation eller annars konfidentiell information används för testning bör alla känsliga detaljer och innehåll tas bort eller ändras (se ISO/IEC 29101[26]).

Följande riktlinjer bör tillämpas för att skydda verksamhetsinformation när den används för testning:

a) rutinerna för åtkomstkontroll som gäller för systemen i produktion bör också gälla för testsystemen;

b) det bör finnas separata tillstånd vid varje tillfälle då verksamhetsinformation kopieras till en testmiljö;

c) verksamhetsinformation bör raderas i testmiljön omedelbart efter genomförd testning;

d) kopiering och användning av verksamhetsinformation bör loggas för att ge en verifieringskedja.

Övrig information

System- och acceptanstest kräver oftast stora volymer av testdata som så nära som möjligt överensstämmer med produktionsdata.

15 Leverantörsrelationer

15.1 Informationssäkerhet i leverantörsrelationer

Mål: Att säkerställa skydd av de av organisationens tillgångar som leverantörer har åtkomst till.

15.1.1 Informationssäkerhetsregler för leverantörsrelationer

Säkerhetsåtgärd

Informationssäkerhetskrav för att reducera riskerna förknippade med leverantörers åtkomst till organisationens tillgångar bör avtalas med leverantören och dokumenteras.

Vägledning för införande

Alla organisationer bör identifiera och fastställa informationssäkerhetsåtgärder i ett regelverk för att specifikt hantera leverantörens åtkomst till organisationens information. Dessa säkerhetsåtgärder bör adressera processer och rutiner som bör implementeras av organisationen, samt de processer och rutiner som organisationen bör kräva att leverantören inför och tillämpar, däribland:

a) identifiera och dokumentera olika typer av leverantörer, t.ex. för IT-tjänster, logistik, affärssystem, IT-infrastruktur, till vilka organisationen ger åtkomst till information;

b) en standardiserad process och livscykel för hantering av leverantörsrelationer;

c) definiera de typer av åtkomst till information som olika typer av leverantörer kommer att bli godkända för, samt vilken övervakning och styrning av åtkomst som är relevant;

d) minimikrav för informationssäkerhet för varje typ av information och typ av åtkomst som bör ligga till grund för enskilda leverantörsavtal utifrån organisationens behov och krav, samt dess riskprofil;

e) processer och rutiner för att övervaka efterlevnad av definierade informationssäkerhetskrav för varje typ av leverantör och typ av tillgång, inklusive tredjepartsgranskning och produktvalidering;

f) säkerhetsåtgärder avseende noggrannhet och fullständighet, i syfte att säkerställa riktigheten för den information, eller den informationsbehandling, som tillhandahålls av endera parten;

g) de typer av skyldigheter som gäller för leverantörer i syfte att skydda organisationens information;

h) hantering av incidenter och oförutsedda avbrott som är förknippade med leverantörens tillgång, inklusive ansvarsförhållanden både för organisationen och för dess leverantörer;

i) motståndskraft och, om nödvändigt, förmåga till återhämtning och kontinuitetsaktiviteter för att säkerställa tillgängligheten till den information eller informationsbehandling tillhandahållen av endera parten;

j) utbildningsprogram för medvetenhet hos personal som medverkar vid upphandling och beställningar, när det gäller tillämpliga regler, processer och rutiner;

k) utbildningsprogram för medvetenhet för personal som samverkar med leverantörens personal. Det bör omfatta lämpliga regler för engagemang och uppförande baserat på typen av leverantör och den nivå på tillgång till organisationens system och information som leverantören har;

l) villkor under vilka informationssäkerhetskrav och säkerhetsåtgärder kommer att dokumenteras i ett avtal som undertecknats av båda parter;

m) hantering av nödvändiga överföringar av information, flytt av informationsbehandlingsresurser och övrigt som behöver flyttas, samt säkerställande av att informationssäkerheten upprätthålls under hela överföringsperioden.

Övrig information

Information kan äventyras av leverantörer med otillräcklig styrning av informationssäkerhet. Säkerhetsåtgärder bör identifieras och användas för att administrera leverantörens tillgång till informationsbehandlingstjänster. Om det t.ex. finns ett särskilt behov av konfidentialitet för informationen, kan avtal om tystnadsplikt användas. Ett annat exempel är risker relaterade till skydd av data när leverantörsavtalet innebär överföring av, eller tillgång till, information över nationella gränser. Organisationen måste vara medveten om att det lagstadgade eller avtalsenliga ansvaret för att skydda information kvarstår hos organisationen.

15.1.2 Hantering av säkerhet inom leverantörsavtal

Säkerhetsåtgärd

Alla relevanta informationssäkerhetskrav bör upprättas och avtalas med varje leverantör som kan tillgå, behandla, lagra, kommunicera eller som tillhandahåller infrastrukturkomponenter för organisationens information.

Vägledning för införande

Leverantörsavtal bör upprättas och dokumenteras för att säkerställa att det inte finns några missförstånd mellan organisationen och leverantören om båda parters skyldigheter att uppfylla relevanta informationssäkerhetskrav.

För att uppfylla informationssäkerhetskraven bör följande områden övervägas att ingå i avtalen:

a) beskrivning av informationen som kommer att tillgängliggöras och metoder för att erhålla eller få tillgång till informationen;

b) klassning av uppgifter enligt organisationens klassningssystem (se 8.2), om nödvändigt också mappning mellan organisationens klassningssystem och leverantörens klassningssystem;

c) rättsliga krav, inklusive skydd av personuppgifter, immateriell äganderätt och upphovsrätt och en beskrivning av hur det säkerställs att de uppfylls;

d) parternas avtalsenliga skyldighet att införa en överenskommen uppsättning säkerhetsåtgärder, inklusive åtkomstkontroll, resultatuppföljning, övervakning, rapportering och revision;

e) regler för tillåten användning av information, samt otillåten användning om nödvändigt;

f) förteckning över den personal hos leverantören som är behörig att komma åt eller ta emot organisationens information. Alternativt rutiner eller villkor för behörighet och borttagande av behörighet, avseende att få tillgång till eller ta emot organisationens information;

g) information om säkerhetsprinciper som är relevanta för det specifika avtalet;

h) krav och rutiner för incidenthantering (särskilt rapportering och samarbete under incidenthantering);

i) krav på utbildning och program för medvetenhet gällande särskilda rutiner och informationssäkerhetskrav, t ex. för incidenter och rutiner för godkännande;

j) relevanta regler för leverantörer inbegripet de säkerhetsåtgärder som måste införas;

k) relevanta avtalsparter, inklusive en kontaktperson för informationssäkerhetsfrågor;

l) eventuella krav på bakgrundskontroll av leverantörens personal bl.a. ansvar för att genomföra bakgrundkontroll och processer för meddelande om bakgrundskontroll inte har avslutats eller om resultaten ger anledning till tvivel eller osäkerhet;

m) rätt till att granska leverantörs processer och säkerhetsåtgärder utifrån avtalet;

n) processer för felhantering och hantering av oenigheter;

o) leverantörens skyldighet att regelbundet leverera en oberoende rapport om verkan av säkerhetsåtgärderna och avtal om snabb korrigering av relevanta frågor i rapporten;

p) leverantörens skyldigheter att uppfylla organisationens säkerhetskrav.

Övrig information

Avtalen kan variera avsevärt för olika organisationer och bland olika typer av leverantörer. Därför bör vikt läggas vid att alla relevanta uppgifter avseende säkerhetsrisker och krav inkluderas. Leverantörsavtal kan också omfatta andra parter (t.ex. underleverantörer).

Rutiner för fortsatt behandling i händelse av att leverantören inte kan leverera sina produkter eller tjänster måste beaktas i avtalet. Detta görs för att undvika förseningar på grund av anskaffande av ersättningsprodukter eller tjänster.

15.1.3 Försörjningskedja för informations- och kommunikationsteknologi

Säkerhetsåtgärd

Avtal med leverantörer bör innehålla krav på att hantera informationssäkerhetsriskerna förknippade med försörjningskedjan för tjänster och produkter baserade på informations- och kommunikationsteknologi.

Vägledning för införande

Följande ämnen bör övervägas att ingå i leverantörsavtal om försörjningskedjan:

a) som tillägg till de allmänna säkerhetskraven vid leverantörsrelationer bör organisationen definiera informationssäkerhetskrav gällande anskaffandet av informations- och kommunikationstekniksprodukt eller –tjänst;

b) för informations- och kommunikationsteknikstjänster, som kräver att leverantörer förmedlar organisationens krav på säkerhet i leveranskedjan om leverantörer anlitar underleverantörer för delar av informations- och kommunikationstekniktjänster, som tillhandahålls till organisationen;

c) för informations- och kommunikationsteknikprodukter, som kräver att leverantörer förmedlar lämpliga säkerhetsrutiner i leveranskedjan, om dessa produkter inkluderar komponenter som köps från andra leverantörer;

d) införa en övervakningsprocess och godtagbara metoder för att validera att informations- och kommunikationsteknikprodukter och -tjänster som levererats följer fastställda säkerhetskrav;

e) införa en process för att identifiera produkt- eller tjänstekomponenter som är kritiska för att upprätthålla funktionalitet och därför kräver ökad uppmärksamhet och granskning om de byggs utanför organisationen, särskilt om huvudleverantören outsourcar delar av produkten eller tjänsten till andra leverantörer;

f) att erhålla försäkran att kritiska komponenter och deras ursprung kan spåras i hela leverantörskedjan;

g) att erhålla försäkran att levererade informations- och kommunikationsteknikprodukter fungerar som förväntat utan några oväntade och oönskade funktioner;

h) definiera regler för utbyte av information om leveranskedjan och alla potentiella frågor och kompromisser mellan organisationen och leverantörer;

i) införa specifika processer för att hantera informations- och kommunikationsteknikkomponenters livscykel, tillgänglighet och tillhörande risker. Detta inkluderar att hantera riskerna för komponenter som inte längre är tillgängliga på grund av att leverantörer inte längre finns kvar eller att leverantörer inte längre tillhandahåller dessa komponenter på grund av tekniska framsteg.

Övrig information

De särskilda riskhanteringsmetoderna för försörjningskedjan för informations- och kommunikationsteknik bygger på allmän informationssäkerhet, kvalitet, projektledning och systemadministrativa metoder men ersätter dem inte.

Organisationer uppmanas att arbeta med att få leverantörer att förstå försörjningskedjan för informations- och kommunikationsteknik och alla frågor som har en viktig inverkan på de produkter och tjänster som tillhandahålls. Organisationer kan påverka informationssäkerhetspraxis i försörjningskedjan för informations- och kommunikationsteknik genom att göra klart i avtal med sina leverantörer de frågor som bör tas upp av andra leverantörer i försörjningskedjan.

Försörjningskedjan för informations- och kommunikationsteknik som behandlas här omfattar molntjänster.

15.2 Hantering av leverantörers tjänsteleverans

Mål: Att upprätthålla en överenskommen nivå av informationssäkerhet och tjänsteleverans i linje med leverantörsavtal.

15.2.1 Övervakning och granskning av leverantörstjänster

Säkerhetsåtgärd

Organisationer bör regelbundet övervaka, granska och revidera leverantörers tjänsteleverans.

Vägledning för införande

Övervakning och granskning av leverantörstjänster bör säkerställa att informationssäkerhetsvillkor och bestämmelser i avtalen följs och att informationssäkerhetsincidenter och problem hanteras korrekt.

Detta bör inbegripa en förvaltningstjänstsrelation mellan organisationen och leverantören för att:

a) övervaka tjänstenivån för att verifiera att avtalen följs;

b) granska tjänsterapporter producerade av leverantören och ordna regelbundna möten enligt avtal;

c) utföra granskningar av leverantörer, i samband med granskning av oberoende revisionsrapporter, om tillgängliga, och följa upp identifierade frågor;

d) ge information om säkerhetsincidenter och granska denna information som krävs enligt avtal och eventuella riktlinjer och rutiner;

e) granska leverantörers verifieringskedjor och loggar över informationssäkerhetshändelser, driftsproblem, misslyckanden, spårning av fel och störningar relaterade till tjänstelevereransen;

f) lösa och hantera identifierade problem;

g) granska informationssäkerhetsaspekter i leverantörens relationer med sina egna leverantörer;

h) säkerställa att leverantören håller tillräcklig tjänsteförmåga tillsammans med fungerande planer för att säkerställa att överenskomna kontinuitetstjänstenivåer bibehålls efter inträffade större fel på tjänster eller katastrof (se avsnitt 17).

Ansvaret för att hantera leverantörsrelationer bör tilldelas till en utsedd person eller en enhet för tjänstehantering. Organisationen bör dessutom se till att leverantörer tilldelar ansvar för att granska efterlevnaden och genomdriva kraven i avtalen. Tillräckliga tekniska kunskaper och resurser bör göras tillgängliga för att övervaka att kraven i avtalet, i synnerhet kraven på informationssäkerhet, är uppfyllda. Lämpliga åtgärder bör vidtas när brister i tjänsteleverans observeras.

Organisationen bör behålla tillräcklig övergripande kontroll och insyn i alla säkerhetsaspekter för känslig eller kritisk information eller databehandlingstjänster som nås, bearbetas eller förvaltas av en leverantör. Organisationen bör behålla insyn i säkerhetsaktiviteter som förändringsarbete, identifiering av sårbarheter samt incidentrapportering och incidenthantering via en definierad rapporteringsprocess.

15.2.2 Ändringshantering av leverantörers tjänster

Säkerhetsåtgärd

Ändringar av tillhandahållande av tjänster från leverantörer, inklusive underhåll och förbättring av befintlig informationssäkerhetspolicy med tillhörande regelverk och befintliga rutiner bör hanteras, med beaktande av informationens, systemens och processernas kritiska betydelse för verksamheten och riskerna ska omvärderas.

Vägledning för införande

Följande aspekter bör beaktas:

a) ändringar av leverantörsavtal;

b) ändringar som gjorts av organisationen för att genomföra:

   1) förbättringar av de nuvarande tjänsterna;

   2) utvecklingen av några nya tillämpningar och system;

   3) ändringar eller uppdateringar av organisationens regler och rutiner;

   4) nya eller ändrade säkerhetsåtgärder att lösa informationssäkerheten och förbättra säkerheten;

c) förändringar i leverantörens tjänster genom att genomföra:

   1) förändringar och förbättring av nätverk;

   2) användning av ny teknik;

   3) antagandet av nya produkter eller nyare versioner/utgåvor;

   4) nya utvecklingsverktyg och miljöer;

   5) ändringar avseende fysiska serviceanläggningar;

   6) ändring av leverantörer;

   7) förändring avseende underleverantörer.

16 Hantering av informationssäkerhetsincidenter

16.1 Hantering av informationssäkerhetsincidenter och förbättringar

Mål: Att säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation kring säkerhetshändelser och svagheter.

