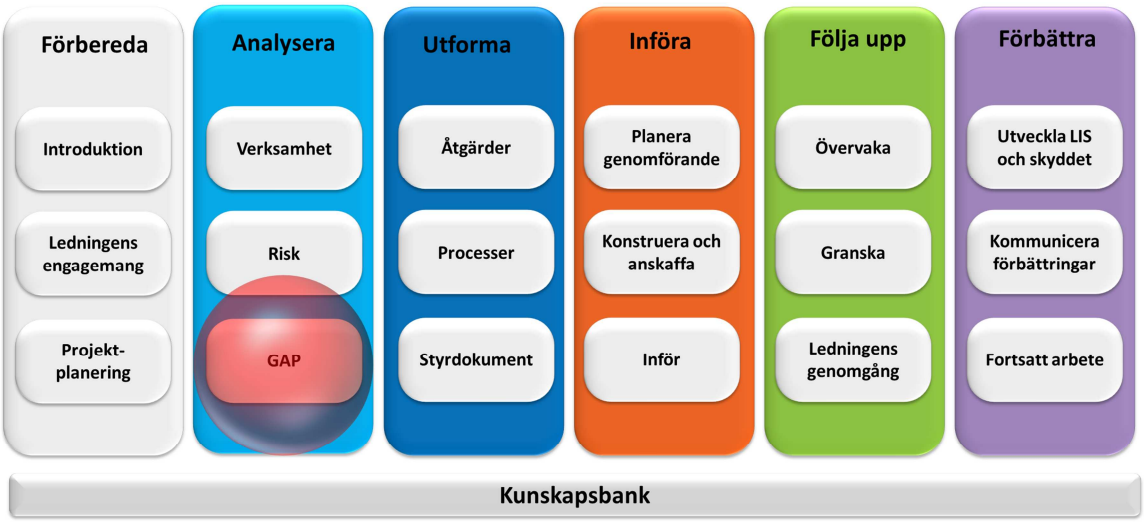
Myndigheten för samhällsskydd och beredskap

Gapanalys - Checklistan



Det här dokumentet är en del av metodstödet som finns att tillgå på www.informationssäkerhet.se

Författare
Helena Andersson, MSB
Jan-Olof Andersson, RPS
Fredrik Björck, MSB konsult (Visente)
Martin Eriksson, MSB
Rebecca Eriksson, RPS
Robert Lundberg, MSB
Michael Patrickson, MSB
Kristina Starkerud, FRA

Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

5. Säkerhetspolicy

5.1 Informationssäkerhetspolicy

Mål: Att ange ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med organisationens verksamhetskrav och relevanta lagar och föreskrifter.

Ledningen bör fastställa en tydlig policyinriktning i enlighet med verksamhetsmål och visa sitt stöd och engagemang för informationssäkerhet genom att utfärda och underhålla en informationssäkerhetspolicy för hela organisationen.

5.1.1 Policydokument för informationssäkerhet

Ett policydokument för informationssäkerhet bör godkännas av ledningen samt publiceras och kommuniceras till alla anställda och relevanta externa parter. *Kritisk säkerhetsåtgärd: JA* *Risk: Om inte ledningen tydligt kommunicerar ut sin viljeinriktning kan risker förbises eller hanteras felaktigt.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**Är åtgärden införd?**		
		JA	**NEJ**	**VET EJ**
1.	Ett policydokument för informationssäkerhet bör uttrycka ledningens engagemang och visa organisationens angreppssätt gällande styrning av informationssäkerhet. Kommentar:			
2.	Policydokumentet bör omfatta uttalanden angående: a) en definition av informationssäkerhet, dess övergripande mål och omfattning samt vikten av säkerhet som en möjliggörande mekanism för delning av information (se Orientering) Kommentar:			

Nivåstyrande frågor		**Är åtgärden införd?**		
		JA	**NEJ**	**VET EJ**
3.	b) ett uttalande om ledningens avsikt som ger stöd för informationssäkerhetens mål och principer i linje med organisationens strategi och mål; Kommentar:			
4.	c) ett ramverk för att besluta om åtgärdsmål och säkerhetsåtgärder, inklusive strukturen för riskbedömning och riskhantering; Kommentar:			
5.	d) en kort förklaring av säkerhetspolicyer, principer, standarder och efterlevnadskrav av särskild betydelse för organisationen, innefattande: 1) överensstämmelse med lagar, förordningar och avtalskrav; 2) krav på medvetenhet, utbildning och praktisk övning rörande säkerhet; 3) kontinuitetsplanering; 4) konsekvenser vid avvikelser från informationssäkerhetspolicyn; Kommentar:			
6.	e) en definition av allmänna och särskilda ansvar rörande styrning av informationssäkerhet, inklusive rapportering av informationssäkerhetsincidenter. Kommentar:			
7.	f) hänvisning till dokumentation som kan stödja policyn, t.ex. mera detaljerade säkerhetspolicyer och rutiner för specifika informationssystem eller säkerhetsregler användare bör efterleva. Kommentar:			
8.	Denna informationssäkerhetspolicy bör kommuniceras genom hela organisationen till användare i en form som är relevant, tillgänglig och begriplig för den avsedda läsaren.			

Nivåstyrande frågor		**Är åtgärden införd?**		
		JA	**NEJ**	**VET EJ**
	Kommentar:			

Övrig information
Informationssäkerhetspolicyn kan utgöra en del av ett övergripande policydokument. Om informationssäkerhetspolicyn sprids utanför organisationen bör försiktighet iakttas så att känslig information inte avslöjas.

Ytterligare information finns i ISO/IEC 13335-1:2004.

5.1.2 Granskning av informationssäkerhetspolicyn

Informationssäkerhetspolicyn bör granskas vid planerade intervall, eller om betydande förändringar inträffar, för att säkerställa sig om dess fortsatta lämplighet, tillräcklighet och verkan. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan regelbunden översyn kan säkerhetspolicyn tappa sin effektivitet som verktyg för riskhantering.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Informationssäkerhetspolicyn bör ha en ägare med uttalat ledningsansvar för utveckling, granskning och utvärdering av säkerhetspolicyn. Kommentar:			
2.	Granskningen bör omfatta bedömning av möjligheter att förbättra organisationens informationssäkerhetspolicy och angreppssätt för att hantera informationssäkerhet som svar på förändringar av organisationsmiljön, verksamhetsförhållanden, juridiska förhållanden eller tekniska miljö. Kommentar:			
3.	Granskningen av informationssäkerhetspolicyn bör beakta resultaten från ledningens genomgångar. Det bör finnas fastställda rutiner för ledningens genomgång, inklusive ett tidsschema eller			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	fastställt intervall mellan genomgångarna. Kommentar:			
4.	Det bör finnas fastställda rutiner för ledningens genomgång, inklusive ett tidsschema eller fastställt intervall mellan genomgångarna. Kommentar:			
5.	Underlag till ledningens genomgång bör inkludera information om: a) återkoppling från intressenter; Kommentar:			
6.	b) resultat av oberoende granskningar (se 6.1.8); Kommentar:			
7.	c) status i fråga om förebyggande och korrigerande åtgärder (se 6.1.8 och 15.2.1); Kommentar:			
8.	d) resultat från tidigare ledningens genomgång; Kommentar:			
9.	e) processernas prestanda och efterlevnaden av informationssäkerhetspolicyn; Kommentar:			
10.	f) förändringar som skulle kunna påverka hur organisationen gör för att styra informationssäkerheten, inklusive förändringar i organisationsmiljö, verksamhetsförhållanden, resursers tillgänglighet, avtalsvillkor, föreskrifter och juridiska förhållanden eller teknisk miljö; Kommentar:			
11.	g) trender i fråga om hot och sårbarhet; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
12.	h) rapporterade informationssäkerhetsincidenter (se 13.1); Kommentar:			
13.	i) rekommendationer föreskrivna av relevanta myndigheter (se 6.1.6). Kommentar:			
14.	Resultatet av ledningens genomgång bör innefatta beslut och åtgärder relaterade till: a) förbättring av organisationens angreppssätt för styrning av informationssäkerhet och dess ingående processer; Kommentar:			
15.	b) förbättring av åtgärdsmål och säkerhetsåtgärder; Kommentar:			
16.	c) förbättring i fråga om fördelning av resurser och/eller ansvar. Kommentar:			
17.	Resultatet av ledningens genomgång bör dokumenteras. Kommentar:			
18.	Ledningens godkännande av reviderad policy bör inhämtas. Kommentar:			

6. Organisation av informationssäkerheten

6.1 Intern organisation

Mål: Att styra informationssäkerhet inom organisationen.

Ett ramverk för styrning bör upprättas för att initiera och styra införandet av informationssäkerhet inom organisationen.

Ledningen bör godkänna informationssäkerhetspolicyn, tilldela roller i säkerhetsarbetet, samt samordna och granska införandet av säkerhet i hela organisationen.

Om det är nödvändigt bör en enhet för specialistrådgivning i säkerhetsfrågor inrättas och göras tillgänglig inom organisationen. Kontakt med externa säkerhetsspecialister eller grupper, innefattandes relevanta myndigheter, bör utvecklas för att kunna följa branschtrender, övervaka standarder och utvärderingsmetoder samt för att tillhandahålla lämpliga kontaktpunkter vid hantering av informationssäkerhetsincidenter. Ett multidisciplinärt förhållningssätt till informationssäkerhet bör uppmuntras.

6.1.1 Ledningens engagemang för informationssäkerhet

Ledningen bör aktivt stödja säkerheten inom organisationen genom tydlig inriktning, påvisat engagemang, tydlig fördelning och bekräftelse av ansvar för informationssäkerhet. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan ett tydligt, aktivt stöd från ledningen finns det risk för att de anställda åsidosätter säkerheten. Säkerhet ska vara djupt inrotat i alla användares beteende.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor	JA	NEJ	VET EJ

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Ledningen bör: a) säkerställa att mål för informationssäkerhet fastställs, uppfyller organisationens krav och är integrerade i relevanta processer; Kommentar:			
2.	b) formulera, granska och godkänna informationssäkerhetspolicyn; Kommentar:			
3.	c) granska verkan av att införa informationssäkerhetspolicyn; Kommentar:			
4.	d) tillhandahålla tydlig riktning och synligt ledningsstöd för säkerhetsinitiativ Bevisas genom: Visa exempel på sådant stöd. Kommentar:			
5.	d) tillgodose behovet av resurser för informationssäkerhet; Kommentar:			
6.	e) godkänna tillsättning av särskilda roller och ansvar för informationssäkerhet inom hela organisationen; Kommentar:			
7.	f) initiera planer och program för att vidmakthålla medvetenhet om informationssäkerheten; Kommentar:			
8.	g) säkerställa att införandet av åtgärder för informationssäkerhet samordnas i hela organisationen (se 6.1.2). Kommentar:			
9.	Ledningen bör identifiera behov av intern eller extern specialist rådgivning om informationssäkerhet, samt granska och samordna resultaten av rådgivning i hela organisationen. Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
10.	Beroende på organisationens storlek kan sådant ansvar hanteras av en särskilt inrättat ledningsgrupp eller av ett existerande ledningsorgan, t.ex. styrelsen. Kommentar:			

Övrig information
Ytterligare information finns i ISO/IEC 13335-1:2004.

6.1.2 Samordning av informationssäkerhetsarbetet

Aktiviteter som rör informationssäkerhet bör samordnas av representanter från olika delar av organisationen med relevanta roller och arbetsuppgifter. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Dålig samordning av aktiviteter inom säkerhetsarbetet kan leda till ineffektivitet eller säkerhetsluckor – till exempel att risker förbises eller hanteras felaktigt.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Samordning av informationssäkerhet bör vanligen omfatta samverkan och samarbete mellan chefer, användare, administratörer, systemerare, revisorer och säkerhetspersonal, liksom även med specialister inom områden som försäkring, juridik, personalfrågor, IT eller riskhantering. Kommentar:			
2.	Denna aktivitet bör: a) säkerställa att säkerhetsaktiviteter utförs i enlighet med informationssäkerhetspolicyn; Kommentar:			
3.	b) bestämma hur fall av bristande efterlevnad skall hanteras;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	c) Godkänna metoder och processer för informationssäkerhet, t.ex. riskbedömning, informationsklassificering; Kommentar:			
5.	d) Identifiera viktiga ändringar av hotbilden och informationens och informationsbehandlingsresursernas utsatthet för hot; Kommentar:			
6.	e) bedöma lämpligheten och samordna införande av åtgärder för informationssäkerhet; Kommentar:			
7.	f) kraftfullt främja utbildning, praktisk övning och medvetande om informationssäkerheten inom hela organisationen; Kommentar:			
8.	g) bedöma information från övervakning och granskning av informationssäkerhetsincidenter och rekommendera lämpliga åtgärder för att hantera identifierade informationssäkerhetsincidenter. Kommentar			
9.	Om organisationen inte använder en särskild tvärfunktionell grupp, t.ex. för att en sådan grupp inte är lämplig med hänsyn till organisationens storlek, bör de åtgärder som beskrivs ovan vidtagas av annat lämpligt ledningsorgan eller en enskild chef. Kommentar:			

6.1.3 Tilldelning av ansvar för informationssäkerhet

Allt informationssäkerhetsansvar bör vara klart definierat. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan en tydlig ansvarsfördelning ökar risken att en uppgift lämnas därhän i tron att någon annan bär ansvaret.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Tilldelning av ansvar för informationssäkerheten bör ske i enlighet med informationssäkerhetspolicyn (se avsnitt 4). Kommentar:			
2.	Ansvar för skydd av enskilda tillgångar och för att utföra särskilda säkerhetsprocesser bör anges tydligt. Kommentar:			
3.	Där så är nödvändigt bör detta ansvar kompletteras med mer detaljerad vägledning som avser särskilda enheter och informationsbehandlingsresurser. Lokalt ansvar för skydd av tillgångar och för att utföra särskilda säkerhetsprocesser, som t.ex. kontinuitetsplanering, bör definieras tydligt. Kommentar:			
4.	Personer med tilldelat säkerhetsansvar kan delegera säkerhetsuppgifter till andra. Icke desto mindre förblir de ansvariga och bör avgöra om delegerade uppgifter har utförts korrekt. Kommentar:			
5.	De områden för vilka personer är ansvariga bör tydligt anges; särskilt bör följande ske: a) tillgångar och säkerhetsrutiner inom varje separat system bör identifieras och definieras tydligt; Kommentar:			
6.	b) för varje tillgång eller säkerhetsrutin bör ansvarig enhet utses och detaljerna i detta ansvar bör dokumenteras (se också 7.1.2); Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	c) behörighetsnivåer bör tydligt definieras och dokumenteras. Kommentar:			

Övrig information

I många organisationer kommer en informationssäkerhetschef eller motsvarande benämning att utses för att ta övergripande ansvar för utveckling och införande av säkerhet och för att ge stöd vid identifieringen av säkerhetsåtgärder.

Ansvar för att anskaffa resurser till och införa säkerhetsåtgärderna stannar emellertid ofta hos individuella chefer. Vanligt är att utse en ägare till varje tillgång som då blir ansvarig för dess dagliga skydd.

6.1.4 Godkännandeprocess för informationsbehandlingsresurser

En driftsgodkännandeprocess för nya informationsbehandlingsresurser bör definieras och införas. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan fungerande processer för driftsgodkännande finns risken att nya IT-resurser inte harmoniserar med verksamhetens behov, att de medför nya eller ökade risker, eller att kostnaden för systemintegration ökar.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer bör övervägas för driftsgodkännandeprocessen: a) Nya resurser bör godkännas genom ett ledningsbeslut i verksamheten som godkänner deras syfte och användning. Godkännande bör också inhämtas från den chef som är ansvarig för informationssäkerheten i den lokala systemmiljön, för att säkerställa att alla relevanta säkerhetspolicyer och krav är uppfyllda; Kommentar:			
2.	b) Där det är nödvändigt bör hård- och programvara kontrolleras för att säkerställa att de är kompatibla med andra systemkomponenter; Kommentar:			
3.	c) Personligt eller privat ägd informationsbehandlingsresurser, t.ex. bärbara datorer, hemdatorer eller handburna apparater som används för organisationens databehandling kan medföra nya sårbarheter. Erforderliga säkerhetsåtgärder bör identifieras och införas. Kommentar:			