16.1.1 Ansvar och rutiner

Säkerhetsåtgärd

Ledningsansvar och rutiner bör fastställas för att säkerställa snabb, verkningsfull och korrekt hantering av informationssäkerhetsincidenter.

Vägledning för införande

Följande riktlinjer för ledningsansvar och rutiner för hantering av informationssäkerhetsincidenter bör övervägas:

a) ledningsansvar bör fastställas för att säkerställa att följande rutiner utarbetas och överlämnas på lämpligt sätt inom organisationen:

   1) rutiner för planering och förberedelser för hantering av incidenter;

2) rutiner för övervakning, upptäckt, analys och rapportering av informationssäkerhetshändelser och incidenter;

3) rutiner för loggning av aktiviteter som rör incidenthantering;

4) rutiner för hantering av kriminaltekniska bevis;

5) rutiner för bedömning av, och beslut om, informationssäkerhetshändelser och hantering av svagheter i informationssäkerheten;

6) rutiner för hantering inkluderande eskalering, styrd återställning efter inträffad incident, samt kommunikation till interna och externa personer eller organisationer;

b) rutiner bör säkerställa att:

1) kompetent personal hanterar frågor som rör informationssäkerhetsincidenter inom organisationen;

2) en kontaktpunkt för rapportering och identifiering av säkerhetsincidenter är etablerad;

3) lämpliga kontakter med myndigheter, externa intressegrupper eller forum som hanterar frågor som rör informationssäkerhetsincidenter upprätthålls;

c) rapporteringsrutiner bör omfatta:

1) förberedda formulär för rapportering av informationssäkerhetshändelser i syfte att underlätta rapportering och för att hjälpa personen som lämnar rapporten att komma ihåg alla nödvändiga åtgärder vid en informationssäkerhetshändelse;

2) rutiner som bör följas vid en informationssäkerhetshändelse, t.ex. att omedelbart notera alla detaljer, såsom om händelsen innebär bristande efterlevnad eller överträdelse av regler, uppkomna fel, meddelanden på skärmen, samt omedelbar rapportering till kontaktpunkten och endast genomföra koordinerade åtgärder;

3) hänvisning till existerande formell disciplinär process för att hantera anställda som begår överträdelser mot regelverket för säkerhet;

4) lämpliga återkopplingsprocesser för att säkerställa att de personer som rapporterar informationssäkerhetshändelser underrättas om resultaten efter att frågan har behandlats och avslutats.

Målen för incidenthantering bör överenskommas med verksamhetsansvariga och det bör säkerställas att ansvariga för incidenthanteringen förstår organisationens prioriteringar för hantering av informationssäkerheten.

Övrig information

Informationssäkerhetsincidenter kan överskrida nationella och organisatoriska gränser. För att hantera sådana incidenter finns det ett ökat behov av samordnad hantering och informationsdelning om dessa händelser med externa organisationer utifrån vad som är lämpligt.

Detaljerad vägledning avseende hantering av informationssäkerhetsincidenter ges i SS-ISO/IEC 27035[20].

16.1.2 Rapportering av informationssäkerhetshändelser

Säkerhetsåtgärd

Informationssäkerhetshändelser bör rapporteras genom lämpliga rapporteringsvägar så snabbt som möjligt.

Vägledning för införande

Alla anställda och leverantörer bör göras medvetna om sitt ansvar att rapportera informationssäkerhetshändelser så snabbt som möjligt. De bör också vara medvetna om rutiner för rapportering av säkerhetshändelser och om den kontaktpunkt som händelserna bör rapporteras till.

Informationssäkerhetshändelser som bör övervägas att rapporteras inkluderar:

a) säkerhetsåtgärder utan verkan;

b) avsteg från förväntningar på informationens riktighet, konfidentialitet och tillgänglighet;

c) mänskliga fel;

d) bristande efterlevnad av policy, regler eller riktlinjer;

e) överträdelser av fysiska skyddsåtgärder;

f) okontrollerade systemförändringar;

g) fel i program och hårdvara;

h) överträdelse av åtkomstregler.

Övrig information

Störningar eller andra onormala beteenden i system kan vara en indikator på ett angrepp eller faktiska säkerhetsbrister, och bör därför alltid rapporteras som en informationssäkerhetshändelse.

16.1.3 Rapportering av svagheter gällande informationssäkerhet

Säkerhetsåtgärd

Anställda och leverantörer som använder organisationens informationssystem och -tjänster bör vara skyldiga att notera och rapportera alla observerade eller misstänkta svagheter gällande informationssäkerhet i system eller tjänster.

Vägledning för införande

Alla anställda och leverantörer bör rapportera dessa svagheter till kontaktpunkten så snabbt som möjligt för att förhindra påverkan på informationssäkerheten. Formen för rapportering bör vara så enkel och tillgänglig som möjligt.

Övrig information

Anställda och leverantörer bör rådas att inte försöka påvisa förekomsten av misstänkta svagheter i säkerheten. Att testa svagheter kan tolkas som ett potentiellt missbruk av systemet och kan också skada informationssystem eller tjänster och resultera i juridiska följder för den enskilde som utför testning.

16.1.4 Bedömning av och beslut om informationssäkerhetshändelser

Säkerhetsåtgärd

Informationssäkerhetshändelser bör bedömas och beslut bör fattas om de klassificeras som informationssäkerhetsincidenter.

Vägledning för införande

Kontaktpunkten bör utvärdera varje informationssäkerhetshändelse med hjälp av en överenskommen skala för klassning av informationssäkerhetshändelser och incidenter. Den bör också besluta om huruvida händelsen bör klassas som en informationssäkerhetsincident. Klassning och prioritering av incidenter kan bidra till att tydliggöra konsekvenser och omfattning av incidenter.

Om organisationen har en grupp för hantering av informationssäkerhetsincidenter (Information Security Incident Response Team, ISIRT), kan bedömningar och beslut vidarebefordras till ISIRT för bekräftelse eller omprövning.

Resultaten av bedömningar och beslut bör dokumenteras detaljerat för framtida referens och verifiering.

16.1.5 Hantering av informationssäkerhetsincidenter

Säkerhetsåtgärd

Informationssäkerhetsincidenter bör hanteras i enlighet med dokumenterade rutiner.

Vägledning för införande

Informationssäkerhetsincidenter bör hanteras av en utsedd kontaktperson och andra relevanta personer inom organisationen eller externa parter (se 16.1.1).

Hanteringen bör inkludera följande:

a) insamling av bevis så snart som möjligt efter inträffande;

b) genomförande av en forensisk analys, om så krävs (se 16.1.7);

c) eskalering efter behov;

d) säkerställande av att alla aktiviteter loggas korrekt för senare analys;

e) kommunikation av informationssäkerhetsincidenten eller relevanta detaljer kopplade till incidenten till interna och externa personer eller organisationer som behöver informeras;

f) hantering av brister i informationssäkerheten som har konstaterats orsaka, eller bidragit till, händelsen;

g) när incidenten har hanterats tillfredställande bör ärendet formellt avslutas och dokumenteras.

Fördjupad analys efter incidenten bör, vid behov, genomföras för att identifiera orsaken till incidenten.

Övrig information

Det första målet med incidenthantering är att återgå till “normal säkerhetsnivå” och därefter inleda den nödvändiga återhämtningen.

16.1.6 Att lära av informationssäkerhetsincidenter

Säkerhetsåtgärd

Kunskaper baserade på analyser av hanterade informationssäkerhetsincidenter bör användas för att minska sannolikheten eller påverkan av framtida incidenter.

Vägledning för införande

Det bör finnas mekanismer som möjliggör kvantifiering och övervakning av typer, omfattning och kostnader avseende informationssäkerhetsincidenter. Informationen som erhålls från utvärderingen av informationssäkerhetsincidenter bör användas för att identifiera återkommande incidenter eller incidenter med stor påverkan.

Övrig information

Utvärderingen av informationssäkerhetsincidenter kan indikera behov av förbättrade, eller kompletterande, säkerhetsåtgärder för att begränsa frekvensen, skador och kostnader för framtida händelser. Utvärderingen kan komma att beaktas i granskningsprocessen av informationssäkerhetspolicyn och tillhörande regelverk (se 5.1.2).

Om hänsyn tas till konfidentialitetsaspekten, kan exempel från verkliga informationssäkerhetsincidenter användas i användarutbildning för medvetenhet (se 7.2.2) som exempel på vad som kan hända, hur hanteringen av sådana incidenter bör vara, och hur de kan undvikas i framtiden.

16.1.7 Insamling av bevis

Säkerhetsåtgärd

Organisationen bör fastställa och tillämpa rutiner för identifiering, insamling, kopiering och bevarande av information som kan tjäna som bevis.

Vägledning för införande

Interna rutiner bör utvecklas och följas för hantering av bevis i syfte att vidta disciplinära och rättsliga åtgärder.

Dessa rutiner för hantering av bevis bör inkludera processer för identifiering, insamling, anskaffande och bevarande av bevis associerade med olika typer av media, enheter och status för enheter, t.ex. om strömförsörjningen är av eller på.

Rutinerna bör ta hänsyn till:

a) spårbarhet;

b) säkerhet för bevis;

c) säkerheten för personalen;

d) roller och ansvar för involverad personal;

e) kompetensen hos personalen;

f) dokumenterad information;

g) delgivning.

I förekommande fall bör certifiering eller andra relevanta kvalifikationer för personal och hjälpmedel eftersträvas för att stärka värdet av de bevarade bevisen.

Kriminaltekniska bevis kan överskrida organisatoriska gränser eller gränser för gällande lagstiftning. I sådana fall bör det säkerställas att organisationen har rätt att samla in nödvändig information som brottsbevis. Kraven i olika jurisdiktioner bör också analyseras i syfte att maximera giltigheten över de relevanta jurisdiktionerna.

Övrig information

Identifiering är delprocessen för sökande efter, igenkänning och dokumentation av potentiella bevis. Insamling är den delprocess som syftar till att samla fysiska objekt som kan innehålla potentiella bevis. Kopiering är delprocessen att skapa en kopia av data för en definierad datamängd. Bevarande är delprocessen att bevara och skydda riktigheten av, och det ursprungliga skicket av, de potentiella bevisen.

När en informationssäkerhetshändelse upptäcks, är det inte alltid uppenbart om händelsen kommer att resultera i rättsliga åtgärder. Därför finns det en risk att nödvändiga bevis avsiktligt, eller oavsiktligt, förstörs innan allvarlighetsgraden i händelsen är helt klarlagd. Det är lämpligt att kontakta en jurist eller polisen tidigt vid planerade rättsliga åtgärder, och rådfråga dem avseende de bevis som krävs.

SS-ISO/IEC 27037[24] ger riktlinjer för identifiering, insamling, anskaffning och bevarande av digitala bevis.

17 Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet

17.1 Kontinuitet för informationssäkerhet

Mål: Kontinuiteten för informationssäkerhet bör vara integrerad i organisationens ledningssystem för kontinuitetshantering.

17.1.1 Planering av kontinuitet för informationssäkerhet

Säkerhetsåtgärd

Organisationen bör fastställa sina krav på informationssäkerhet och kontinuitet för styrning av informationssäkerhet vid svåra situationer, exempelvis under en kris eller katastrof.

Vägledning för införande

En organisation bör avgöra om kontinuiteten för informationssäkerhet hanteras inom verksamhetens kontinuitetsplanering eller inom processen för katastrofhantering. Informationssäkerhetskraven bör fastställas när man planerar för verksamhetens kontinuitet och för återhämtning från katastrofer.

Svensk ANM. I den svenska översättningen har ordet katastrofhantering använts för att täcka in de processer och/eller planer som verksamheten har för att kunna återställa delar av verksamheten t.ex. ett ICT-system.

Vid avsaknad av kontinuitetsplan för verksamheten och plan för katastrofhantering, bör ledningsfunktionen för informationssäkerhet utgå från att kraven på informationssäkerhet är desamma i svåra situationer som vid normala driftsituationer. Alternativt kan en organisation utföra en konsekvensanalys för att bestämma vilka informationssäkerhetskrav som gäller vid svåra situationer.

Övrig information

För att minska tiden och resursåtgången för en "extra" konsekvensanalys för informationssäkerhet, rekommenderas att informationssäkerhetsaspekter identifieras i analysen för verksamhetens kontinuitets- eller katastrofplanering. Detta innebär att kraven på kontinuitet för informationssäkerhet uttryckligen formuleras i verksamhetens kontinuitets- eller katastrofhantering.

Information om kontinuitetsplanering för verksamheter finns i ISO/IEC 27031[14], SS-ISO 22313[9] och SS-ISO 22301[8].

17.1.2 Införa kontinuitet för informationssäkerhet

Säkerhetsåtgärd

Organisationen bör fastställa, dokumentera, införa och upprätthålla processer, rutiner och säkerhetsåtgärder för att säkerställa den nivå av kontinuitet för informationssäkerhet som krävs vid en svår situation.

Vägledning för införande

En organisation bör säkerställa att:

a) en lämplig organisation finns på plats för att förbereda, mildra och ge respons på en störande händelse, med personal med nödvändig auktoritet, erfarenhet och kompetens;

b) det finns utsedd personal med nödvändigt ansvar, befogenheter och kompetens för att hantera en incident och upprätthålla informationssäkerheten;

c) planer och rutiner för hantering och återhämtning utarbetas, dokumenteras och godkänns, som beskriver hur organisationen kommer att hantera en störning. De bör också beskriva hur organisationen kommer att upprätthålla sin informationssäkerhet på en förutbestämd nivå, baserat på målen för informationssäkerhetens kontinuitet som har fastställts av ledningen (se 17.1.1).

Utifrån kraven på informationssäkerhetens kontinuitet, bör organisationen upprätta, dokumentera, tillämpa och upprätthålla:

a) informationssäkerhetsåtgärder inom verksamhetens kontinuitets- eller katastrofhantering, rutiner, stödjande system och verktyg;

b) förändringar i processer, rutiner och implementeringar för att upprätthålla befintliga informationssäkerhetsåtgärder vid en svår störning eller avbrott;

c) kompletterande säkerhetsåtgärder som ersättning för de informationssäkerhetsåtgärder som inte kan upprätthållas vid en svår störning eller avbrott.

Övrig information

Inom ramen för verksamhetens kontinuitets- och katastrofhantering kan särskilda processer och rutiner ha definierats. Information som hanteras inom dessa processer och rutiner, eller inom särskilda informationssystem som stödjer dem, bör skyddas. En organisation bör därför involvera informationssäkerhetsspecialister för att fastställa, genomföra och upprätthålla processer och rutiner för verksamhetens kontinuitet och katastrofhantering.

Informationssäkerhetsåtgärder som har införts bör fortsätta att fungera även under en störning. Om säkerhetsåtgärder inte kan upprätthålla skyddet av information, bör andra säkerhetsåtgärder fastställas, införas och upprätthållas för att nå en godtagbar nivå av informationssäkerhet.

17.1.3 Styra, granska och utvärdera kontinuitet för informationssäkerhet

Säkerhetsåtgärd

Organisationen bör verifiera de fastställda och införda säkerhetsåtgärderna för kontinuitet för informationssäkerhet med jämna mellanrum för att säkerställa att de är giltiga och verkningsfulla under störningar.

Vägledning för införande

Förändringar av organisationen, teknik, rutiner och processer, kan leda till förändrade krav på kontinuiteten för informationssäkerhet. Det gäller avseende såväl drift som kontinuitet. I dessa fall bör kontinuiteten avseende processer, rutiner och säkerhetsåtgärder för informationssäkerhet granskas mot dessa ändrade krav.

Organisationer bör verifiera kontinuiteten av deras informationssäkerhet genom att:

a) utöva och testa funktionerna hos processer, rutiner och säkerhetsåtgärder för informationssäkerhetens kontinuitet, i syfte att säkerställa att de överensstämmer med målen för informationssäkerhetens kontinuitet;

b) utöva och testa kunskapen och arbetssätt för att genomföra processer, rutiner och säkerhetsåtgärder för informationssäkerhetens kontinuitet, i syfte att säkerställa att de överensstämmer med målen för informationssäkerhetens kontinuitet;

c) granska giltighet och verkan i mätningen av kontinuiteten för informationssäkerhet vid ändring av informationssystem, processer, rutiner och säkerhetsåtgärder för informationssäkerhet eller processer och lösningar för kontinuitets- och katastrofhantering.

Övrig information

Verifiering av säkerhetsåtgärder för kontinuitet av informationssäkerhet skiljer sig från generella tester och verifiering av informationssäkerhet och bör utföras separerat från testning av ändringar. Om möjligt, bör verifiering av säkerhetsåtgärder för kontinuitet av informationssäkerhet genomföras i samband med organisationens tester av verksamhetens kontinuitets- eller katastrofhantering.

17.2 Redundans

Mål: Att säkerställa tillgänglighet till informationsbehandlingsresurser.

17.2.1 Tillgänglighet för informationsbehandlingsresurser

Säkerhetsåtgärd

Informationsbehandlingsresurser bör vid införande ha tillräcklig redundans för att uppfylla krav på tillgänglighet.

Vägledning för införande

Organisationer bör identifiera verksamhetskrav rörande tillgänglighet av informationssystem. Där tillgången inte kan garanteras med hjälp av den befintliga systemarkitekturen bör redundanta enheter eller redundant arkitektur övervägas.

I tillämpliga fall bör redundanta informationssystem testas för att säkerställa att övergången från en enhet till en annan fungerar som avsett.

Övrig information

Införandet av redundans kan medföra risker avseende riktighet och konfidentialitet för information och informationssystem. Detta bör beaktas vid utformningen av informationssystem.

18 Efterlevnad

18.1 Efterlevnad av juridiska och avtalsmässiga krav

Mål: Att undvika överträdelser av författningsenliga eller avtalsmässiga skyldigheter relaterade till informationssäkerhet och av eventuella säkerhetskrav.

18.1.1 Identifiering av gällande lagstiftning och avtalsmässiga krav

Säkerhetsåtgärd

Alla relevanta författningsenliga och avtalsmässiga krav samt organisationens tillvägagångssätt för att uppfylla dessa krav bör uttryckligen identifieras, dokumenteras och hållas uppdaterade för varje informationssystem och organisationen.

Vägledning för införande

De specifika säkerhetsåtgärder och individuella ansvar som behövs för att uppfylla dessa krav bör också fastställas och dokumenteras.

Högsta ledningen bör identifiera all lagstiftning som berör deras organisation i syfte att uppfylla kraven på deras typ av verksamhet. Om organisationen bedriver verksamhet i andra länder, bör högsta ledningen ta i beaktande att kraven för alla berörda länder uppfylls.

18.1.2 Immateriella rättigheter

Säkerhetsåtgärd

Lämpliga rutiner bör införas för att säkerställa efterlevnad av författningsenliga och avtalsmässiga krav relaterade till immateriella rättigheter och användning av proprietära programprodukter.

Vägledning för införande

Följande riktlinjer bör övervägas för att skydda material som kan betraktas som immateriella:

a) fastställa regler för efterlevnad av immateriella rättigheter som definierar den lagliga användningen av program- och informationsprodukter;

b) endast köpa program från kända och välrenommerade källor för att se till att upphovsrätten inte kränks;

c) upprätthålla medvetenheten om regler för att skydda immateriella rättigheter och markera sin avsikt att vidta disciplinära åtgärder mot personal som bryter mot dem;

d) upprätthålla lämpliga förteckningar över tillångar och identifiera alla tillgångar med krav att skydda immateriella rättigheter;

e) underhålla licensbevis, masterdiskar, manualer, etc.;

f) genomföra granskningar för att se till att maximala antalet användare inom licenser inte överskrids;

g) utföra granskningar för att se till att endast godkända program och licensierade produkter installeras;

h) tillhandahålla regler för att upprätthålla villkor i licenser;

i) tillhandahålla regler för avyttring eller överföring av program;

j) uppfylla villkoren för program och information som inhämtats från publika nätverk;

k) inte duplicera, konvertera till annat format eller extrahera från kommersiella inspelningar (film, ljud) annat än vad som är tillåtet enligt lagen om upphovsrätt;

l) inte kopiera, helt eller delvis, böcker, artiklar, rapporter eller andra handlingar, annat än vad som är tillåtet av upphovsrättslagen.

Övrig information

Immateriella rättigheter inkluderar upphovsrätt till program eller dokument, mönsterrätt, varumärken, patent och licenser för källkod.

Proprietära program levereras vanligtvis under ett licensavtal som anger licensvillkor och villkor, t.ex. begränsar användningen av produkterna till särskild hårdvara eller begränsar kopiering till endast skapande av säkerhetskopior. Betydelsen av och medvetenhet om immateriella rättigheter bör meddelas till personal för program utvecklade av organisationen.

Lagar och avtalskrav kan medföra restriktioner för kopiering av eget material. I synnerhet kan de kräva att endast material som är utvecklat av organisationen eller som är licensierat eller tillhandahålls av utvecklaren till organisationen, kan användas. Upphovsrättsintrång kan leda till rättsliga åtgärder, som kan medföra böter och brottmål.

18.1.3 Skydd av dokumenterad information

Säkerhetsåtgärd

Dokumenterad information bör skyddas från förlust, förstörelse, förfalskning, obehörig åtkomst och otillåten utgivning i enlighet med författningsenliga, avtalsmässiga och verksamhetsmässiga krav.

Vägledning för införande

Vid val av skydd för dokumenterad information, bör klassificeringen av informationen, i enlighet med organisationens klassningssystem, tas i beaktande. Dokumenterad information bör indelas olika typer, t.ex. redovisning, databaser, transaktionsloggar, granskningsloggar och operativa rutiner, med krav på lagringstid och godkänd lagringsmedia, t.ex. papper, mikrofilm, magnetiska och optiska. Alla kryptografiska nycklar och program som har en koppling till krypterade arkiv eller digitala signaturer (se avsnitt 10), bör också lagras för dekryptering av dokumenterad information, lika länge som dokumenterad information avses bevaras.

Hänsyn bör tas till att media som används för lagring av dokumenterad information kan försämras över tid. Lagring och hantering bör genomföras i enlighet med tillverkarens rekommendationer.

När elektroniska lagringsmedia är valt bör rutiner för att säkerställa förmågan till åtkomst till data (läsbarhet av media och format) fastställas för att skydda mot förlust på grund av förändring av framtida teknik.

Datalagringssystem bör väljas så att nödvändiga data kan hämtas inom en acceptabel tidsram och i ett acceptabelt format, beroende på vilka krav som bör uppfyllas.

Systemet för lagring och hantering av dokumenterad information bör säkerställa identifiering av poster och lagringstiden som definieras av nationella eller regionala författningar, om tillämpligt. Detta system bör även medge gallring av dokumenterad information som inte längre behöver lagras av organisationen.

För att möta dessa mål för skydd av dokumenterad information, bör följande steg tas inom en organisation:

a) riktlinjer bör utfärdas för lagring, arkivering, hantering och gallring av dokumenterad information;

b) en bevarande plan bör upprättas för att identifiera dokumenterad information och hur länge den behöver sparas;

c) en inventering av viktiga informationskällor bör upprätthållas.

Övrig information

Viss dokumentation kan behöva sparas på ett säkert sätt för att möta författningsenliga och avtalsmässiga krav samt att stödja viktig verksamhet. Exempel inkluderar dokumentation som kan krävas som bevis för att en organisation författningar och regler i övrigt i syfte att säkerställa skydd mot eventuella civilrättsliga eller straffrättsliga åtgärder eller för att bekräfta den finansiella statusen i en organisation till aktieägare, externa parter och revisorer. Nationella författningar kan ange tidramar och innehåll för lagring av dokumenterad information.

Ytterligare information om hantering av dokumenterad information kan hittas i SS-ISO 15489-1[5].

18.1.4 Skydd av personlig integritet och personuppgifter

Säkerhetsåtgärd

I förekommande fall bör skydd av personlig integritet och personuppgifter säkerställas i enlighet med gällande författningar.

Vägledning för införande

Organisationens bör utveckla och införa regler för skydd av personuppgifter. Dessa regler bör kommuniceras till alla personer som hanterar personuppgifter.

Efterlevnad av dessa regler och författningsenliga krav om skydd av privatlivet och skydd av personuppgifter kräver särskild organisation och vägledning. Ofta uppnås detta bäst genom utnämningen av en person som är ansvarig, t.ex. ett personuppgiftsombud, som ger vägledning till verksamhetsansvariga, användare och tjänsteleverantörer rörande vars och ens ansvar och de särskilda rutiner som bör följas. Ansvar för hantering av personuppgifter och medvetenhet om personlig integritet bör behandlas i enlighet med gällande författningar. Lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter bör införas.

Övrig information

ISO/IEC 29100[25] beskriver ett ramverk för hantering av personuppgifter i informations- och IT-system. Ett antal länder har infört lagkrav avseende säkerhetsåtgärder vid insamling, bearbetning och överföring av personuppgifter (information som på något sätt kan associeras med en person). Beroende på den respektive nationella lagstiftningen, kan sådana säkerhetsåtgärder medföra ansvar avseende insamling, behandling och spridning av personuppgifter, och kan också begränsa möjligheten att överföra personuppgifter till andra länder.

18.1.5 Reglering av kryptografiska säkerhetsåtgärder

Säkerhetsåtgärd

Kryptografiska säkerhetsåtgärder bör användas i enlighet med alla gällande avtal och författningar.

Vägledning för införande

Följande bör övervägas för överensstämmelse med relevanta avtal och författningar:

a) restriktioner för import eller export av hårdvara och program med kryptografiska funktioner;

b) restriktioner för import eller export av maskinvara och program som är utformad att lägga till kryptografiska funktioner;

c) restriktioner för användning av kryptering;

d) obligatoriska eller icke begränsande åtkomstmetoder för ländernas myndigheter till information som krypteras av hårdvara eller program för bevarande av innehållets konfidentialitet.

För att säkerställa efterlevnad av relevant lagstiftning bör juridisk kompetens inhämtas. Innan krypterad information eller kryptografiska säkerhetsåtgärder flyttas över gränser för gällande lagstiftning, bör juridisk rådgivning också inhämtas.

18.2 Granskningar av informationssäkerhet

Mål: Att säkerställa att informationssäkerhet införs och drivs i enlighet med organisationens regler och rutiner.

18.2.1 Oberoende granskning av informationssäkerhet

Säkerhetsåtgärd

Organisationens tillvägagångssätt för att hantera informationssäkerhet och dess införande (d.v.s. mål, säkerhetsåtgärder, regler, processer och rutiner för informationssäkerhet) bör med jämna mellanrum eller när betydande förändringar sker genomgå oberoende granskning.

Vägledning för införande

Högsta ledningen bör inleda den oberoende granskningen. En sådan oberoende granskning är nödvändig för att säkerställa att organisationen är fortsatt lämplig, tillräcklig och verkningsfull i sin hantering av informationssäkerhet. Granskningen bör omfatta bedömning av möjligheter till förbättringar och förändringar av informationssäkerheten, inklusive krav och målbild för informationssäkerheten.

En sådan granskning bör utföras av personer som är oberoende i förhållande till verksamheten som avses att granskas, t.ex. internrevision, en oberoende ledningsfunktion eller en extern part som specialiserat sig på sådana granskningar. Individer som utför dessa granskningar bör ha lämplig kompetens och erfarenhet.

Resultatet av den oberoende granskningen bör dokumenteras och rapporteras till beställaren av granskningen. Dokumentation om genomförd granskning bör bibehållas.

Om den oberoende granskningen identifierar att organisationens strategi och genomförande för att hantera informationssäkerhet är otillräcklig, t.ex. att dokumenterade mål och krav inte uppfylls eller inte är förenliga med inriktningen för informationssäkerhet såsom den är uttryckt i informationssäkerhetspolicyn (se 5.1.1), bör högsta ledningen överväga korrigerande åtgärder.

Övrig information

ISO/IEC 27007[12], "Guidelines for information security management systems auditing" och SIS-ISO/IEC TR 27008[13], "Vägledning för revisorer om informationssäkerhetsåtgärder" ger också vägledning för genomförandet av den oberoende granskningen.

18.2.2 Efterlevnad av säkerhetspolicy, regler och standarder

Säkerhetsåtgärd

Högsta ledningen bör inom gällande ansvarsområden regelbundet granska efterlevnaden av informationssäkerhetspolicyn, gällande regler och riktlinjer, standarder och eventuella andra säkerhetskrav i förhållande till informationsbearbetning och rutiner.

Vägledning för införande

Verksamhetsansvariga bör identifiera hur gransking av informationssäkerhetskrav i regler, avtal, standarder och andra tillämpliga bestämmelser uppfylls. Verktyg för automatisk mätning och rapportering bör övervägas för verkningsfull regelbunden granskning.

Om någon överträdelse upptäcks i granskningen bör verksamhetsansvariga:

a) identifiera orsakerna till bristande efterlevnad;

b) utvärdera behovet av åtgärder för att uppnå efterlevnad;

c) genomföra lämpliga korrigerande åtgärder;

d) granska korrigerande åtgärder för att säkerställa dess verkan och identifiera eventuella brister eller svagheter.

Resultaten av granskningar och korrigerande åtgärder utförda av verksamhetsansvariga bör dokumenteras och sparas. Verksamhetsansvariga bör rapportera resultaten till de personer som utför oberoende granskningar (se 18.2.1) då en oberoende granskning sker inom deras ansvarsområde.

Övrig information

Operativ övervakning av systemet är täckt av 12.4.