6.1.6 Konfidentialitetsavtal

Krav på konfidentialitetsavtal eller överenskommelser om icke-avslöjande som speglar organisationens behov av skydd för information skall fastställas och regelbundet granskas. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfällig hantering av säkerhetsfrågor i avtal och överenskommelser kan leda till att tredje part inte arbetar enligt organisationens säkerhetskrav.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Konfidentialitetsavtal eller överenskommelser om icke-avslöjande bör behandla kravet att skydda konfidentiell information med användning av juridiskt tillämpliga villkor. Kommentar:			
2.	Konfidentialitetsavtal eller överenskommelser om icke-avslöjande bör behandla kravet att skydda konfidentiell information med användning av juridiskt tillämpliga villkor. Kommentar:			
3.	För att identifiera kraven på konfidentialitetsavtal eller överenskommelser om icke-avslöjande, bör följande delar övervägas: a) En definition av den information som skall skyddas (t.ex. konfidentiell information); Kommentar:			
4.	b) Förväntad varaktighet för ett avtal inklusive fall där konfidentialitet kan behöva bibehållas under obegränsad tid; Kommentar:			
5.	c) åtgärder som krävs när ett avtal upphör; Kommentar:			
6.	d) den undertecknandes ansvar och åtgärder för att undvika otillåtet avslöjande av information (såsom ”behöver känna till”); Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	e) ägandet till informationen, affärshemligheter och upphovsrätt och hur detta sammanhänger med skyddet av konfidentiell information; Kommentar:			
8.	f) tillåten användning av konfidentiell information och signatärernas rätt att använda den; Kommentar:			
9.	g) rätten att revidera och övervaka aktiviteter som innefattar konfidentiell information; Kommentar:			
10.	h) rutin för anmälan och rapportering av obehörigt avslöjande eller avvikelse från konfidentialitetskrav; Kommentar:			
11.	i) villkor för att återsända eller förstöra information när avtal upphör; Kommentar:			
12.	j) förväntade åtgärder om ett avtal bryts. Kommentar:			
13.	Beroende på en organisations säkerhetskrav kan andra villkor behövas i ett konfidentialitetsavtal eller avtal om icke-avslöjande. Kommentar:			
14.	Konfidentialitetsavtal och avtal om icke-avslöjande bör överensstämma med alla tillämpliga lagar och föreskrifter inom den jurisdiktion där avtalen tillämpas (se också 15.1.1). Kommentar:			
15.	Krav på konfidentialitetsavtal och avtal om icke-avslöjande bör granskas periodiskt och när ändringar sker som påverkar dessa krav.			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			

Övrig information

Konfidentialitetsavtal eller avtal om icke-avslöjande skyddar organisationens information och upplyser signatärer om deras ansvar när det gäller att skydda, använda och sprida information på ett ansvarsfullt och godkänt sätt.

Det kan finnas ett behov för en organisation att använda olika former av konfidentialitetsavtal eller avtal om icke-avslöjande vid olika omständigheter.

6.1.7 Myndighetskontakt

Lämpliga kontakter bör upprätthållas med relevanta myndigheter. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan lämpliga kontakter med relevanta myndigheter försämras förmågan att hantera incidenter och angrepp (både fysiska och elektroniska), ansvarsskyldigheten ökar och effekten av kontinuitetsplanering minskar.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Organisationer bör ha rutiner som klargör när och av vem olika myndigheter (t.ex. polis, brandkår, tillsynsmyndigheter) bör kontaktas och hur identifierade informationssäkerhetsincidenter bör rapporteras på lämpligt sätt vid misstanke om att lagbrott kan ha skett. Kommentar:			
2.	Organisationer som angrips från Internet kan behöva utomstående part (t.ex. en Internettjänst-leverantör eller teleoperatör) för att vidta åtgärder mot angreppets källa. Kommentar:			

Övrig information

Att upprätthålla sådana kontakter kan vara ett krav som stöd för incidenthantering (Avsnitt 13.2) eller kontinuitets- och katastrofplaneringen (Avsnitt 14). Kontakter med föreskrivande myndigheter är också värdefulla för att förutse och förbereda för kommande ändringar i författningar som organisationen måste följa. Kontakter med andra myndigheter omfattar affärsdrivande verk, kris- och räddningsmyndigheter, och myndigheter för hälsa och säkerhet, t.ex. brandkår (rörande verksamhetens kontinuitet), teleoperatörer (för linjedragning och tillgänglighet) och vattenuppdragstagare (för kylanläggningar för utrustning).

6.1.8 Kontakt med särskilda intressegrupper

Lämpliga kontakter bör upprätthållas med särskilda intressegrupper eller andra forum och yrkesorganisationer för säkerhetsspecialister. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Att arbeta isolerat kan leda till ineffektiva ("uppfinna hjulet på nytt") och dåligt utformade (omedvetenhet av "best practice") säkerhetsåtgärder och ineffektiv administration.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Medlemskap i särskilda intressegrupper eller forum bör övervägas som ett medel att: a) Förbättra kunskapen om bästa praxis och för att hålla sig uppdaterad om relevant säkerhetsinformation; Kommentar:			
2.	b) Försäkra sig om att förståelsen av informationssäkerhetsmiljön är aktuell och fullständig; Kommentar:			
3.	c) Få tidiga varningar om larm, samt råd och programändringar avseende attacker och sårbarhet; Kommentar:			
4.	d) Få tillgång till specialistråd i informationssäkerhetsfrågor; Kommentar:			
5.	e) Få och utbyta information om nya tekniker, produkter, hot eller sårbarheter; Kommentar:			
6.	f) Informera om lämpliga kontakter vid behandling av informationssäkerhetsincidenter (se också 13.2.1). Kommentar:			

Övrig information

Överenskommelser om utbyte av information kan upprättas för att förbättra samarbete och samordning i informationssäkerhetsfrågor. Sådana överenskommelser bör identifiera kraven för skydd av känslig information.

6.1.9 Oberoende granskning av informationssäkerhet

Organisationens metod för att hantera informationssäkerhet och dess tillämpning (t.ex. åtgärdsmål, säkerhetsåtgärder, policyer, processer och rutiner för informationssäkerhet) bör granskas oberoende med planerade mellanrum eller när det inträffar väsentliga förändringar som berör tillämpningen av säkerheten. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan oberoende granskningar riskerar organisationen att fastna i gamla tankebanor, och därmed missa väsentliga brister i informationssäkerhetsarbetet.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Den oberoende granskningen bör initieras av ledningen. Kommentar:			
2.	En sådan oberoende granskning är nödvändig för att säkerställa fortsatt lämplighet, tillräcklighet och verkan i organisationens sätt att hantera informationssäkerhet. Kommentar:			
3.	Granskningen bör omfatta bedömning av möjligheter till förbättringar och behovet av förändringar i sättet att hantera säkerhet inklusive policyn och åtgärdsmålen. Kommentar:			
4.	En sådan granskning bör utföras av personer som är oberoende av det granskade området, t.ex. internrevisionen, en oberoende chef eller en tredjeparts organisation som är specialiserad på sådana granskningar. Kommentar:			
5.	Personer som utför dessa granskningar bör ha lämplig kunskap och erfarenhet. Kommmentar:			
6.	Resultatet av den oberoende granskningen bör dokumenteras och rapporteras till ledningen som initierade granskningen. Dokumentationen bör bevaras. Kommentar:			
7.	Om den oberoende granskningen visar att organisationens sätt att hantera och tillämpa informationssäkerheten är otillräcklig eller			

Nivåstyrande frågor		JA	NEJ	VET EJ
	inte i enlighet med direktiven för informationssäkerhet i informationssäkerhetspolicyn (se 5.1.1) bör ledningen överväga korrigerande åtgärder. Kommentar:			

Övrig information
Det område som chefer bör granska regelbundet (se 15.2.1) bör också få en oberoende granskning. Granskning kan ske genom intervjuer av ledningen, kontroll av redovisande dokument eller granskning av säkerhetspolicydokument. SS-EN ISO 19011 (2002), Vägledning för revision av kvalitets- och/eller miljöledningssystem, kan också ge värdefull vägledning för att utföra oberoende granskning inklusive att upprätta och genomföra ett granskningsprogram. Avsnitt 15.3 anger åtgärder som är relevanta för den oberoende granskningen av informationssystem i drift och användningen av systemrevisionsverktyg.

6.2 Utomstående parter

Mål: Att bibehålla säkerheten hos organisationens information och informationsbehandlingsresurser som är åtkomliga för, bearbetas av, kommuniceras till eller hanteras av utomstående parter.

Säkerheten hos organisationens information och informationsbehandlingsresurser bör inte minskas genom introduktion av utomstående parters produkter eller tjänster.

All åtkomst till organisationens informationsbehandlingsresurser liksom utomståendes bearbetning och kommunikation av information bör styras.

Där verksamhetsbehov finns för att arbeta med utomstående parter som kan kräva åtkomst till organisationens information och informationsbehandlingsresurser eller att erhålla eller lämna en produkt eller tjänst från eller till en utomstående part, bör en riskbedömning göras. Riskbedömningen görs för att avgöra säkerhetskonsekvenser och behov av styrning. Säkerhetsåtgärder bör överenskommas och definieras i en överenskommelse med den utomstående parten.

6.2.1 Identifiering av risker med utomstående parter

Riskerna för organisationens information och informationsbehandlingsresurser i verksamhetsprocesser där utomstående parter är involverade bör identifieras och lämpliga säkerhetsåtgärder införas innan åtkomst beviljas. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan skyddsåtgärder specifikt inriktade mot arbete med utomstående parter, ökar risken att utomstående part (omedvetet eller avsiktligt) avslöjar, ändrar eller förlorar kritisk information eller informationsbehandlingsresurser.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Där det finns behov av att tillåta en utomstående part att ha åtkomst till informationsbehandlingsresurser eller information i en organisation bör en riskbedömning (se även avsnitt 4) utföras för att identifiera eventuella krav på särskilda säkerhetsåtgärder. Kommentar:			
2.	Vid identifieringen av risker vid utomståendes åtkomst bör följande faktorer beaktas: a) de informationsbehandlingsresurser som den utomstående parten behöver få åtkomst till; Kommentar:			
3.	b) den typ av åtkomst som den utomstående kommer att ha till information och informationsbehandlingsresurser, t.ex. 1) fysisk åtkomst, t.ex. till kontorsutrymmen, datorrum, arkiv; 2) logisk åtkomst, t.ex. till en organisations databaser, informationssystem; 3) nätverkskoppling mellan organisationens och den utomstående partens nätverk, t.ex. permanent uppkoppling, fjärråtkomst; 4) om åtkomsten äger rum inom eller utanför organisationens lokaler; Kommentar:			
4.	c) den berörda informationens värde och känslighet samt hur kritisk den är för organisationens verksamhet; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	d) de säkerhetsåtgärder som är nödvändiga för att skydda information som inte avses vara åtkomlig för utomstående parter; Kommentar:			
6.	e) den personal från den utomstående parten som deltar i hanteringen av organisationens information; Kommentar:			
7.	f) hur organisationen eller den personal som är behörig att ha åtkomst kan identifieras, att behörigheten verifieras och hur ofta detta behöver bekräftas på nytt: Kommentar:			
8.	g) de olika metoder och åtgärder som används av den utomstående parten för att lagra, bearbeta, kommunicera, dela och utbyta information; Kommentar:			
9.	h) betydelsen av att åtkomst inte är tillgänglig för den utomstående parten när den behövs liksom när den utomstående parten för in eller tar emot felaktig eller vilseledande information; Kommentar:			
10.	i) praxis och rutiner för att hantera informationssäkerhetsincidenter och tänkbara skador liksom villkor och förutsättningar för den utomstående partens fortsatta åtkomst om en informationssäkerhetsincident inträffar; Kommentar:			
11.	j) krav i författningar och andra avtal som är relevanta för den utomstående parten vilka bör beaktas; Kommentar:			
12.	k) hur andra intressenters intressen kan påverkas av arrangemangen. Kommentar:			
13.	Utomstående parts åtkomst till organisationens information bör inte medges förrän lämpliga säkerhetsåtgärder har införts och, där			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	så är möjligt, ett avtal har undertecknats som definierar villkor och förutsättningar för uppkoppling eller åtkomst och hur arbetet bör ordnas. Kommentar:			
14.	Generellt bör alla säkerhetskrav som är resultatet av arbetet med utomstående parter eller interna säkerhetsåtgärder återspeglas i avtalet med den utomstående parten (se också 6.2.2 och 6.2.3). Kommentar:			
15.	Det bör säkerställas att den utomstående parten är medveten om sina skyldigheter och accepterar ansvar och skyldigheter vid åtkomst, bearbetning, kommunikation eller annan hantering av organisationens information och informationsbehandlingsresurser. Kommentar:			

Övrig information

Information kan utsättas för risk från utomstående part som har otillräcklig styrning av säkerheten. Säkerhetsåtgärder bör identifieras och tillämpas för att administrera utomstående parts åtkomst till informationsbehandlingsresurser. Om det exempelvis finns ett särskilt behov av att vidmakthålla informationens konfidentialitet kan avtal om icke-avslöjande användas.

Organisationer kan utsättas för risker som hänger samman med inter-organisatoriska processer, hantering och kommunikation om utläggning tillämpas i stor utsträckning eller då flera utomstående parter är inblandade.

Säkerhetsåtgärderna i 6.2.2 och 6.2.3 behandlar olika arrangemang för utomstående parter inklusive t.ex.:

a) tjänsteuppdragstagare som t.ex. uppdragstagare av Internettjänster, nätverksuppdragstagare, teleoperatörer, underhålls- och serviceföretag

b) hanterade säkerhetstjänster

c) kunder

d) utläggning av resurser och/eller drift, t.ex. IT-system, datainsamlingstjänster, call center-verksamhet

e) verksamhets- och organisationskonsulter och revisorer

f) utvecklare och uppdragstagare, t.ex. av programvaruprodukter och IT-system

g) städning, catering och andra utlagda stödtjänster

h) tillfällig personal, praktikanter och andra tillfälliga korttidsengagemang.

Sådana överenskommelser kan bidra till att minska riskerna med utomstående parter.

6.2.2 Hantering av säkerhet vid kundkontakter

Alla identifierade säkerhetskrav bör behandlas innan kunder ges åtkomst till organisationens information eller andra tillgångar. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan skyddsåtgärder specifikt inriktade mot arbete med utomstående parter, ökar risken att utomstående part (omedvetet eller avsiktligt) avslöjar, ändrar eller förlorar kritisk information eller informationsbehandlingsresurser.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Med tanke på säkerheten bör följande villkor övervägas innan kunder ges åtkomst till organisationens information eller tillgångar (beroende på den tillåtna åtkomstens typ och omfattning är kanske inte alla tillämpliga): a) skydd av tillgångar, inkluderande; 1) rutiner för att skydda organisationens tillgångar inklusive information och program liksom hanteringen av kända sårbarheter; 2) rutiner för att avgöra om några tillgångar äventyrats, t.ex. förlust eller förändring av data; 3) datas riktighet; 4) begränsningar i rätten att kopiera och avslöja information; Kommentar:			
2.	b) beskrivning av den produkt eller tjänst som tillhandahålls; Kommentar:			
3.	c) de olika anledningarna, kraven och fördelarna med kunders åtkomst; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
4.	d) åtkomstpolicy som täcker: 1) tillåtna åtkomstmetoder, samt styrning och användning av unika identifieringsbegrepp såsom användar-ID och lösenord; 2) en behörighetsrutin för användaråtkomst och rättigheter; 3) ett uttalande om att all åtkomst som inte uttryckligt är godkänd är förbjuden; 4) en process för att återkalla åtkomsträtt eller för att avbryta kopplingen mellan system Kommentar:			
5.	e) rutiner för rapportering, anmälan och undersökning av oriktigheter i informationen (t.ex. i personuppgifter), informationssäkerhetsincidenter och brott mot säkerheten; Kommentar:			
6.	f) en beskrivning av alla tjänster som görs tillgängliga; Kommentar:			
7.	g) avsedd tjänstenivå och oacceptabel tjänstenivå; Kommentar:			
8.	h) rätten att övervaka och avbryta varje aktivitet relaterad till organisationens tillgångar; Kommentar:			
9.	i) organisationens och kunders respektive skyldigheter; Kommentar:			
10.	j) ansvar med avseende på juridiska förhållanden och hur det säkerställs att de legala kraven tillgodoses, t.ex. skydd av personuppgifter, med särskild hänsyn till olika nationella juridiska system om överenskommelsen omfattar samarbete med kunder i andra länder (se också 15.1); Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
11.	k) immateriella rättigheter (IPR) och upphovsrättsliga villkor (se 15.1.2) samt skydd av resultatet av samarbete (se 6.2.1). Kommentar:			

Övrig information

De säkerhetskrav som rör kunders åtkomst till organisationens tillgångar kan variera avsevärt beroende på informationsbehandlingsresurserna och den information som åtkomsten avser. Dessa säkerhetskrav kan anges i kundavtal som omfattar alla identifierade risker och säkerhetskrav (se 6.2.1).

Avtal med utomstående parter kan också beröra andra parter. Avtal som ger utomstående part åtkomst bör omfatta utrymme för att utse andra lämpliga parter och villkor för deras åtkomst och engagemang.