18.2.3 Granskning av teknisk efterlevnad

Säkerhetsåtgärd

Informationssystem bör granskas regelbundet avseende efterlevnad av organisationens informationssäkerhetspolicy, regler, riktlinjer och standarder.

Vägledning för införande

Teknisk överensstämmelse bör helst granskas med hjälp av automatiserade verktyg som genererar tekniska rapporter för efterföljande tolkning av en teknisk specialist. Alternativt så kan manuella granskningar (stödda av lämpliga program, om nödvändigt) genomföras av en erfaren systemerare.

Om penetrationstester eller sårbarhetsgranskningar används bör försiktighet iakttas eftersom sådan aktivitet kan leda till att säkerheten i systemet hotas. Sådana tester bör vara planerade, dokumenterade och repeterbara.

Granskning av teknisk efterlevnad bör endast utföras av behöriga, auktoriserade personer eller under tillsyn av sådana personer.

Övrig information

Granskningar av teknisk efterlevnad innebär granskning av fungerande system för att säkerställa att skyddsåtgärder för maskinvara och program har införts korrekt. Denna typ av granskning av teknisk efterlevnad kräver teknisk specialistkompetens.

Granskningar av teknisk efterlevnad omfattar också, t.ex. penetrationstester och sårbarhetsgranskningar, som kan utföras av oberoende experter som har anlitats särskilt för detta ändamål. Detta kan vara användbart för att upptäcka sårbarheter i system och för kontroll av hur verkningsfulla säkerhetsåtgärderna är att förhindra obehörig åtkomst på grund av dessa sårbarheter.

Penetrationstester och sårbarhetsgranskningar ger en ögonblicksbild av ett system i ett särskilt tillstånd vid en viss tidpunkt. Ögonblicksbilden är begränsad till de delar av systemet som faktiskt testats. Penetrationstester och sårbarhetsbedömningar är inte en ersättning för riskbedömning.

SIS-ISO/IEC TR 27008[13] ger viss vägledning när det gäller revision av teknisk efterlevnad.

Litteraturförteckning

[1] ISO/IEC-direktiven, del 2

[2] ISO/IEC 11770-1, *Information technology — Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[4] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[5] SS-ISO 15489-1, *Dokumentation — Dokumenthantering (Records Management) — Del 1: Allmänt*

[6] SS-ISO/IEC 20000-1, *Informationsteknik — Ledningssystem för tjänster — Del 1: Krav*

[7] SS-ISO/IEC 20000-2, *Informationsteknik — Ledningssystem för tjänster — Del 2: Vägledning*

[8] SS-ISO 22301, *Samhällssäkerhet — Ledningssystem för kontinuitet — Krav*

[9] SS-ISO 22313, *Samhällssäkerhet — Ledningssystem för kontinuitet — Riktlinjer*

[10] ISO/IEC 27001, I*nformation technology — Security techniques — Information security management systems — Requirements*

[11] SS-ISO/IEC 27005, *Informationsteknik — Säkerhetstekniker — Riskhantering för informationssäkerhet*

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

[13] SIS-ISO/IEC TR 27008, *Informationsteknik — Säkerhetstekniker — Vägledning om säkerhetsåtgärder för revisorer*

[14] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[15] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[16] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[17] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[18] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[19] ISO/IEC 27033-5, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)*

[20] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[21] ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

[22] ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements*

[23] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security*

[24] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[27] SS-ISO 31000, *Riskhantering — Principer och riktlinjer*

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

This second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structurally revised.

0 Introduction

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

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

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

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

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

0.3 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.[11]

0.4 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

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

1 Scope

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

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

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

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

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

4 Structure of this standard

This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

4.1 Clauses

Each clause defining security controls contains one or more main security categories.

The order of the clauses in this standard does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organization applying this standard should identify applicable controls, how important these are and their application to individual business processes. Furthermore, lists in this standard are not in priority order.

4.2 Control categories

Each main security control category contains:

a) a control objective stating what is to be achieved;

b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control

Defines the specific control statement, to satisfy the control objective.

Implementation guidance

Provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements. .

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

c) processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of such policy topics include:

a) access control (see Clause 9);

b) information classification (and handling) (see 8.2);

c) physical and environmental security (see Clause 11);

d) end user oriented topics such as:

   1) acceptable use of assets (see 8.1.3);

   2) clear desk and clear screen (see 11.2.9);

   3) information transfer (see 13.2.1);

   4) mobile devices and teleworking (see 6.2);

   5) restrictions on software installations and use (see 12.6.2);

e) backup (see 12.3);

f) information transfer (see 13.2);

g) protection from malware (see 12.2);

h) management of technical vulnerabilities (see 12.6.1);

i) cryptographic controls (see Clause 10);

j) communications security (see Clause 13);

k) privacy and protection of personally identifiable information (see 18.1.4);

l) supplier relationships (see Clause 15).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme" (see 7.2.2).

Other information

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single "information security policy" document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information.

Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

The review of policies for information security should take the results of management reviews into account.

Management approval for a revised policy should be obtained.

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

Implementation guidance

Allocation of information security responsibilities should be done in accordance with the information security policies (see 5.1.1). Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined. These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes should be defined.

Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless they remain accountable and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be stated. In particular the following should take place:

a) the assets and information security processes should be identified and defined;

b) the entity responsible for each asset or information security process should be assigned and the details of this responsibility should be documented (see 8.1.2);

c) authorization levels should be defined and documented;

d) to be able to fulfil responsibilities in the information security area the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments;

e) coordination and oversight of information security aspects of supplier relationships should be identified and documented.

Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

Other information

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Implementation guidance

Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may have been broken).

Other information

Organizations under attack from the Internet may need authorities to take action against the attack source.

Maintaining such contacts may be a requirement to support information security incident management (see Clause 16) or the business continuity and contingency planning process (see Clause 17). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).

6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

Implementation guidance

Membership in special interest groups or forums should be considered as a means to:

a) improve knowledge about best practices and stay up to date with relevant security information;

b) ensure the understanding of the information security environment is current and complete;

c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;

d) gain access to specialist information security advice;

e) share and exchange information about new technologies, products, threats or vulnerabilities;

f) provide suitable liaison points when dealing with information security incidents (see Clause 16).

Other information

Information sharing agreements can be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of confidential information.

6.1.5 Information security in project management

Control

Information security should be addressed in project management, regardless of the type of the project.

Implementation guidance

Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes. The project management methods in use should require that:

a) information security objectives are included in project objectives;

b) an information security risk assessment is conducted at an early stage of the project to identify necessary controls;

c) information security is part of all phases of the applied project methodology.

Information security implications should be addressed and reviewed regularly in all projects. Responsibilities for information security should be defined and allocated to specified roles defined in the project management methods.

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Implementation guidance

When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

The mobile device policy should consider:

a) registration of mobile devices;

b) requirements for physical protection;

c) restriction of software installation;

d) requirements for mobile device software versions and for applying patches;

e) restriction of connection to information services;

f) access controls;

g) cryptographic techniques;

h) malware protection;

i) remote disabling, erasure or lockout;

j) backups;

k) usage of web services and web apps.

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques (see Clause 10) and enforcing use of secret authentication information (see 9.2.4).

Mobile devices should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of mobile devices. Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

Training should be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented.

Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

a) separation of private and business use of the devices, including using software to support such separation and protect business data on a private device;

b) providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.

Other information

Mobile device wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are:

a) some wireless security protocols are immature and have known weaknesses;

b) information stored on mobile devices may not be backed-up because of limited network bandwidth or because mobile devices may not be connected at the times when backups are scheduled.

Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organization's premises.

6.2.2 Teleworking

Control

A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

Implementation guidance

Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed physical teleworking environment;

c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system;

d) the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;

e) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;

f) the use of home networks and requirements or restrictions on the configuration of wireless network services;

g) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

h) access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;

i) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users;

j) malware protection and firewall requirements.

The guidelines and arrangements to be considered should include:

a) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed;

b) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;

c) the provision of suitable communication equipment, including methods for securing remote access;

d) physical security;

e) rules and guidance on family and visitor access to equipment and information;

f) the provision of hardware and software support and maintenance;

g) the provision of insurance;

h) the procedures for backup and business continuity;

i) audit and security monitoring;

j) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

Other information

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as "telecommuting", "flexible workplace", "remote work" and "virtual work" environments.

7 Human resource security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Control

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Implementation guidance

Verification should take into account all relevant privacy, protection of personally identifiable information and employment based legislation, and should, where permitted, include the following:

a) availability of satisfactory character references, e.g. one business and one personal;

b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;

c) confirmation of claimed academic and professional qualifications;

d) independent identity verification (passport or similar document);

e) more detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, organizations should make sure the candidate:

a) has the necessary competence to perform the security role;

b) can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and, in particular, if these are handling confidential information, e.g. financial information or highly confidential information, the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process should also be ensured for contractors. In these cases, the agreement between the organization and the contractor should specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organization should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

7.1.2 Terms and conditions of employment

Control

The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

Implementation guidance

The contractual obligations for employees or contractors should reflect the organization's policies for information security in addition to clarifying and stating:

a) that all employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities (see 13.2.4);

b) the employee's or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (see 18.1.2 and 18.1.4);

c) responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handled by the employee or contractor (see Clause 8);

d) responsibilities of the employee or contractor for the handling of information received from other companies or external parties;

e) actions to be taken if the employee or contractor disregards the organization's security requirements (see 7.2.3).

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The organization should ensure that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see 7.3).

Other information

A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. An external party, with which a contractor is associated, can be required to enter into contractual arrangements on behalf of the contracted individual.

7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1 Management responsibilities

Control

Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

Implementation guidance

Management responsibilities should include ensuring that employees and contractors:

a) are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems;

b) are provided with guidelines to state information security expectations of their role within the organization;

c) are motivated to fulfil the information security policies of the organization;

d) achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see 7.2.2);

e) conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working;

f) continue to have the appropriate skills and qualifications and are educated on a regular basis;

g) are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

Management should demonstrate support of information security policies, procedures and controls, and act as a role model.

Other information

If employees and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organization. For example, poor management can lead to information security being neglected or potential misuse of the organization's assets.

7.2.2 Information security awareness, education and training

Control

All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation guidance

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

An information security awareness programme should be established in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

The awareness programme should be planned taking into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. The awareness programme should also be updated regularly so it stays in line with organizational policies and procedures, and should be built on lessons learnt from information security incidents.

Awareness training should be performed as required by the organization's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others.

Information security education and training should also cover general aspects such as:

a) stating management's commitment to information security throughout the organization;

b) the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements;

c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and external parties;

d) basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks);

e) contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

Information security education and training should take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

The organization should develop the education and training programme in order to conduct the education and training effectively. The programme should be in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The programme should consider different forms of education and training, e.g. lectures or self-studies.

Other information

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why'. It is important that employees understand the aim of information security and the potential impact, positive and negative, on the organization of their own behaviour.

Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills.

An assessment of the employees' understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.

7.2.3 Disciplinary process

Control

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

Implementation guidance

The disciplinary process should not be commenced without prior verification that an information security breach has occurred (see 16.1.7).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of information security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

The disciplinary process should also be used as a deterrent to prevent employees from violating the organization's information security policies and procedures and any other information security breaches. Deliberate breaches may require immediate actions.

Other information

The disciplinary process can also become a motivation or an incentive if positive sanctions are defined for remarkable behaviour with regards to information security.

7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

7.3.1 Termination or change of employment responsibilities

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

Implementation guidance

The communication of termination responsibilities should include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement (see 13.2.4) and the terms and conditions of employment (see 7.1.2) continuing for a defined period after the end of the employee's or contractor's employment.

Responsibilities and duties still valid after termination of employment should be contained in the employee's or contractor's terms and conditions of employment (see 7.1.2).

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Other information

The human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the information security aspects of the relevant procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

It may be necessary to inform employees, customers or contractors of changes to personnel and operating arrangements.

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

Control

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

Implementation guidance

An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.

The asset inventory should be accurate, up to date, consistent and aligned with other inventories.

For each of the identified assets, ownership of the asset should be assigned (see 8.1.2) and the classification should be identified (see 8.2).

Other information

Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

ISO/IEC 27005[11] provides examples of assets that might need to be considered by the organization when identifying assets. The process of compiling an inventory of assets is an important prerequisite of risk management (see also ISO/IEC 27000 and ISO/IEC 27005[11]).

8.1.2 Ownership of assets

Control

Assets maintained in the inventory should be owned.

Implementation guidance

Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.

A process to ensure timely assignment of asset ownership is usually implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle.

The asset owner should:

a) ensure that assets are inventoried;

b) ensure that assets are appropriately classified and protected;

c) define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;

d) ensure proper handling when the asset is deleted or destroyed.

Other information

The identified owner can be either an individual or an entity who has approved management responsibility for controlling the whole lifecycle of an asset. The identified owner does not necessarily have any property rights to the asset.

Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the owner.

In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.

8.1.3 Acceptable use of assets

Control

Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.

Implementation guidance

Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

8.1.4 Return of assets

Control

All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

Implementation guidance

The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see 11.2.7).

In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period of termination, the organization should control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification of information

Control

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

Implementation guidance

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Assets other than information can also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information assets should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. The level of protection in the scheme should be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered. The scheme should be aligned to the access control policy (see 9.1.1).

Each level should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organization so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.

Classification should be included in the organization's processes, and be consistent and coherent across the organization. Results of classification should indicate value of assets depending on their sensitivity and criticality to the organization, e.g. in terms of confidentiality, integrity and availability. Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their life-cycle.

Other information

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or on the contrary under-classification can endanger the achievement of business objectives.

An example of an information confidentiality classification scheme could be based on four levels as follows:

a) disclosure causes no harm;

b) disclosure causes minor embarrassment or minor operational inconvenience;

c) disclosure has a significant short term impact on operations or tactical objectives;

d) disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

8.2.2 Labelling of information

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

"Implementation guidance"

Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established in 8.2.1. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information to reduce workloads. Employees and contractors should be made aware of labelling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information

Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and metadata are a common form of labelling.

Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.

8.2.3 Handling of assets

Control

Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Implementation guidance

Procedures should be drawn up for handling, processing, storing and communicating information consistent with its classification (see 8.2.1).

The following items should be considered:

a) access restrictions supporting the protection requirements for each level of classification;

b) maintenance of a formal record of the authorized recipients of assets;

c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;

d) storage of IT assets in accordance with manufacturers' specifications;

e) clear marking of all copies of media for the attention of the authorized recipient.

The classification scheme used within the organization may not be equivalent to the schemes used by other organizations, even if the names for levels are similar; in addition, information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical.

Agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organizations.

8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

Control

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Implementation guidance

The following guidelines for the management of removable media should be considered:

a) if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable;

b) where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail;

c) all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;

d) if data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media;

e) to mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable;

f) multiple copies of valuable data should be stored on separate media to further reduce the risk of coincidental data damage or loss;

g) registration of removable media should be considered to limit the opportunity for data loss;

h) removable media drives should only be enabled if there is a business reason for doing so;

i) where there is a need to use removable media the transfer of information to such media should be monitored.