6.2.3 Hantering av säkerhet i tredje partsavtal

Avtal med en tredje part omfattande åtkomst, bearbetning, kommunikation och hantering av organisationens information eller informationsbehandlingsresurser alternativt tillägg av produkter eller tjänster till informationsbehandlingsresurserna bör omfatta alla relevanta säkerhetskrav. *Kritisk säkerhetsåtgärd: JA* *Risk: Om avtal och överenskommelser skrivs utan att ta hänsyn till säkerhetsfrågor ökar risken för att tjänster från tredje part inte utförs i enlighet med säkerhetskraven.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Avtalet bör säkerställa att inget missförstånd finns mellan organisationen och den tredje parten. Kommentar:			
2.	Organisationen bör försäkra sig om skadeslöshet gentemot tredje part. Kommentar:			
3.	Följande villkor bör man överväga att införa i avtalet för att uppfylla de identifierade säkerhetskraven (se 6.2.1): a) informationssäkerhetspolicyn; Kommentar:			
4.	b) Säkerhetsåtgärder för att säkerställa skydd av tillgångar: 1) rutiner för att skydda organisationens tillgångar inklusive information, mjukvara och hårdvara 2) erforderliga säkerhetsåtgärder och mekanismer för fysiskt skydd 3) säkerhetsåtgärder för att säkerställa skydd mot skadlig programvara 4) rutiner för att avgöra om några tillgångar har äventyrats, t.ex. förlust eller förändring av information, mjuk- eller hårdvara 5) säkerhetsåtgärder för att säkerställa återlämnande eller förstöring av information och andra tillgångar vid slutet av, eller vid en överenskommen tid under perioden 6) konfidentialitet, riktighet, tillgänglighet och eventuell annan			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	relevant egenskap (se 2.1.5) hos tillgången 7) restriktioner för att kopiera och avslöja information samt användning av konfidentialitetsavtal (se 6.1.5) 8) Kommentar:			
5.	c) utbildning för användare och administratör i metoder, rutiner och säkerhet; Kommentar:			
6.	d) tillförsäkra att användare är medvetna om ansvar och regler för informationssäkerhet; Kommentar:			
7.	e) i förekommande fall bestämmelser för placering av personal; Kommentar:			
8.	f) ansvarsfördelning för installation och underhåll av mjuk- och hårdvara; Kommentar:			
9.	g) tydlig rapporteringsstruktur och -format; Kommentar:			
10.	h) En tydlig och detaljerad rutin för hantering av ändrings hantering; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
11.	i) policy för åtkomststyrning som omfattar: 1) de olika skäl, krav och fördelar som gör tredje partens åtkomst nödvändig 2) tillåtna åtkomstmetoder samt styrning och användning av identifieringsbegrepp såsom användar-ID och lösenord 3) en behörighetsprocess för användaråtkomst och rättigheter 4) ett krav på att föra en förteckning över personer med behörighet att nyttja tillgängliga tjänster och deras rättigheter och privilegier med avseende på sådan användning 5) ett uttalande om att all åtkomst som inte är uttryckligt godkänd är förbjuden 6) en process för att återkalla åtkomsträtt eller avbryta uppkoppling mellan system; Kommentar:			
12.	j) arrangemang för att rapportera, identifiera och utreda informationssäkerhetsincidenter och säkerhetsförluster liksom även brott mot avtalade krav; Kommentar:			
13.	k) en beskrivning av den produkt eller tjänst som skall tillhandahållas och en beskrivning av den information som behöver göras tillgänglig inklusive dess säkerhetsklassificering (se 7.2.1); Kommentar:			
14.	l) mål i fråga om tjänstenivå och oacceptabel tjänstenivå; Kommentar:			
15.	m) definition av verifierbara prestationskrav och deras uppföljning och rapportering; Kommentar:			
16.	n) rätten att övervaka och återkalla alla aktiviteter som rör organisationens tillgångar; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
17.	o) rätten att genomföra revision av ansvar som angavs i avtalet, att låta tredje part utföra sådana revisioner och att nämna revisorers stadgeenliga rättigheter; Kommentar:			
18.	p) fastställande av eskaleringsmetod för problemlösning; Kommentar:			
19.	q) krav på tjänstekontinuitet inklusive mått på tillgänglighet och tillförlitlighet i enlighet med organisationens verksamhetsprioriteter; Kommentar:			
20.	r) parternas respektive skyldigheter enligt avtal; Kommentar:			
21.	s) ansvar med avseende på juridiska förhållanden och hur det säkerställs att de legala kraven tillgodoses, t.ex. persondataskydd med särskild hänsyn till olika nationella juridiska system om avtalet omfattar samarbete med kunder i andra länder (se också 15.1); Kommentar:			
22.	t) immateriella rättigheter (IPR) och upphovsrättsliga villkor (se 15.1.2) samt skydd av resultatet av eventuellt samarbete; Kommentar:			
23.	u) utomstående parts samverkan med underuppdragstagare och de säkerhetsåtgärder dessa underuppdragstagare behöver införa; Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
24.	v) villkor för omförhandling/avslut av avtal: 1) en kontinuitetsplan bör finnas ifall endera parten önskar avbryta samarbetet innan avtalet går ut; 2) omförhandling av avtalet om organisationens säkerhetskrav förändras; 3) aktuell dokumentation över tillgångar, licenser, avtal eller rättigheter som hör till dem. Kommentar:			

Övrig information

Avtalen kan variera avsevärt för olika organisationer och för olika kategorier av tredje parter. Noggrannhet bör därför iakttas så att alla identifierade risker och säkerhetskrav (se också 6.2.1) inkluderas i avtalen. Där så är nödvändigt kan den styrning och de rutiner som krävs utvecklas i en handlingsplan för säkerhet.

Om hanteringen av informationssäkerhet är utlagd bör avtalen ta upp frågan hur den tredje parten kommer att garantera att adekvat säkerhet upprätthålls, så som definierad utifrån riskbedömningen, och hur säkerheten kommer att anpassas för att identifiera och bemöta förändrade risker.

Vissa av skillnaderna mellan utläggning och de andra formerna av tjänster som tredje part erbjuder omfattar frågan om ansvar, planering av övergångsperioden och tänkbar störning av driften under denna period, arrangemang för kontinuitetsplanering och planerade granskningar samt insamling och hantering av information om säkerhetsincidenter. Det är därför viktigt att organisationen planerar och hanterar övergången till en lösning som innebär utläggning och har utvecklat lämpliga rutiner för att hantera ändringar och omförhandling/avslut av avtal.

I den händelse att den tredje parten inte klarar av att leverera sina tjänster behöver avtalet beakta rutinerna för att utan förseningar kunna anskaffa ersättningstjänster för fortsatt verksamhet.

Avtal med tredje part kan också involvera ytterligare parter. Avtal som ger tredje part åtkomst bör omfatta möjlighet att utse andra lämpliga parter och villkoren för deras åtkomst och medverkan.

I allmänhet utformas avtal i huvudsak av organisationen. Det kan finnas tillfällen under vissa omständigheter då ett avtal kan utformas och åläggs en organisation av en tredje part. Organisationen behöver säkerställa att dess egen säkerhet inte i onödan påverkas av tredje parts krav i ålagda avtal.

7. Hantering av tillgångar

7.1 Ansvar för tillgångar

Mål: Att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar.

Alla tillgångar bör redovisas och ha en utsedd ägare.

Ägare bör fastställas för alla tillgångar och ansvaret för underhåll av lämpliga säkerhetsåtgärder bör tilldelas. Införandet av specifika säkerhetsåtgärder kan delegeras av ägaren om lämpligt, men ägaren förblir ansvarig för att tillgångarna ges rätt skydd.

7.1.1 Förteckning över tillgångar

Alla tillgångar bör tydligt märkas och en förteckning omfattande alla viktiga tillgångar bör upprättas och underhållas. *Kritisk säkerhetsåtgärd: JA* *Risk: Bristfällig hantering av tillgångar ökar risken för produktionsfel vilket i sin tur påverkar driftsäkerheten (till exempel på grund av otillräcklig konsekvensanalys eller förbisedda komponenter under uppgraderingar). Arbetet med att återställa informationshanteringsresurser efter allvarliga incidenter blir också dyrare och mer omfattande om inte tillgångarna hanteras korrekt.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	En organisation bör identifiera alla tillgångar och dokumentera betydelsen av dessa tillgångar. Kommentar:			
2.	Förteckningen över tillgångar bör omfatta all information som är nödvändig för återhämtning efter en katastrof, inklusive typ av tillgång, format, placering, information om säkerhetskopiering, licensinformation och värdet för organisationen. Kommentar:			
3.	Förteckningen bör inte dubblera andra förteckningar i onödan men			

Nivåstyrande frågor		JA	NEJ	VET EJ
	överensstämmelse mellan förteckningar bör säkerställas. Kommentar:			
4.	Dessutom bör ägande (se 7.1.2) och informationsklassning (se 7.2) bestämmas och dokumenteras för varje tillgång. Kommentar:			
5.	Skyddsnivå i överensstämmelse med tillgångens vikt bör bestämmas på grundval av tillgångens betydelse, dess värde för organisationen och dess säkerhetsklassning (mer information om hur tillgångar värderas i enlighet med dess betydelse finns i ISO/IEC TR 13335-3). Kommentar:			

Övrig information

Det finns många typer av tillgångar, inklusive:

a) information: databaser och datafiler, avtal och överenskommelser, systemdokumentation, forskningsinformation, användarmanualer, utbildningsmaterial, drift- och stödrutiner, organisationens kontinuitetsplaner, nödrutiner, revisionsspår och arkiverad information

b) programvarutillgångar: tillämpningsprogram, systemprogram, utvecklingsverktyg och stödprogram

c) fysiska tillgångar: datorutrustning, kommunikationsutrustning, flyttbara datamedia och annan utrustning

d) tjänster: data- och kommunikationstjänster, försörjningssystem för t.ex. värme, ljus, elkraft och luftkonditionering

e) personal och deras kvalifikationer, talanger och erfarenhet

f) immateriella, såsom organisationens rykte och profil.

Förteckning över tillgångar bidrar till att säkerställa effektivt skydd av tillgångarna och kan också krävas av andra skäl såsom hälsa och säkerhet, eller av försäkrings- eller finansiella orsaker (hantering av tillgångar). Arbetet att upprätta en förteckning över tillgångar är en viktig förutsättning för riskhantering (se också avsnitt 4).

7.1.2 Ägarskap för tillgångar

All information och tillgångar tillhörandes informationsbehandlingsresurserna bör ägas[1] av en utsedd organisationsenhet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Otydlighet i ägandefrågan innebär en otydlig ansvarsfördelning. Detta kan innebära att viktiga uppgifter inte utförs i tron att någon annan bär ansvaret.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Tillgångens ägare bör ansvara för: a) att säkerställa att information och tillgångar som utgör informationsbehandlingsresurser är riktigt klassade; Kommentar:			
2.	b) att definiera och periodiskt granska åtkomstbegränsningar och klassning och därvid ta hänsyn till tillämpliga åtkomstpolicyer. Kommentar:			
3.	Ägandet kan gälla: a) en verksamhetsprocess; Kommentar:			
4.	b) en definierad uppsättning aktiviteter; Kommentar:			
5.	c) en tillämpning; Kommentar:			

[1] Termen ”ägare” identifierar en individ eller enhet som har godkänt ledningsansvaret för att styra produktion, utveckling, underhåll, användning och säkerhet hos tillgången. Termen ”ägare” betyder inte att personen har någon personlig äganderätt till tillgången.

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	d) en definierad datamängd. Kommentar:			

Övrig information
Rutinuppgifter kan delegeras, t.ex. till en person som ser efter tillgången dagligen men ansvaret stannar hos ägaren.

I komplexa informationssystem kan det vara lämpligt att utse en grupp tillgångar vilka tillsammans står för en viss funktion såsom ”tjänster”. I detta fall är tjänsteägaren ansvarig för att leverera tjänsten, inklusive funktionen hos de tillgångar som utför den.

7.1.3 Godtagbar användning av tillgångar

	Nivå
Regler för hur information och tillgångar tillhörandes informationsbehandlingsresurser får användas bör utformas, dokumenteras och införas. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan tydliga riktlinjer för hantering av användartillgångar (och i enlighet med partner) finns det risk för att känslig information behandlas/hanteras annorlunda, och eventuellt felaktigt av partner/medarbetare (t.ex. känslig information skickas via Internet, eller lagras oskyddade på mobila enheter).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Alla anställda, uppdragstagare och tredjeparts användare bör följa regler för hur information och tillgångar som tillhör informationsbehandlingsresurser får användas, inklusive; a) regler för e-post och Internetanvändning (se 10.8) Kommentar:			
2.	b) riktlinjer för användning av mobila enheter, särskilt för användningen utanför organisationens lokaler (se 11.7.1). Kommentar:			
3.	Specifika regler eller vägledning bör ges av berörda chefer. Anställda, uppdragstagare och tredjepartsanvändare som använder eller har åtkomst till organisationens tillgångar bör vara medvetna om gällande begränsningar vid sin användning av organisationens information och de tillgångar som hör till informationsbehandlingsresurser och andra resurser. De bör ha ansvar för sin egen användning av informationsbehandlingsresurser och för all annan användning som utförs under deras ansvar. Kommentar:			

7.1.4 Klassificering av information

Mål: Att säkerställa att information erhåller en lämplig skyddsnivå.

Information bör klassificeras för att indikera behovet, prioritet och förväntad skyddsnivå vid hantering av informationen.

Information är i varierande grad känslig och kritisk. Vissa tillgångar kan behöva utökat skydd eller speciell hantering. En informationsklassificeringsmodell bör användas för att definiera en lämplig uppsättning skyddsnivåer och kommunicera behov av särskilda åtgärder vid hantering.

7.1.5 Riktlinjer för klassificering

	Nivå
Information bör klassificeras i termer av dess värde, legala krav, känslighet och betydelse för organisationen. *Kritisk säkerhetsåtgärd: JA* *Risk: Otydliga riktlinjer för klassificering av information ökar risken för under- eller överklassificering, vilket senare kan leda till spridning av känsliga uppgifter eller att tillgången på information försämras.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Klassificering och tillhörande skyddande säkerhetsåtgärder för information bör ta hänsyn till verksamhetens behov av att dela eller begränsa information och den påverkan på verksamheten sådana behov ger upphov till. Kommentar:			
2.	Vägledning för klassificering bör omfatta regler för en första klassificering och omklassificering över tid i enlighet med en förbestämd policy för åtkomstkontroll (se 11.1.1). Kommentar:			
3.	Tillgångens ägare (se 7.1.2) bör ansvara för att fastställa klassificeringen av en tillgång, periodiskt granska den, och säkerställa att den hålls aktuell och på lämplig nivå. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
4.	Klassificeringen bör ta hänsyn till den ackumuleringseffekt som nämns i 10.7.2. Kommentar:			
5.	Antalet klassificeringskategorier bör övervägas och de fördelar som kan uppnås genom att använda dem. Kommentar:			
6.	Alltför komplexa system kan bli betungande och oekonomiska att tillämpa eller visa sig opraktiska. Kommentar:			
7.	Försiktighet bör iakttas vid tolkning av klassificeringsmärkning på dokument från andra organisationer som kan ha olika definitioner för samma eller likartat utformad märkning. Kommentar:			

Övrig information
Skyddsnivån kan bedömas genom analys av konfidentialitet, riktighet och tillgänglighet samt andra eventuella krav på den aktuella informationen.

Information är ofta inte längre känslig eller kritisk efter en viss tid, t.ex. när informationen har offentliggjorts. Hänsyn bör tas till dessa synpunkter eftersom överklassificering kan leda till införande av onödiga åtgärder som medför ytterligare kostnader.

Att bedöma dokument med liknande säkerhetskrav tillsammans när klassificeringsnivåer åsätts kan förenkla klassificeringsarbetet.

I allmänhet är klassificeringen av information en genväg till att avgöra hur informationen bör hanteras och skyddas.

7.1.6 Märkning och hantering av information

	Nivå
En lämplig uppsättning rutiner för märkning och hantering av information bör utvecklas och införas i enlighet med det klassificeringssystem som antagits av organisationen. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Med obefintliga (eller ineffektiva) metoder/rutiner för märkning och hantering av information, ökar risken att känslig information avslöjas. Felaktig märkning kan till exempel leda till att känsliga dokument delas ut till leverantörer.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Rutiner för märkning av information behöver omfatta informationstillgångar i fysisk och elektronisk form. Kommentar:			
2.	Utdata från system som innehåller information som är klassificerad som känslig eller kritisk bör ha en lämplig klassmärkning (i utdata). Kommentar:			
3.	Märkningen bör visa klassificeringen enligt de regler som bestämdes i 7.2.1. Kommentar:			
4.	Det som bör övervägas innefattar tryckta rapporter, skärmbilder, inspelade media (t.ex. band, diskar, CD-skivor), e-post och filöverföringar. . Kommentar:			
5.	För varje klassificeringsnivå bör det finnas rutiner gällande säker hantering vid bearbetning, lagring, överföring, avklassificering och destruering. Kommentar:			
6.	Det bör också finnas rutiner för hantering av elektronisk bevisning och loggning av eventuella händelser som är relevanta för säkerhet. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	Överenskommelser med andra organisationer, där åtkomst till information ingår, bör omfatta rutiner för att identifiera klassificeringen av sådan information och för tolkning av andra organisationers klassificeringsmärkning. Kommentar:			

Övrig information

Märkning och säker hantering av klassificerad information är ett nyckelkrav vid informationsdelning. Fysiska etiketter är en vanlig form av märkning. Emellertid kan vissa informationstillgångar såsom t.ex. dokument i elektronisk form inte märkas fysiskt och då måste elektronisk märkning användas. Märkningen kan t.ex. visas på bildskärmen. Där märkning inte är lämplig får andra sätt att ange informationsklassificeringen tillämpas, t.ex. via rutiner eller metadata.

8. Personalresurser och säkerhet

8.1 Före anställning[2]

Mål: Att säkerställa att anställda, uppdragstagare och tredjepartsanvändare förstår sitt ansvar och är lämpliga för de roller de avses ha och för att minska risken för stöld, bedrägeri eller missbruk av resurser.