Procedures and authorization levels should be documented.

8.3.2 Disposal of media

Control

Media should be disposed of securely when no longer required, using formal procedures.

Implementation guidance

Formal procedures for the secure disposal of media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure disposal of media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

a) media containing confidential information should be stored and disposed of securely, e.g. by incineration or shredding, or erasure of data for use by another application within the organization;

b) procedures should be in place to identify the items that might require secure disposal;

c) it may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items;

d) many organizations offer collection and disposal services for media; care should be taken in selecting a suitable external party with adequate controls and experience;

e) disposal of sensitive items should be logged in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

Other information

Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded (see 11.2.7).

8.3.3 Physical media transfer

Control

Media containing information should be protected against unauthorized access, misuse or corruption during transportation.

Implementation guidance

The following guidelines should be considered to protect media containing information being transported:

a) reliable transport or couriers should be used;

b) a list of authorized couriers should be agreed with management;

c) procedures to verify the identification of couriers should be developed;

d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;

e) logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

Other information

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. In this control, media include paper documents.

When confidential information on media is not encrypted, additional physical protection of the media should be considered.

9 Access control

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

Control

An access control policy should be established, documented and reviewed based on business and information security requirements.

Implementation guidance

Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

Access controls are both logical and physical (see Clause 11) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

a) security requirements of business applications;

b) policies for information dissemination and authorization, e.g. the need-to-know principle and information security levels and classification of information (see 8.2);

c) consistency between the access rights and information classification policies of systems and networks;

d) relevant legislation and any contractual obligations regarding limitation of access to data or services (see 18.1);

e) management of access rights in a distributed and networked environment which recognizes all types of connections available;

f) segregation of access control roles, e.g. access request, access authorization, access administration;

g) requirements for formal authorization of access requests (see 9.2.1 and 9.2.2);

h) requirements for periodic review of access rights (see 9.2.5);

i) removal of access rights (see 9.2.6);

j) archiving of records of all significant events concerning the use and management of user identities and secret authentication information;

k) roles with privileged access (see 9.2.3).

Other information

Care should be taken when specifying access control rules to consider:

a) establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";

b) changes in information labels (see 8.2.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;

d) rules which require specific approval before enactment and those which do not.

Access control rules should be supported by formal procedures (see 9.2, 9.3, 9.4) and defined responsibilities (see 6.1.1, 9.3).

Role based access control is an approach used successfully by many organisations to link access rights with business roles.

Two of the frequent principles directing the access control policy are:

a) Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile);

b) Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

9.1.2 Access to networks and network services

Control

Users should only be provided with access to the network and network services that they have been specifically authorized to use.

Implementation guidance

A policy should be formulated concerning the use of networks and network services. This policy should cover:

a) the networks and network services which are allowed to be accessed;

b) authorization procedures for determining who is allowed to access which networks and networked services;

c) management controls and procedures to protect access to network connections and network services;

d) the means used to access networks and network services (e.g. use of VPN or wireless network);

e) user authentication requirements for accessing various network services;

f) monitoring of the use of network services.

The policy on the use of network services should be consistent with the organization's access control policy (see 9.1.1).

Other information

Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's information security management and control.

9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

9.2.1 User registration and de-registration

Control

A formal user registration and de-registration process should be implemented to enable assignment of access rights.

Implementation guidance

The process for managing user IDs should include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;

b) immediately disabling or removing user IDs of users who have left the organization (see 9.2.6);

c) periodically identifying and removing or disabling redundant user IDs;

d) ensuring that redundant user IDs are not issued to other users.

Other information

Providing or revoking access to information or information processing facilities is usually a two-step procedure:

a) assigning and enabling, or revoking, a user ID;

b) providing, or revoking, access rights to such user ID (see 9.2.2).

9.2.2 User access provisioning

Control

A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

Implementation guidance

The provisioning process for assigning or revoking access rights granted to user IDs should include:

a) obtaining authorization from the owner of the information system or service for the use of the information system or service (see control 8.1.2); separate approval for access rights from management may also be appropriate;

b) verifying that the level of access granted is appropriate to the access policies (see 9.1) and is consistent with other requirements such as segregation of duties (see 6.1.2);

c) ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed;

d) maintaining a central record of access rights granted to a user ID to access information systems and services;

e) adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization;

f) periodically reviewing access rights with owners of the information systems or services (see 9.2.5).

Other information

Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews (see 9.2.4) are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or contractors (see 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 Management of privileged access rights

Control

The allocation and use of privileged access rights should be restricted and controlled.

Implementation guidance

The allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access control policy (see control 9.1.1). The following steps should be considered:

a) the privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom they need to be allocated should be identified;

b) privileged access rights should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (see 9.1.1), i.e. based on the minimum requirement for their functional roles;

c) an authorization process and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorization process is complete;

d) requirements for expiry of privileged access rights should be defined;

e) privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID;

f) the competences of users with privileged access rights should be reviewed regularly in order to verify if they are in line with their duties;

g) specific procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities;

h) for generic administration user IDs, the confidentiality of secret authentication information should be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

Other information

Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

9.2.4 Management of secret authentication information of users

Control

The allocation of secret authentication information should be controlled through a formal management process.

Implementation guidance

The process should include the following requirements:

a) users should be required to sign a statement to keep personal secret authentication information confidential and to keep group (i.e. shared) secret authentication information solely within the members of the group; this signed statement may be included in the terms and conditions of employment (see 7.1.2);

b) when users are required to maintain their own secret authentication information they should be provided initially with secure temporary secret authentication information`, which they are forced to change on first use;

c) procedures should be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information;

d) temporary secret authentication information should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided;

e) temporary secret authentication information should be unique to an individual and should not be guessable;

f) users should acknowledge receipt of secret authentication information;

g) default vendor secret authentication information should be altered following installation of systems or software.

Other information

Passwords are a commonly used type of secret authentication information and are a common means of verifying a user's identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes.

9.2.5 Review of user access rights

Control

Asset owners should review users' access rights at regular intervals.

Implementation guidance

The review of access rights should consider the following:

a) users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment (see Clause 7);

b) user access rights should be reviewed and re-allocated when moving from one role to another within the same organization;

c) authorizations for privileged access rights should be reviewed at more frequent intervals;

d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

e) changes to privileged accounts should be logged for periodic review.

Other information

This control compensates for possible weaknesses in the execution of controls 9.2.1, 9.2.2 and 9.2.6.

9.2.6 Removal or adjustment of access rights

Control

The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Implementation guidance

Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended. This will determine whether it is necessary to remove access rights. Changes of employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.

Access rights for information and assets associated with information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a) whether the termination or change is initiated by the employee, the external party user or by management, and the reason for termination;

b) the current responsibilities of the employee, external party user or any other user;

c) the value of the assets currently accessible.

Other information

In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees and external party users involved to no longer share this information with the person departing.

In cases of management-initiated termination, disgruntled employees or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they may be tempted to collect information for future use.

9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

9.3.1 Use of secret authentication information

Control

Users should be required to follow the organization's practices in the use of secret authentication information.

Implementation guidance

All users should be advised to:

a) keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority;

b) avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. password vault);

c) change secret authentication information whenever there is any indication of its possible compromise;

d) when passwords are used as secret authentication information, select quality passwords with sufficient minimum length which are:

   1) easy to remember;

   2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.;

   3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);

   4) free of consecutive identical, all-numeric or all-alphabetic characters;

   5) if temporary, changed at the first log-on;

e) not share individual user's secret authentication information;

f) ensure proper protection of passwords when passwords are used as secret authentication information in automated log-on procedures and are stored;

g) not use the same secret authentication information for business and non-business purposes.

Other information

Provision of Single Sign On (SSO) or other secret authentication information management tools reduces the amount of secret authentication information that users are required to protect and thus can increase the effectiveness of this control. However, these tools can also increase the impact of disclosure of secret authentication information.

9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

9.4.1 Information access restriction

Control

Access to information and application system functions should be restricted in accordance with the access control policy.

Implementation guidance

Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy.

The following should be considered in order to support access restriction requirements:

a) providing menus to control access to application system functions;

b) controlling which data can be accessed by a particular user;

c) controlling the access rights of users, e.g. read, write, delete and execute;

d) controlling the access rights of other applications;

e) limiting the information contained in outputs;

f) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

9.4.2 Secure log-on procedures

Control

Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

Implementation guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance. A good log-on procedure should:

a) not display system or application identifiers until the log-on process has been successfully completed;

b) display a general notice warning that the computer should only be accessed by authorized users;

c) not provide help messages during the log-on procedure that would aid an unauthorized user;

d) validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

e) protect against brute force log-on attempts;

f) log unsuccessful and successful attempts;

g) raise a security event if a potential attempted or successful breach of log-on controls is detected;

h) display the following information on completion of a successful log-on:

   1) date and time of the previous successful log-on;

   2) details of any unsuccessful log-on attempts since the last successful log-on;

i) not display a password being entered;

j) not transmit passwords in clear text over a network;

k) terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on mobile devices;

l) restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Other information

Passwords are a common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user authentication should be appropriate for the classification of the information to be accessed.

If passwords are transmitted in clear text during the log-on session over a network, they can be captured by a network "sniffer" program.

9.4.3 Password management system

Control

Password management systems should be interactive and should ensure quality passwords.

Implementation guidance

A password management system should:

a) enforce the use of individual user IDs and passwords to maintain accountability;

b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

c) enforce a choice of quality passwords;

d) force users to change their passwords at the first log-on;

e) enforce regular password changes and as needed;

f) maintain a record of previously used passwords and prevent re-use;

g) not display passwords on the screen when being entered;

h) store password files separately from application system data;

i) store and transmit passwords in protected form.

Other information

Some applications require user passwords to be assigned by an independent authority; in such cases, points b), d) and e) of the above guidance do not apply. In most cases the passwords are selected and maintained by users.

9.4.4 Use of privileged utility programs

Control

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Implementation guidance

The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be considered:

a) use of identification, authentication and authorization procedures for utility programs;

b) segregation of utility programs from applications software;

c) limitation of the use of utility programs to the minimum practical number of trusted, authorized users (see 9.2.3);

d) authorization for ad hoc use of utility programs;

e) limitation of the availability of utility programs, e.g. for the duration of an authorized change;

f) logging of all use of utility programs;

g) defining and documenting of authorization levels for utility programs;

h) removal or disabling of all unnecessary utility programs;

i) not making utility programs available to users who have access to applications on systems where segregation of duties is required.

Other information

Most computer installations have one or more utility programs that might be capable of overriding system and application controls.

9.4.5 Access control to program source code

Control

Access to program source code should be restricted.

Implementation guidance

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines should then be considered to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

a) where possible, program source libraries should not be held in operational systems;

b) the program source code and the program source libraries should be managed according to established procedures;

c) support personnel should not have unrestricted access to program source libraries;

d) the updating of program source libraries and associated items and the issuing of program sources to programmers should only be performed after appropriate authorization has been received;

e) program listings should be held in a secure environment;

f) an audit log should be maintained of all accesses to program source libraries;

g) maintenance and copying of program source libraries should be subject to strict change control procedures (see 14.2.2).

If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

10 Cryptography

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

Control

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Implementation guidance

When developing a cryptographic policy the following should be considered:

a) the management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected;

b) based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required;

c) the use of encryption for protection of information transported by mobile or removable media devices or across communication lines;

d) the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

e) roles and responsibilities, e.g. who is responsible for:

   1) the implementation of the policy;

   2) the key management, including key generation (see 10.1.2);

f) the standards to be adopted for effective implementation throughout the organization (which solution is used for which business processes);

g) the impact of using encrypted information on controls that rely upon content inspection (e.g. malware detection).

When implementing the organization's cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see 18.1.5).

Cryptographic controls can be used to achieve different information security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b) integrity/authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information;

c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;

d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

Other information

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

Specialist advice should be sought in selecting appropriate cryptographic controls to meet the information security policy objectives.

10.1.2 Key management

Control

A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.

Implementation guidance

The policy should include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

Cryptographic algorithms, key lengths and usage practices should be selected according to best practice. Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system should be based on an agreed set of standards, procedures and secure methods for:

a) generating keys for different cryptographic systems and different applications;

b) issuing and obtaining public key certificates;

c) distributing keys to intended entities, including how keys should be activated when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;

g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);

h) recovering keys that are lost or corrupted;

i) backing up or archiving keys;

j) destroying keys;

k) logging and auditing of key management related activities.

In order to reduce the likelihood of improper use, activation and deactivation dates for keys should be defined so that the keys can only be used for the period of time defined in the associated key management policy.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates, which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see 15.2).

Other information

The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770[2][3][4] provides further information on key management.

Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case.

11 Physical and environmental security

11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

11.1.1 Physical security perimeter

Control

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

Implementation guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

b) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;

c) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;

d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;

e) all fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner;

f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;

g) information processing facilities managed by the organization should be physically separated from those managed by external parties.

Other information

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.

A secure area may be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter. Special attention to physical access security should be given in the case of buildings holding assets for multiple organizations.

The application of physical controls, especially for the secure areas, should be adapted to the technical and economic circumstances of the organization, as set forth in the risk assessment.

11.1.2 Physical entry controls

Control

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Implementation guidance

The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means;

b) access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN;

c) a physical log book or electronic audit trail of all access should be securely maintained and monitored;

d) all employees, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

e) external party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorized and monitored;

f) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see 9.2.5 and 9.2.6).

11.1.3 Securing offices, rooms and facilities

Control

Physical security for offices, rooms and facilities should be designed and applied.

Implementation guidance

The following guidelines should be considered to secure offices, rooms and facilities:

a) key facilities should be sited to avoid access by the public;

b) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;

c) facilities should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;

d) directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

11.1.4 Protecting against external and environmental threats

Control

Physical protection against natural disasters, malicious attack or accidents should be designed and applied.

Implementation guidance

Specialist advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

11.1.5 Working in secure areas

Control

Procedures for working in secure areas should be designed and applied.

Implementation guidance

The following guidelines should be considered:

a) personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis;

b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

c) vacant secure areas should be physically locked and periodically reviewed;

d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.

The arrangements for working in secure areas include controls for the employees and external party users working in the secure area and they cover all activities taking place in the secure area.

11.1.6 Delivery and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Implementation guidance

The following guidelines should be considered:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;

b) the delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;

c) the external doors of a delivery and loading area should be secured when the internal doors are opened;

d) incoming material should be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;

e) incoming material should be registered in accordance with asset management procedures (see Clause 8) on entry to the site;

f) incoming and outgoing shipments should be physically segregated, where possible;

g) incoming material should be inspected for evidence of tampering en route. If such tampering is discovered it should be immediately reported to security personnel.

11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

11.2.1 Equipment siting and protection

Control

Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Implementation guidance

The following guidelines should be considered to protect equipment:

a) equipment should be sited to minimize unnecessary access into work areas;

b) information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;

c) storage facilities should be secured to avoid unauthorized access;

d) items requiring special protection should be safeguarded to reduce the general level of protection required;

e) controls should be adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism;

f) guidelines for eating, drinking and smoking in proximity to information processing facilities should be established;

g) environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities;

h) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;

i) the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;

j) equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

11.2.2 Supporting utilities

Control

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Implementation guidance

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) should:

a) conform to equipment manufacturer's specifications and local legal requirements;

b) be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;

c) be inspected and tested regularly to ensure their proper functioning;

d) if necessary, be alarmed to detect malfunctions;

e) if necessary, have multiple feeds with diverse physical routing.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms.

Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

11.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.

Implementation guidance

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;

b) power cables should be segregated from communications cables to prevent interference;

c) for sensitive or critical systems further controls to consider include:

   1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

   2) use of electromagnetic shielding to protect the cables;

   3) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;

   4) controlled access to patch panels and cable rooms.

11.2.4 Equipment maintenance

Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

Implementation guidance

The following guidelines for equipment maintenance should be considered:

a) equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;

b) only authorized maintenance personnel should carry out repairs and service equipment;

c) records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance;

d) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared;

e) all maintenance requirements imposed by insurance policies should be complied with;

f) before putting equipment back into operation after its maintenance, it should be inspected to ensure that the equipment has not been tampered with and does not malfunction.

11.2.5 Removal of assets

Control

Equipment, information or software should not be taken off-site without prior authorization.

Implementation guidance

The following guidelines should be considered:

a) employees and external party users who have authority to permit off-site removal of assets should be identified;

b) time limits for asset removal should be set and returns verified for compliance;

c) where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned;

d) the identity, role and affiliation of anyone who handles or uses assets should be documented and this documentation returned with the equipment, information or software.

Other information

Spot checks, undertaken to detect unauthorized removal of assets, can also be performed to detect unauthorized recording devices, weapons, etc., and to prevent their entry into and exit from, the site. Such spot checks should be carried out in accordance with relevant legislation and regulations. Individuals should be made aware that spot checks are carried out, and the verifications should only be performed with authorization appropriate for the legal and regulatory requirements.

11.2.6 Security of equipment and assets off-premises

Control

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Implementation guidance

The use of any information storing and processing equipment outside the organization's premises should be authorized by management. This applies to equipment owned by the organization and that equipment owned privately and used on behalf of the organization.

The following guidelines should be considered for the protection of off-site equipment:

a) equipment and media taken off premises should not be left unattended in public places;

b) manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields;

c) controls for off-premises locations, such as home-working, teleworking and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office (see also ISO/IEC 27033[15][16][17][18][19]);

d) when off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.

Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Other information

Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.

More information about other aspects of protecting mobile equipment can be found in 6.2.

It may be appropriate to avoid the risk by discouraging certain employees from working off-site or by restricting their use of portable IT equipment;

11.2.7 Secure disposal or re-use of equipment

Control

All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Implementation guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Other information

Damaged equipment containing storage media may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk erasure, whole-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files, etc.);

b) the encryption keys are long enough to resist brute force attacks;

c) the encryption keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on encryption, see Clause 10.

Techniques for securely overwriting storage media differ according to the storage media technology. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

11.2.8 Unattended user equipment

Control

Users should ensure that unattended equipment has appropriate protection.

Implementation guidance

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

b) log-off from applications or network services when no longer needed;

c) secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

11.2.9 Clear desk and clear screen policy

Control

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

Implementation guidance

The clear desk and clear screen policy should take into account the information classifications (see 8.2), legal and contractual requirements (see 18.1) and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:

a) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

b) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

c) unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented;

d) media containing sensitive or classified information should be removed from printers immediately.

Other information

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Consider the use of printers with PIN code function, so the originators are the only ones who can get their print-outs and only when standing next to the printer.

12 Operations security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1 Documented operating procedures

Control

Operating procedures should be documented and made available to all users who need them.

Implementation guidance

Documented procedures should be prepared for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management and safety.

The operating procedures should specify the operational instructions, including:

a) the installation and configuration of systems;

b) processing and handling of information both automated and manual;

c) backup (see 12.3);

d) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

e) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see 9.4.4);

f) support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;

g) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (see 8.3 and 11.2.7);

h) system restart and recovery procedures for use in the event of system failure;

i) the management of audit-trail and system log information (see 12.4);

j) monitoring procedures.

Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

12.1.2 Change management

Control

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

Implementation guidance

In particular, the following items should be considered:

a) identification and recording of significant changes;

b) planning and testing of changes;

c) assessment of the potential impacts, including information security impacts, of such changes;

d) formal approval procedure for proposed changes;

e) verification that information security requirements have been met;

f) communication of change details to all relevant persons;

g) fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events;

h) provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident (see 16.1).

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.

Other information

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (see 14.2.2).

12.1.3 Capacity management

Control

The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Implementation guidance

Capacity requirements should be identified, taking into account the business criticality of the concerned system. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or information systems management tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. Examples of managing capacity demand include:

a) deletion of obsolete data (disk space);

b) decommissioning of applications, systems, databases or environments;

c) optimising batch processes and schedules;

d) optimising application logic or database queries;

e) denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

Other information

This control also addresses the capacity of the human resources, as well as offices and facilities.

12.1.4 Separation of development, testing and operational environments

Control

Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

Implementation guidance

The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

a) rules for the transfer of software from development to operational status should be defined and documented;

b) development and operational software should run on different systems or computer processors and in different domains or directories;

c) changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems;

d) other than in exceptional circumstances, testing should not be done on operational systems;

e) compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;

f) users should use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error;

g) sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system (see 14.3).

Other information

Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the operational environment.

Where development and testing personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud or introduce untested or malicious code, which can cause serious operational problems.

Development and testing personnel also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, testing and operational environments is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data (see 14.3 for the protection of test data).

12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

Control

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Implementation guidance

Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The following guidance should be considered:

a) establishing a formal policy prohibiting the use of unauthorized software (see 12.6.2 and 14.2.);

b) implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);

c) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting);

d) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken;

e) reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management (see 12.6);

f) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;

g) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:

   1) scan any files received over networks or via any form of storage medium, for malware before use;

   2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;

   3) scan web pages for malware;

h) defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;

i) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (see 12.3);

j) implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware;

k) implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them;

l) isolating environments where catastrophic impacts may result.

Other information

The use of two or more software products protecting against malware across the information processing environment from different vendors and technology can improve the effectiveness of malware protection.

Care should be taken to protect against the introduction of malware during maintenance and emergency procedures, which may bypass normal malware protection controls.

Under certain conditions, malware protection might cause disturbance within operations.

Use of malware detection and repair software alone as a malware control is not usually adequate and commonly needs to be accompanied by operating procedures that prevent introduction of malware.

12.3 Backup

Objective: To protect against loss of data.

12.3.1 Information backup

Control

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

Implementation guidance

A backup policy should be established to define the organization's requirements for backup of information, software and systems.

The backup policy should define the retention and protection requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

When designing a backup plan, the following items should be taken into consideration:

a) accurate and complete records of the backup copies and documented restoration procedures should be produced;

b) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved and the criticality of the information to the continued operation of the organization;

c) the backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

d) backup information should be given an appropriate level of physical and environmental protection (see Clause 11) consistent with the standards applied at the main site;

e) backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss;

f) in situations where confidentiality is of importance, backups should be protected by means of encryption.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.

Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information should be determined, taking into account any requirement for archive copies to be permanently retained.

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Implementation guidance

Event logs should include, when relevant:

a) user IDs;

b) system activities;

c) dates, times and details of key events, e.g. log-on and log-off;

d) device identity or location if possible and system identifier;

e) records of successful and rejected system access attempts;

f) records of successful and rejected data and other resource access attempts;

g) changes to system configuration;

h) use of privileges;

i) use of system utilities and applications;

j) files accessed and the kind of access;

k) network addresses and protocols;

l) alarms raised by the access control system;

m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;

n) records of transactions executed by users in applications.

Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

Other information

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (see 18.1.4).

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 12.4.3).

12.4.2 Protection of log information

Control

Logging facilities and log information should be protected against tampering and unauthorized access.

Implementation guidance

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

a) alterations to the message types that are recorded;

b) log files being edited or deleted;

c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence (see 16.1.7).

Other information

System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the copying of appropriate message types automatically to a second log, or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.

12.4.3 Administrator and operator logs

Control

System administrator and system operator activities should be logged and the logs protected and regularly reviewed.

Implementation guidance

Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.

Other information

An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

12.4.4 Clock synchronisation

Control

The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.

Implementation guidance

External and internal requirements for time representation, synchronisation and accuracy should be documented. Such requirements can be legal, regulatory, contractual requirements, standards compliance or requirements for internal monitoring. A standard reference time for use within the organization should be defined.

The organization's approach to obtaining a reference time from external source(s) and how to synchronise internal clocks reliably should be documented and implemented.

Other information

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

Control

Procedures should be implemented to control the installation of software on operational systems.

Implementation guidance

The following guidelines should be considered to control changes of software on operational systems:

a) the updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorization (see 9.4.5);

b) operational systems should only hold approved executable code and not development code or compilers;

c) applications and operating system software should only be implemented after extensive and successful testing; the tests should cover usability, security, effects on other systems and user-friendliness and should be carried out on separate systems (see 12.1.4); it should be ensured that all corresponding program source libraries have been updated;

d) a configuration control system should be used to keep control of all implemented software as well as the system documentation;

e) a rollback strategy should be in place before changes are implemented;

f) an audit log should be maintained of all updates to operational program libraries;

g) previous versions of application software should be retained as a contingency measure;

h) old versions of software should be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. Software patches should be applied when they can help to remove or reduce information security weaknesses (see 12.6).

Physical or logical access should only be given to suppliers for support purposes when necessary and with management approval. The supplier's activities should be monitored (see 15.2.1).

Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Control

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Implementation guidance

A current and complete inventory of assets (see Clause 8) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

Appropriate and timely action should be taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

a) the organization should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;

b) information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list, see 8.1.1); these information resources should be updated based on changes in the inventory or when other new or useful resources are found;

c) a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;

d) once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls;

e) depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management (see 12.1.2) or by following information security incident response procedures (see 16.1.5);

f) if a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);

g) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:

   1) turning off services or capabilities related to the vulnerability;

   2) adapting or adding access controls, e.g. firewalls, at network borders (see 13.1);

   3) increased monitoring to detect actual attacks;

   4) raising awareness of the vulnerability;

h) an audit log should be kept for all procedures undertaken;

i) the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;

j) systems at high risk should be addressed first;

k) an effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur;

l) define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

Other information

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see 12.1.2 and 14.2.2).

Vendors are often under significant pressure to release patches as soon as possible. Therefore, there is a possibility that a patch does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling a patch cannot be easily achieved once the patch has been applied.

If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031[14] can be beneficial.

12.6.2 Restrictions on software installation

Control

Rules governing the installation of software by users should be established and implemented.

Implementation guidance

The organization should define and enforce strict policy on which types of software users may install.

The principle of least privilege should be applied. If granted certain privileges, users may have the ability to install software. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted having regard to the roles of the users concerned.

Other information

Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights.

12.7 Information systems audit considerations

Objective: To minimise the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Control

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.

Implementation guidance

The following guidelines should be observed:

a) audit requirements for access to systems and data should be agreed with appropriate management;

b) the scope of technical audit tests should be agreed and controlled;

c) audit tests should be limited to read-only access to software and data;

d) access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

e) requirements for special or additional processing should be identified and agreed;

f) audit tests that could affect system availability should be run outside business hours;

g) all access should be monitored and logged to produce a reference trail.

13 Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

Control

Networks should be managed and controlled to protect information in systems and applications.

Implementation guidance

Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a) responsibilities and procedures for the management of networking equipment should be established;

b) operational responsibility for networks should be separated from computer operations where appropriate (see 6.1.2);

c) special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (see Clause 10 and 13.2); special controls may also be required to maintain the availability of the network services and computers connected;

d) appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security;

e) management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;

f) systems on the network should be authenticated;

g) systems connection to the network should be restricted.

Other information

Additional information on network security can be found in ISO/IEC 27033.[15][16][17][18][19]

13.1.2 Security of network services

Control

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Implementation guidance

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Other information

Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption and network connection controls;

b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;

c) procedures for the network service usage to restrict access to network services or applications, where necessary.

13.1.3 Segregation in networks

Control

Groups of information services, users and information systems should be segregated on networks.

Implementation guidance

One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks (e.g.virtual private networking).

The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy (see 9.1.1), access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy (see 13.1.1) before granting access to internal systems.

The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organization's internal network when properly implemented.

Other information

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Control

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Implementation guidance

The procedures and controls to be followed when using communication facilities for information transfer should consider the following items:

a) procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction;

b) procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications (see 12.2.1);

c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

d) policy or guidelines outlining acceptable use of communication facilities (see 8.1.3);

e) personnel, external party and any other user's responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.;

f) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Clause 10);

g) retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations;

h) controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

i) advising personnel to take appropriate precautions not to reveal confidential information;

j) not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;

k) advising personnel about the problems of using facsimile machines or services, namely:

   1) unauthorized access to built-in message stores to retrieve messages;

   2) deliberate or accidental programming of machines to send messages to specific numbers;

   3) sending documents and messages to the wrong number either by misdialling or using the wrong stored number.

In addition, personnel should be reminded that they should not have confidential conversations in public places or over insecure communication channels, open offices and meeting places.

Information transfer services should comply with any relevant legal requirements (see 18.1).

Other information

Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile and video.

Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products.

The business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls should be considered.

13.2.2 Agreements on information transfer

Control

Agreements should address the secure transfer of business information between the organization and external parties.

Implementation guidance

Information transfer agreements should incorporate the following:

a) management responsibilities for controlling and notifying transmission, dispatch and receipt;

b) procedures to ensure traceability and non-repudiation;

c) minimum technical standards for packaging and transmission;

d) escrow agreements;

e) courier identification standards;

f) responsibilities and liabilities in the event of information security incidents, such as loss of data;

g) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see 8.2);

h) technical standards for recording and reading information and software;

i) any special controls that are required to protect sensitive items, such as cryptography (see Clause 10);

j) maintaining a chain of custody for information while in transit;

k) acceptable levels of access control.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit (see 8.3.3), and should be referenced in such transfer agreements.

The information security content of any agreement should reflect the sensitivity of the business information involved.

Other information

Agreements may be electronic or manual, and may take the form of formal contracts. For confidential information, the specific mechanisms used for the transfer of such information should be consistent for all organizations and types of agreements.