Säkerhetsansvar bör klargöras före anställning i lämpliga befattningsbeskrivningar och i villkor och förutsättningar för anställningen.

Alla platssökande, uppdragstagare och tredjepartsanvändare bör kontrolleras på lämpligt sätt särskilt då det gäller känsliga arbetsuppgifter.

Anställda, uppdragstagare och tredjepartsanvändare av informationsbehandlingsresurser bör skriva under en förbindelse rörande sina säkerhetsroller och sitt ansvar.

8.1.1 Roller och ansvar

	Nivå
Anställdas, uppdragstagares och tredjepartsanvändares roller och ansvar bör definieras och dokumenteras i enlighet med organisationens informationssäkerhetspolicy. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan definierade ansvarsförhållanden uppstår risken att viktiga uppgifter inte utförs i tron att någon annan bär ansvaret.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

[2] Förklaring: Med ordet ”anställning” avses här alla följande olika situationer: anställning av personal (temporärt eller fast), tilldelning av roller i arbetet, förändring av sådana roller, tilldelning av kontrakt och avslutande av något av dessa arrangemang.

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Roller och ansvar när det gäller säkerhet bör omfatta krav att: a) tillämpas och handla i enlighet med organisationens informationssäkerhetspolicy (se 5.1); Kommentar:			
2.	b) skydda tillgångar från obehörig åtkomst, avslöjande, förändring, förstöring och störning; Kommentar:			
3.	c) utföra särskilda säkerhetsrutiner eller aktiviteter; Kommentar:			
4.	d) säkerställa att ansvar tilldelas rätt person för utförda uppgifter; Kommentar:			
5.	e) rapportera säkerhetshändelser, tänkbara händelser eller andra säkerhetsrisker till organisationen. Kommentar:			
6.	Säkerhetsroller och ansvar bör definieras och tydligt kommuniceras till platssökande under anställningsförfarandet. Kommentar:			

Övrig information

Befattningsbeskrivningar kan användas för att dokumentera säkerhetsroller och ansvar. Säkerhetsroller och ansvar för personer som inte genomgått organisationens anställningsförfarande, t.ex. anlitats via en tredjepartsorganisation, bör också tydligt definieras och kommuniceras.

8.1.2 Kontroll av personal

	Nivå
Verifiering av personens bakgrund bör göras för alla rekryteringskandidater, uppdragstagare och tredjepartsanvändare i enlighet med relevanta författningar och etiska regler. Kontrollerna bör stå i proportion till organisationens krav, klassificeringen av den information för vilken åtkomst behövs och de uppfattade riskerna. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan en noggrann verifiering av kandidatens kompetens (vilja och förmåga) att arbeta enligt organisationens krav gällande informationssäkerhet ökar risken för informationsläckage eller att information modifieras eller förstörs.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Vid verifiering av bakgrunden bör hänsyn tas till all relevant lagstiftning gällande skydd av personuppgifter och/eller anställning och bör, där så är tillåtet, innefatta: a) att tillfredsställande personliga referenser finns – t.ex. en för yrkesliv och en personlig; Kommentar:			
2.	b) en kontroll (av fullständighet och riktighet) av sökandens meritförteckning; Kommentar:			
3.	c) bekräftelse av angivna akademiska och yrkesmässiga kvalifikationer; Kommentar:			
4.	d) oberoende kontroll av identitet (ID-kort eller motsvarande); Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	e) mer detaljerade kontroller, såsom kreditupplysning eller kontroll av brottsregister. Kommentar:			
6.	I de fall en befattning, vid rekrytering eller befordran, medför att personen får tillgång till informationsbehandlingsresurser och särskilt om dessa hanterar känslig information, t.ex. ekonomisk information eller strängt konfidentiell information, bör organisationen också överväga flera och mera detaljerade kontroller. Kommentar:			
7.	Rutinerna bör definiera kriterier och begränsningar för kontroll, t.ex. vem som är kvalificerad för att kontrollera människor och hur, när och varför verifieringskontroller utförs. Kommentar:			
8.	Uppdragstagare och utomstående användare bör också genomgå en kontroll. Kommentar:			
9.	En kontrollprocess bör också genomföras för uppdragstagare och tredjepartsanvändare. Då uppdragstagare engageras genom en förmedling bör avtalet tydligt precisera förmedlingens kontrollansvar och den anmälningsrutin som måste följas om kontrollen inte har fullföljts eller om resultatet ger anledning till tvivel eller osäkerhet. Kommentar:			
10.	På samma sätt bör avtal med tredje part (se också 6.2.3) klart specificera allt ansvar och anmälningsrutiner för kontroll. Kommentar:			
11.	Information om alla kandidater som övervägs för befattningar inom organisationen bör insamlas och hanteras i enlighet med tillämplig lagstiftning inom den relevanta jurisdiktionen. Kommentar:			
12.	Beroende på tillämplig lagstiftning bör kandidaterna informeras i förväg om kontrollaktiviteterna. Kommentar:			

8.1.3 Anställningsvillkor

	Nivå
Som en del av sina avtalsskyldigheter bör anställda, uppdragstagare och tredjepartsanvändare godta och underteckna de villkor och förhållanden i anställningsavtalet som bör ange det egna och organisationens ansvar för informationssäkerhet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristande medvetenhet ökar risken att (Tredje Part) personal inte agerar i enlighet med säkerhetskrav, inklusive sekretess.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Anställningsvillkoren bör spegla organisationens säkerhetspolicy förutom att klargöra och meddela: a) att alla anställda, uppdragstagare och tredjepartsanvändare som medges åtkomst till känslig information bör underteckna ett konfidentialitetssavtal eller avtal om icke-avslöjande innan åtkomst beviljas till informationsbehandlingsresurser; Kommentar:			
2.	b) den anställdes, uppdragstagarens och tredjepartsanvändarens legala ansvar och rättigheter, t.ex. avseende upphovsrättslagar eller persondatalag (se också 15.1.1 och 15.1.2); Kommentar:			
3.	c) ansvar för den klassificering av information och hantering av organisationstillgångar i anslutning till informationssystem och tjänster som utförs av den anställde, uppdragstagaren eller tredjepartsanvändare (se också 7.2.1 och 10.7.3); Kommentar:			
4.	d) den anställdes, uppdragstagarens eller tredjepartsanvändarens ansvar för hantering av information mottagen från andra företag eller externa parter; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	e) organisationens ansvar för hanteringen av personinformation inklusive den personinformation som tillkommit som ett resultat av eller under loppet av anställning inom organisationen (se också 15.1.4); Kommentar:			
6.	f) ansvar som gäller utanför organisationens lokaler och utanför normal arbetstid, t.ex. vid hemarbete (se också 9.2.5 och 11.7.1); Kommentar:			
7.	g) åtgärder som bör vidtas om den anställde, uppdragstagare eller tredjepartsanvändare åsidosätter organisationens säkerhetskrav (se också 8.2.3). Kommentar:			
8.	Organisationen bör säkerställa att anställda, uppdragstagare och tredjepartsanvändare 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. Kommentar:			
9.	Där så är lämpligt bör ansvar som ingår i anställningsvillkoren fortsätta att gälla under en bestämd period efter anställningens slut (se också 8.3). Kommentar:			

Övrig information

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

8.2 Under anställningen

Mål: Att säkerställa att anställda, uppdragstagare och tredjepartsanvändare är medvetna om hot och problem som rör informationssäkerhet, sitt ansvar och sina skyldigheter samt är rustade för att stödja organisationens säkerhetspolicy när de utför sitt normala arbete och för att minska risken för mänskliga fel.

Ledningsansvar bör definieras för att säkerställa att säkerhet tillämpas under en persons hela anställningstid inom organisationen.

En tillräcklig nivå av medvetenhet, utbildning och övning i säkerhetsrutiner och korrekt användning av informationsbehandlingsresurser bör ges till alla anställda, uppdragstagare och tredjepartsanvändare i syfte att minimera möjliga säkerhetsrisker. Ett formellt disciplinärt förfarande för att hantera säkerhetsöverträdelser bör inrättas.