13.2.3 Electronic messaging

Control

Information involved in electronic messaging should be appropriately protected.

Implementation guidance

Information security considerations for electronic messaging should include the following:

a) protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organization;

b) ensuring correct addressing and transportation of the message;

c) reliability and availability of the service;

d) legal considerations, for example requirements for electronic signatures;

e) obtaining approval prior to using external public services such as instant messaging, social networking or file sharing;

f) stronger levels of authentication controlling access from publicly accessible networks.

Other information

There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications.

13.2.4 Confidentiality or non-disclosure agreements

Control

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.

Implementation guidance

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external parties or employees of the organization. Elements should be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);

b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

c) required actions when an agreement is terminated;

d) responsibilities and actions of signatories to avoid unauthorized information disclosure;

e) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

f) the permitted use of confidential information and rights of the signatory to use information;

g) the right to audit and monitor activities that involve confidential information;

h) process for notification and reporting of unauthorized disclosure or confidential information leakage;

i) terms for information to be returned or destroyed at agreement cessation;

j) expected actions to be taken in case of a breach of the agreement.

Based on an organization's information security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply (see 18.1).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other information

Confidentiality and non-disclosure agreements protect organizational information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner.

There may be a need for an organization to use different forms of confidentiality or non-disclosure agreements in different circumstances.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 Information security requirements analysis and specification

Control

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

Implementation guidance

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the identification should be documented and reviewed by all stakeholders.

Information security requirements and controls should reflect the business value of the information involved (see 8.2) and the potential negative business impact which might result from lack of adequate security.

Identification and management of information security requirements and associated processes should be integrated in early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage can lead to more effective and cost efficient solutions.

Information security requirements should also consider:

a) the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements;

b) access provisioning and authorization processes, for business users as well as for privileged or technical users;

c) informing users and operators of their duties and responsibilities;

d) the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity;

e) requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements;

f) requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems.

For applications that provide services over public networks or which implement transactions, the dedicated controls 14.1.2 and 14.1.3 should be considered.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality

in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls should be reconsidered prior to purchasing the product.

Available guidance for security configuration of the product aligned with the final software / service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined e.g. in terms of their functionality, which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Additional functionality should be reviewed to ensure it does not introduce unacceptable additional risks.

Other information

ISO/IEC 27005[11] and ISO 31000[27] provide guidance on the use of risk management processes to identify controls to meet information security requirements.

14.1.2 Securing application services on public networks

Control

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Implementation guidance

Information security considerations for application services passing over public networks should include the following:

a) the level of confidence each party requires in each other's claimed identity, e.g. through authentication;

b) authorization processes associated with who may approve contents of, issue or sign key transactional documents;

c) ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;

d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

e) the level of trust required in the integrity of key documents;

f) the protection requirements of any confidential information;

g) the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;

h) the degree of verification appropriate to verify payment information supplied by a customer;

i) selecting the most appropriate settlement form of payment to guard against fraud;

j) the level of protection required to maintain the confidentiality and integrity of order information;

k) avoidance of loss or duplication of transaction information;

l) liability associated with any fraudulent transactions;

m) insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls (see Clause 10), taking into account compliance with legal requirements (see Clause 18, especially see 18.1.5 for cryptography legislation).

Application service arrangements between partners should be supported by a documented agreement which commits both parties to the agreed terms of services, including details of authorization (see b) above).

Resilience requirements against attacks should be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.

Other information

Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Application services can make use of secure authentication methods, e.g. using public key cryptography and digital signatures (see Clause 10) to reduce the risks. Also, trusted third parties can be used, where such services are needed.

14.1.3 Protecting application services transactions

Control

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Implementation guidance

Information security considerations for application service transactions should include the following:

a) the use of electronic signatures by each of the parties involved in the transaction;

b) all aspects of the transaction, i.e. ensuring that:

   1) user's secret authentication information of all parties are valid and verified;

   2) the transaction remains confidential;

   3) privacy associated with all parties involved is retained;

c) communications path between all involved parties is encrypted;

d) protocols used to communicate between all involved parties are secured;

e) ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on a storage medium directly accessible from the Internet;

f) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

Other information

The extent of the controls adopted needs to be commensurate with the level of the risk associated with each form of application service transaction.

Transactions may need to comply with legal and regulatory requirements in the jurisdiction which the transaction is generated from, processed via, completed at or stored in.

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

Control

Rules for the development of software and systems should be established and applied to developments within the organization.

Implementation guidance

Secure development is a requirement to build up a secure service, architecture, software and system. Within a secure development policy, the following aspects should be put under consideration:

a) security of the development environment;

b) guidance on the security in the software development lifecycle:

   1) security in the software development methodology;

   2) secure coding guidelines for each programming language used;

c) security requirements in the design phase;

d) security checkpoints within the project milestones;

e) secure repositories;

f) security in the version control;

g) required application security knowledge;

h) developers' capability of avoiding, finding and fixing vulnerabilities.

Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use. Developers should be trained in their use and testing and code review should verify their use.

If development is outsourced, the organization should obtain assurance that the external party complies with these rules for secure development (see 14.2.7).

Other information

Development may also take place inside applications, such as office applications, scripting, browsers and databases.

14.2.2 System change control procedures

Control

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

Implementation guidance

Formal change control procedures should be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts.

Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated (see 12.1.2). The change control procedures should include but not be limited to:

a) maintaining a record of agreed authorization levels;

b) ensuring changes are submitted by authorized users;

c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

d) identifying all software, information, database entities and hardware that require amendment;

e) identifying and checking security critical code to minimize the likelihood of known security weaknesses;

f) obtaining formal approval for detailed proposals before work commences;

g) ensuring authorized users accept changes prior to implementation;

h) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

i) maintaining a version control for all software updates;

j) maintaining an audit trail of all change requests;

k) ensuring that operating documentation (see 12.1.1) and user procedures are changed as necessary to remain appropriate;

l) ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

Other information

Changing software can impact the operational environment and vice versa.

Good practice includes the testing of new software in an environment segregated from both the production and development environments (see 12.1.4). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Where automatic updates are considered, the risk to the integrity and availability of the system should be weighed against the benefit of speedy deployment of updates. Automated updates should not be used on critical systems as some updates can cause critical applications to fail.

14.2.3 Technical review of applications after operating platform changes

Control

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Implementation guidance

This process should cover:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes;

b) ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation;

c) ensuring that appropriate changes are made to the business continuity plans (see Clause 17).

Other information

Operating platforms include operating systems, databases and middleware platforms. The control should also be applied for changes of applications.

14.2.4 Restrictions on changes to software packages

Control

Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.

Implementation guidance

As far as possible and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered:

a) the risk of built-in controls and integrity processes being compromised;

b) whether the consent of the vendor should be obtained;

c) the possibility of obtaining the required changes from the vendor as standard program updates;

d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes;

e) compatibility with other software in use.

If changes are necessary the original software should be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software (see 12.6.1). All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

14.2.5 Secure system engineering principles

Control

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Implementation guidance

Secure information system engineering procedures based on security engineering principles should be established, documented and applied to in-house information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

These principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They

should also be regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

The established security engineering principles should be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization should confirm that the rigour of suppliers' security engineering principles is comparable with its own.

Other information

Application development procedures should apply secure engineering techniques in the development of applications that have input and output interfaces. Secure engineering techniques provide guidance on user authentication techniques, secure session control and data validation, sanitisation and elimination of debugging codes.

14.2.6 Secure development environment

Control

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Implementation guidance

A secure development environment includes people, processes and technology associated with system development and integration.

Organizations should assess risks associated with individual system development efforts and establish secure development environments for specific system development efforts, considering:

a) sensitivity of data to be processed, stored and transmitted by the system;

b) applicable external and internal requirements, e.g. from regulations or policies;

c) security controls already implemented by the organization that support system development;

d) trustworthiness of personnel working in the environment (see 7.1.1);

e) the degree of outsourcing associated with system development;

f) the need for segregation between different development environments;

g) control of access to the development environment;

h) monitoring of change to the environment and code stored therein;

i) backups are stored at secure offsite locations;

j) control over movement of data from and to the environment.

Once the level of protection is determined for a specific development environment, organizations should document corresponding processes in secure development procedures and provide these to all individuals who need them.

14.2.7 Outsourced development

Control

The organization should supervise and monitor the activity of outsourced system development.

Implementation guidance:

Where system development is outsourced, the following points should be considered across the organization's entire external supply chain:

a) licensing arrangements, code ownership and intellectual property rights related to the outsourced content (see 18.1.2);

b) contractual requirements for secure design, coding and testing practices (see 14.2.1);

c) provision of the approved threat model to the external developer;

d) acceptance testing for the quality and accuracy of the deliverables;

e) provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;

f) provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery;

g) provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;

h) escrow arrangements, e.g. if source code is no longer available;

i) contractual right to audit development processes and controls;

j) effective documentation of the build environment used to create deliverables;

k) the organization remains responsible for compliance with applicable laws and control efficiency verification.

Other information

Further information on supplier relationships can be found in ISO/IEC 27036.[21][22][23]

14.2.8 System security testing

Control

Testing of security functionality should be carried out during development.

Implementation guidance

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected (see 14.1.1 and 14.1.9). The extent of testing should be in proportion to the importance and nature of the system.

14.2.9 System acceptance testing

Control

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Implementation guidance

System acceptance testing should include testing of information security requirements (see 14.1.1 and 14.1.2) and adherence to secure system development practices (see 14.2.1). The testing should also be conducted on received components and integrated systems. Organizations can leverage automated tools,

such as code analysis tools or vulnerability scanners, and should verify the remediation of security-related defects.

Testing should be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organization's environment and that the tests are reliable.

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1 Protection of test data

Control

Test data should be selected carefully, protected and controlled.

Implementation guidance

The use of operational data containing personally identifiable information or any other confidential information for testing purposes should be avoided. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification (see ISO/IEC 29101[26]).

The following guidelines should be applied to protect operational data, when used for testing purposes:

a) the access control procedures, which apply to operational application systems, should also apply to test application systems;

b) there should be separate authorization each time operational information is copied to a test environment;

c) operational information should be erased from a test environment immediately after the testing is complete;

d) the copying and use of operational information should be logged to provide an audit trail.

Other information

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance

The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes

and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

a) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;

b) a standardised process and lifecycle for managing supplier relationships;

c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;

e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;

f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;

g) types of obligations applicable to suppliers to protect the organization's information;

h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;

i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;

j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;

k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;

l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;

m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information

Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

15.1.2 Addressing security within supplier agreements

Control

All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;

b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;

c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

e) rules of acceptable use of information, including unacceptable use if necessary;

f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;

g) information security policies relevant to the specific contract;

h) incident management requirements and procedures (especially notification and collaboration during incident remediation);

i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures;

j) relevant regulations for sub-contracting, including the controls that need to be implemented;

k) relevant agreement partners, including a contact person for information security issues;

l) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

m) right to audit the supplier processes and controls related to the agreement;

n) defect resolution and conflict resolution processes;

o) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

p) supplier's obligations to comply with the organization's security requirements.

Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers).

The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance

The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;

c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

d) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

e) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;

f) obtaining assurance that critical components and their origin can be traced throughout the supply chain;

g) obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

h) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

i) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information

The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Control

Organizations should regularly monitor, review and audit supplier service delivery.

Implementation guidance

Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organization and the supplier to:

a) monitor service performance levels to verify adherence to the agreements;

b) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

c) conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

d) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

e) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

f) resolve and manage any identified problems;

g) review information security aspects of the supplier's relationships with its own suppliers;

h) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing changes to supplier services

Control

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Implementation guidance

The following aspects should be taken into consideration:

a) changes to supplier agreements;

b) changes made by the organization to implement:

   1) enhancements to the current services offered;

   2) development of any new applications and systems;

   3) modifications or updates of the organization's policies and procedures;

   4) new or changed controls to resolve information security incidents and to improve security;.

c) changes in supplier services to implement:

   1) changes and enhancement to networks;

   2) use of new technologies;

   3) adoption of new products or newer versions/releases;

   4) new development tools and environments;

   5) changes to physical location of service facilities;

   6) change of suppliers;

   7) sub-contracting to another supplier.

16 Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

Control

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Implementation guidance

The following guidelines for management responsibilities and procedures with regard to information security incident management should be considered:

a) management responsibilities should be established to ensure that the following procedures are developed and communicated adequately within the organization:

   1) procedures for incident response planning and preparation;

   2) procedures for monitoring, detecting, analysing and reporting of information security events and incidents;

3) procedures for logging incident management activities;

4) procedures for handling of forensic evidence;

5) procedures for assessment of and decision on information security events and assessment of information security weaknesses;

6) procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations;

b) procedures established should ensure that:

1) competent personnel handle the issues related to information security incidents within the organization;

2) a point of contact for security incidents' detection and reporting is implemented;

3) appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained;

c) reporting procedures should include:

1) preparing information security event reporting forms to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event;

2) the procedure to be undertaken in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact and taking only coordinated actions;

3) reference to an established formal disciplinary process for dealing with employees who commit security breaches;

4) suitable feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

Other information

Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.

Detailed guidance on information security incident management is provided in ISO/IEC 27035.[20]

16.1.2 Reporting information security events

Control

Information security events should be reported through appropriate management channels as quickly as possible.

Implementation guidance

All employees and contractors should be made aware of their responsibility to report information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported.

Situations to be considered for information security event reporting include:

a) ineffective security control;

b) breach of information integrity, confidentiality or availability expectations;

c) human errors;

d) non-compliances with policies or guidelines;

e) breaches of physical security arrangements;

f) uncontrolled system changes;

g) malfunctions of software or hardware;

h) access violations.

Other information

Malfunctions or other anomalous system behaviour may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

16.1.3 Reporting information security weaknesses

Control

Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

Implementation guidance

All employees and contractors should report these matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible and available as possible.

Other information

Employees and contractors should be advised not to attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

16.1.4 Assessment of and decision on information security events

Control

Information security events should be assessed and it should be decided if they are to be classified as information security incidents.

Implementation guidance

The point of contact should assess each information security event using the agreed information security event and incident classification scale and decide whether the event should be classified as an information security incident. Classification and prioritization of incidents can help to identify the impact and extent of an incident.

In cases where the organization has an information security incident response team (ISIRT), the assessment and decision can be forwarded to the ISIRT for confirmation or reassessment.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

16.1.5 Response to information security incidents

Control

Information security incidents should be responded to in accordance with the documented procedures.

Implementation guidance

Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organization or external parties (see 16.1.1).

The response should include the following:

a) collecting evidence as soon as possible after the occurrence;

b) conducting information security forensics analysis, as required (see 16.1.7);

c) escalation, as required;

d) ensuring that all involved response activities are properly logged for later analysis;

e) communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;

f) dealing with information security weakness(es) found to cause or contribute to the incident;

g) once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis should take place, as necessary, to identify the source of the incident.

Other information

The first goal of incident response is to resume 'normal security level' and then initiate the necessary recovery.

16.1.6 Learning from information security incidents

Control

Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Implementation guidance

There should be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

Other information

The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process (see 5.1.2).

With due care of confidentiality aspects, anecdotes from actual information security incidents can be used in user awareness training (see 7.2.2) as examples of what could happen, how to respond to such incidents and how to avoid them in the future.

16.1.7 Collection of evidence

Control

The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Implementation guidance

Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.

In general, these procedures for evidence should provide processes of identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off. The procedures should take account of:

a) chain of custody;

b) safety of evidence;

c) safety of personnel;

d) roles and responsibilities of personnel involved;

e) competency of personnel;

f) documentation;

g) briefing.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Forensic evidence may transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as forensic evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.

Other information

Identification is the process involving the search for, recognition and documentation of potential evidence. Collection is the process of gathering the physical items that can contain potential evidence. Acquisition is the process of creating a copy of data within a defined set. Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence.

When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037[24] provides guidelines for identification, collection, acquisition and preservation of digital evidence.

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 Planning information security continuity

Control

The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

Implementation guidance

An organization should determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process. Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

Other information

In order to reduce the time and effort of an 'additional' business impact analysis for information security, it is recommended to capture information security aspects within the normal business continuity management or disaster recovery management business impact analysis. This implies that the information security continuity requirements are explicitly formulated in the business continuity management or disaster recovery management processes.

Information on business continuity management can be found in ISO/IEC 27031,[14] ISO 22313[9] and ISO 22301.[8]

17.1.2 Implementing information security continuity

Control

The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Implementation guidance

An organization should ensure that:

a) an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;

b) incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;

c) documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives (see 17.1.1).

According to the information security continuity requirements, the organization should establish, document, implement and maintain:

a) information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;

b) processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;

c) compensating controls for information security controls that cannot be maintained during an adverse situation.

Other information

Within the context of business continuity or disaster recovery, specific processes and procedures may have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them should be protected. Therefore an organization should

involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures.

Information security controls that have been implemented should continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls should be established, implemented and maintained to maintain an acceptable level of information security.

17.1.3 Verify, review and evaluate information security continuity

Control

The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

"Implementation guidance"

Organizational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such cases, the continuity of processes, procedures and controls for information security should be reviewed against these changed requirements.

Organizations should verify their information security management continuity by:

a) exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;

b) exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives;

c) reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

Other information

The verification of information security continuity controls is different from general information security testing and verification and should be performed outside the testing of changes. If possible, it is preferable to integrate verification of information security continuity controls with the organization's business continuity or disaster recovery tests.

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Implementation guidance

Organizations should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures should be considered.

Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

Other information

The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems.

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

Control

All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization.

Implementation guidance

The specific controls and individual responsibilities to meet these requirements should also be defined and documented.

Managers should identify all legislation applicable to their organization in order to meet the requirements for their type of business. If the organization conducts business in other countries, managers should consider compliance in all relevant countries.

18.1.2 Intellectual property rights

Control

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

Implementation guidance

The following guidelines should be considered to protect any material that may be considered intellectual property:

a) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;

b) acquiring software only through known and reputable sources, to ensure that copyright is not violated;

c) maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them;

d) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;

e) maintaining proof and evidence of ownership of licences, master disks, manuals, etc.;

f) implementing controls to ensure that any maximum number of users permitted within the licence is not exceeded;

g) carrying out reviews that only authorized software and licensed products are installed;

h) providing a policy for maintaining appropriate licence conditions;

i) providing a policy for disposing of or transferring software to others;

j) complying with terms and conditions for software and information obtained from public networks;

k) not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law;

l) not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. The importance and awareness of intellectual property rights should be communicated to staff for software developed by the organization.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which may involve fines and criminal proceedings.

18.1.3 Protection of records

Control

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

Implementation guidance

When deciding upon protection of specific organizational records, their corresponding classification based on the organization's classification scheme, should be considered. Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of allowable storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys and programs associated with encrypted archives or digital signatures (see Clause 10), should also be stored to enable decryption of the records for the length of time the records are retained.

Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

To meet these record safeguarding objectives, the following steps should be taken within an organization:

a) guidelines should be issued on the retention, storage, handling and disposal of records and information;

b) a retention schedule should be drawn up identifying records and the period of time for which they should be retained;

c) an inventory of sources of key information should be maintained.

Other information

Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organization operates within statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status of an organization to shareholders, external parties and auditors. National law or regulation may set the time period and data content for information retention.

Further information about managing organizational records can be found in ISO 15489-1.[5]

18.1.4 Privacy and protection of personally identifiable information

Control

Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

Implementation guidance

An organization's data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information.

Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented.

Other information

ISO/IEC 29100[25] provides a high-level framework for the protection of personally identifiable information within information and communication technology systems. A number of countries have introduced legislation placing controls on the collection, processing and transmission of personally identifiable information (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing and disseminating personally identifiable information, and may also restrict the ability to transfer personally identifiable information to other countries.

18.1.5 Regulation of cryptographic controls

Control

Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.

Implementation guidance

The following items should be considered for compliance with the relevant agreements, laws and regulations:

a) restrictions on import or export of computer hardware and software for performing cryptographic functions;

b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) restrictions on the usage of encryption;

d) mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with relevant legislation and regulations. Before encrypted information or cryptographic controls are moved across jurisdictional borders, legal advice should also be taken.

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

18.2.1 Independent review of information security

Control

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

Implementation guidance

Management should initiate the independent review. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

Such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience.

The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained.

If the independent review identifies that the organization's approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies (see 5.1.1), management should consider corrective actions.

Other information

ISO/IEC 27007[12], "Guidelines for information security management systems auditing" and ISO/IEC TR 27008[13], "Guidelines for auditors on information security controls" also provide guidance for carrying out the independent review.

18.2.2 Compliance with security policies and standards

Control

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

Implementation guidance

Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

a) identify the causes of the non-compliance;

b) evaluate the need for actions to achieve compliance;

c) implement appropriate corrective action;

d) review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews (see 18.2.1) when an independent review takes place in the area of their responsibility.

Other information

Operational monitoring of system use is covered in 12.4.

18.2.3 Technical compliance review

Control

Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.

Implementation guidance

Technical compliance should be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed.

If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.

Any technical compliance review should only be carried out by competent, authorized persons or under the supervision of such persons.

Other information

Technical compliance reviews involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance review requires specialist technical expertise.

Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorized access due to these vulnerabilities.

Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). Penetration testing and vulnerability assessments are not a substitute for risk assessment.

ISO/IEC TR 27008[13] provides specific guidance regarding technical compliance reviews.

Bibliography

[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1, *Information technology Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[4] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[5] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[6] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[7] ISO/IEC 20000-2,[1)]*Information technology — Service management — Part 2: Guidance on the application of service management systems*

[8] ISO 22301, *Societal security — Business continuity management systems — Requirements*

[9] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[10] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[11] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

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

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

[14] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[15] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[16] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[17] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[18] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[19] ISO/IEC 27033-5, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)*

[20] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[21] ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

1) ISO/IEC 20000-2:2005 has been cancelled and replaced by ISO/IEC 20000-2:2012, *Information technology — Service management — Part 2: Guidance on the application of service management systems.*

[22] ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements*

[23] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security*

[24] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[27] ISO 31000, *Risk management — Principles and guidelines*

Anteckningar/Notes

Anteckningar/Notes

Anteckningar/Notes

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 NI OCH ACCEPTERAR VILLKOREN I DETTA LICENSAVTAL.

1. Parter
Detta licensavtal är ingått mellan SIS Förlag AB (”SIS Förlag”) och det företag/den person som licensierar de produkter som medföljer eller levereras under licensen (”Kunden”).

2. Upphovsrätt till Produkten
Den produkt 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 Förlag upplåter till Kunden en icke-exklusiv, icke-överlåtbar nyttjanderätt att använda Produkten enligt följande:
(a) Om Produkten levereras i pappersform har Kunden rätt att använda det exemplar av Produkten som levereras med detta licensavtal.
(b) Om Produkten levereras i elektronisk form har Kunden rätt att installera Produkten på en (1) dator, vilken ägs, hyrs eller kontrolleras av Kunden. Kunden har även rätt att flytta Produkten till en annan dator, 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 kopiera, anpassa, förändra, översätta, hyra eller leasa ut, sälja, underlicensiera eller på annat sätt distribuera eller överlåta Produkten på annat sätt än som uttryckligen anges i detta licensavtal. Kunden får inte ta bort eller förändra någon upplysning om upphovsrätt och äganderätt som finns på Produkten och ansvarar vidare för att de upplysningar om upphovsrätt och äganderätt som finns på originalexemplaren av Produkten återges på samtliga kopior (om några) som Kunden har rätt att göra enligt detta licensavtal.

5. SIS Förlags ansvar samt ansvarsbegränsning
SIS Förlag ansvarar för att innehållet i den textmassa som Produkten omfattar levereras till Kunden i det skick som den kommit SIS Förlag tillhanda. I övrigt levereras Produkten i ”befintligt skick” och SIS Förlag ansvarar inte för att den information som Produkten förmedlar är korrekt eller fullständig, eller för resultatet av användningen av Produkten.
SIS Förlags ansvar omfattar endast direkta skador och ej indirekta skador såsom exempelvis förlorad handelsvinst och inte i något fall förlust av data. I inget fall ska SIS Förlags totala skadeståndsansvar enligt detta licensavtal överstiga ett belopp motsvarande den avgift som Kunden betalat för nyttjanderätten enligt detta licensavtal.

6. Intrång i immaterialrätt
Om det, enligt SIS Förlag föreligger risk för att krav avseende intrång i tredje mans immateriella rättigheter kan komma att ställas på grund av användningen av Produkterna, har SIS Förlag 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 Förlag ansvarar inte gentemot Kunden för krav som kunde ha undvikits om Kunden accepterat ersättningsprodukt eller om användningen av Produkten stoppats.

7. 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.

8. Avtalstid och uppsägning
Detta avtal gäller tills vidare. Kunden har rätt att säga upp licensavtalet när som helst. SIS Förlag 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.

9. Tillämplig lag
Svensk lag, förutom dess bestämmelser om lagkonflikter, ska tillämpas på detta licensavtal, och tvister ska avgöras genom förfarande vid svensk domstol.

10. 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 licens-avtalet kan endast ske genom skriftligen upprättad handling vilken undertecknats av SIS Förlag. 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.

End user license

IMPORTANT – PLEASE READ THESE TERMS AND CONDITIONS BEFORE USING THE PRODUCTS DISTRIBUTED WITH THIS LICENSE. BY USING THE PRODUCTS YOU ARE ACCEPTING THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

1. Parties
This License Agreement is by and between SIS Förlag AB (”SIS Förlag”) and the company/ individual licensing the products distributed and/or delivered with the License Agreement (“Customer”).

2. Rights to the Products
The Product distributed and/or delivered with the License Agreement (“Product”) is protected by Swedish and international copyright and other intellectual property laws and are the exclusive property of the proprietary owner/s stated on such Product.

3. Grant of Rights
SIS Förlag grants to Customer, a non-exclusive, non-assignable, limited right to use the Products as follows:
(a) If the Product is distributed in paper format you may use the copy of the Product distributed with this License Agreement.
(b) If the Product is distributed in electronic format you may install the Product on one (1) computer owned, leased or otherwise controlled by Customer. Customer may transfer the Product to another
computer, provided that the Product is removed from the computer from which it is transferred. Neither concurrent use on two or more computers nor use in a local area network or other network is permitted.

4. Restrictions in Use
Except as expressly permitted by this Agreement, Customer shall not copy, adapt, modify, translate, rent or lease, sell, sublicense or in any other manner distribute or transfer the Products. Customer shall not remove or change any copyright notices or proprietary legends on the Products, and is responsible for and shall ensure that each copy of the Products which Customer is allowed to make under this License Agreement (if any), are distributed with all copyright notices or proprietary legends contained on the original Products.

5. Limited Warranty, Limitation of Liability
SIS Förlag warrants that the content of the text encompassed by the Products is delivered to Customer in the same condition in which it was delivered to SIS Förlag. Except as provided for in this section 5 the Products are delivered “as is” and
SIS Förlag does not give any warranty of correctness or completeness as to the information conveyed by the Products or for the result of the use of the Products. SIS Förlag’s liability pursuant to this Agreement shall only be for direct damage and not for indirect damage, including but not limited to loss of profit. Under no circumstances shall SIS Förlag be liable for loss of data. SIS Förlag’s total liability pursuant to this Agreement shall never exceed the fees paid by Customer for the rights granted pursuant to this license agreement.

6. Intellectual Property Infringement
If, in the opinion of SIS Förlag, there is a risk of a claim is instituted against Customer, alleging that a Product distributed by SIS Förlag hereunder infringes any duly issued intellectual property right of a third party, SIS Förlag may, at its sole option and expense: (i) procure for Customer the right to use or sell such Product; (ii) substitute a functionally equivalent, non-infringing unit of the Product or modify such Product so that it no longer infringes but is substantially equivalent in functionality; or (iii) stop the Customer’s use of the Product and refund the License Agreement paid by Customer for such Product during the time hen such Product could not be used. SIS Förlag shall have no liability to Customer for claims that could have been avoided if the Customer would haveaccepted a replacement product or if the use of the Product would have been stopped.

7. Export
Customer shall not export or re-export, in whole or in part, the Products or any information regarding the Products, in contradiction to any stipulations contained on the Products or contrary to Swedish or any other applicable export legislation.

8. Term and Termination
This License Agreement will continue for an indefinite duration. Customer may terminate this License Agreement at any time. SIS Förlag may terminate this License Agreement immediately upon breach of any provision of this License Agreement. Upon any termination of this License Agreement, Customer shall immediately discontinue the use of the Product and destroy all copies of the Product.

9. Governing Law
This License Agreement shall be governed by the laws of Sweden without reference to its conflict of law provisions and any dispute shall be settled by Swedish courts.

10. Miscellaneous
This License Agreement constitutes the complete and exclusive agreement between SIS Förlag and you with respect to the subject matter hereof, and supercedes all prior oral or written understandings, communications or agreements not specifically incorporated herein. This License Agreement may not be modified except in writing duly signed by an authorized representative of SIS Förlag and you. If any provision of this License Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable, and such decision shall not affect the enforceability (i) of such provision under other circumstances, or (ii) of the remaining provisions here of under all circumstances.

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 Förlag AB är störst i Norden på att leverera standarder och allt som rör dess tillämpning. En tryckt standard från SIS Förlag AB 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 Förlag AB is the leading supplier in the Nordic area of standards and all related applications. Printed standards from SIS Förlag AB 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 Förlag AB SE-118 80 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