8.2.1 Ledningens ansvar

	Nivå
Ledningen bör kräva att anställda, uppdragstagare och tredjepartsanvändare tillämpar säkerhet i enlighet med organisationens beslutade policyer och rutiner. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan ett tydligt stöd från ledningen ökar risken att personalen försummar säkerheten. Säkerhet ska vara djupt inrotat i alla användares beteende. (se 6.1.1).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Ledningsansvaret bör omfatta säkerställande av att anställda, uppdragstagare och tredjepartsanvändare: a) är tillräckligt informerade om sina roller och ansvar ifråga om informationssäkerhet innan de ges åtkomst till känslig information eller informationssystem; Kommentar:			
2.	b) erhåller riktlinjer som anger säkerhetsförväntningar för deras roll inom organisationen;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
3.	c) är motiverade att uppfylla organisationens säkerhetspolicyer; Kommentar:			
4.	d) uppnår en nivå av medvetande om säkerhet som är relevant för sina roller och sitt ansvar inom organisationen (se också 8.2.2); Kommentar:			
5.	e) följer anställnings villkoren och -förhållandena, inklusive organisationens informationssäkerhetspolicy och lämpliga arbetsmetoder; Kommentar:			
6.	f) upprätthåller lämpliga färdigheter och kvalifikationer. Kommentar:			

Övrig information

Om anställda, uppdragstagare och tredjepartsanvändare inte görs medvetna om sitt säkerhetsansvar kan de orsaka avsevärd skada för en organisation. Motiverad personal kan förväntas vara mera pålitlig och orsaka färre informationssäkerhetsincidenter.

Dålig ledning kan orsaka att personal känner sig undervärderad vilket kan ge en negativ inverkan på organisationens säkerhet. Dålig ledning kan t.ex. leda till att säkerheten försummas eller till tänkbart missbruk av organisationens tillgångar.

8.2.2 Informationssäkerhetsmedvetande, utbildning och övning

	Nivå
Alla anställda i organisationen och, där det är relevant, uppdragstagare och tredjepartsanvändare bör få erforderlig utbildning och regelbunden uppdatering om organisationens policyer och rutiner som är relevanta för deras arbetsuppgifter. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan ett tydligt, aktivt stöd från ledningen är risken stor att de anställda åsidosätter säkerheten. Säkerhet ska vara djupt inrotat i alla användares beteende.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Utbildningen bör inledas med ett formell introduktionsförfarande med avsikt att introducera organisationens policies och rutiner innan åtkomst till information eller tjänster beviljas. Kommentar:			
2.	Kontinuerlig övning bör omfatta säkerhetskrav, juridiskt ansvar och organisationens säkerhetsåtgärder liksom även övning i korrekt användning av informationsbehandlingsresurser t.ex. påloggningsrutin, utnyttjande av programvarupaket och information om den disciplinära processer (se 8.2.3). Kommentar:			

Övrig information

Åtgärder som rör medvetenhet, utbildning och övning kopplat till säkerhet bör vara anpassade till och relevanta för personens roll, ansvar och kunskaper. De bör också omfatta information om kända hot, vem som ska kontaktas för ytterligare säkerhetsråd och lämpliga kanaler för att rapportera informationssäkerhetsincidenter (se också 13.1).

Praktisk övning för att öka medvetenheten är avsedd att göra det möjligt för individer att känna igen informationssäkerhetsproblem och incidenter och svara upp allt efter behoven i deras yrkesroll.

8.2.3 Disciplinär process

Det bör finnas en formell disciplinär process för anställda som har åsidosatt säkerheten. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om personalen inte hålls ansvarig för säkerhetsöverträdelser (luckor) ökar risken för fortsatta överträdelser.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Den disciplinära processen bör inte inledas utan föregående verifiering av att säkerheten verkligen har åsidosatts (se också 13.2.3 om insamling av bevis). Kommentar:			
2.	Den formella disciplinära processen bör garantera korrekt och rättvis behandling av anställda som misstänks för att åsidosatt säkerheten. Kommentar:			
3.	Den formella disciplinära processen bör ge utrymme för en skala av åtgärder som tar i beaktande faktorer som t.ex. brottets art och allvar och dess betydelse för organisationens verksamhet, om det är den första eller upprepad förseelse, om den misstänkte fått riktig utbildning, relevant lagstiftning, organisationens kontrakt och andra faktorer alltefter vad som erfordras. Kommentar:			
4.	Om det är fråga om allvarliga förseelser bör förfarandet innebära omedelbar avlägsnande från sin tjänst, åtkomsträtt och rätt till privilegierad åtkomst och, om så är nödvändigt, genast eskorteras ut ur lokalen. Kommentar:			

Övrig information
Den disciplinära processen bör också användas för att avskräcka anställda, uppdragstagare och tredjepartsanvändare från att bryta mot organisationens säkerhetspolicyer och rutiner eller utföra andra säkerhetsöverträdelser.

8.3 Upphörande eller ändring av anställning

Mål: Att säkerställa att anställda, uppdragstagare och tredjepartsanvändare lämnar organisationen eller ändrar sina anställningsförhållanden på ett ordnat sätt.

Ansvar bör definieras för hanteringen av när en anställd, uppdragstagare eller tredjepartsanvändare lämnar organisationen och för att all utrustning återlämnas och att alla åtkomsträttigheter avslutas.

Förändring av ansvar och anställning inom en organisation bör hanteras på samma sätt som upphörande av respektive ansvar och anställning, i enlighet med detta avsnitt, och nya anställningar bör handläggas som beskrivs i avsnitt 8.1..

8.3.1 Ansvar vid upphörande av anställning

	Nivå
Ansvaret för att avsluta eller förändra anställning bör vara klart definierat och fördelat. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Oklara ansvarsförhållanden i samband med uppsägning eller ändring av arbetsuppgifter innebär en ökad risk för att personal behåller sina åtkomsträttigheter, kringgår arbets- och ansvarsfördelning eller tar sig in i system utifrån.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Ansvar vid upphörande bör omfatta gällande säkerhetskrav och legalt ansvar och, där så är lämpligt, ansvar inom ramen för eventuellt konfidentialitetsavtal (se 6.1.5), samt anställningsvillkor och -förhållanden (se 8.1.3) som fortsätter under en bestämd tid efter det att den anställdes, uppdragstagarens eller tredjepartens engagemang upphört. Kommentar:			
2.	Ansvar och plikter som fortfarande gäller efter anställningens slut bör återfinnas i den anställdes, uppdragstagarens eller tredjepartsanvändarens avtal. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
3.	Förändring av ansvar eller anställning bör hanteras som upphörande av respektive ansvar eller anställning och det nya ansvaret eller anställningen bör styras i enlighet med beskrivningen i avsnitt 8.1. Kommentar:			

Övrig information

Personalavdelningen är i allmänhet ansvarig för den övergripande processen vid upphörande av anställning och arbetar tillsammans med närmsta chefen till den person som slutar. Då det gäller en uppdragstagare kan förfarandet vid upphörande av ansvaret eventuellt utföras av den förmedling som är ansvarig för uppdragstagaren, medan det för andra användare kan skötas av organisationen själv.

Det kan vara nödvändigt att informera anställda, kunder, uppdragstagare eller tredje parter om ändringar i personal- och driftförhållanden

8.3.2 Återlämnande av tillgångar

	Nivå
Alla anställda, uppdragstagare och tredjepartsanvändare bör återlämna alla organisationens tillgångar som de innehar när anställningen, avtalet eller överenskommelsen upphör. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om tillgångar inte återlämnas uppstår en risk för ekonomisk förlust, avslöjande av hemlig information och brott mot immaterialrätten.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Förfarandet då en person slutar bör vara formaliserat och innefatta återlämnande av all tidigare uthämtad programvara, organisationens dokument och utrustning. Organisationens övriga tillhörigheter som t.ex. mobil datautrustning, kreditkort, passerkort, programvara, manualer och information lagrad på elektroniska media måste också återlämnas. . Kommentar:			
2.	I fall då en anställd, uppdragstagare eller tredjepartsanvändare köper utrustning av organisationen eller använder egen personlig utrustning, bör rutiner följas för att all relevant information överförs till organisationen och raderas från utrustningen på ett säkert sätt (se också 10.7.1). Kommentar:			
3.	I de fall en anställd, uppdragstagare eller tredjepartsanvändare har kunskap som är av vikt för pågående verksamhet bör sådan information dokumenteras och överföras till organisationen. Kommentar:			

8.3.3 Indragning av åtkomsträttigheter

	Nivå
Alla anställdas, uppdragstagares och tredjepartsanvändares åtkomsträtt till information och informationsbehandlingsresurser bör dras in när anställningen, avtalet eller överenskommelsen avslutas eller justeras vid förändringar. *Kritisk säkerhetsåtgärd: JA* *Risk: Om åtkomsträttigheter inte återlämnas uppstår en risk för ekonomisk förlust, avslöjande av hemlig information och brott mot immaterialrätten.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	En persons rätt till åtkomst av tillgångar som rör informationssystem och tjänster bör prövas vid avslutat engagemang. Detta avgör om det är nödvändigt att eliminera åtkomsträtten. Kommentar:			
2.	Då en anställning ändras bör det återspeglas i att åtkomsträtt som inte är godkänd för den nya befattningen dras in. Kommentar:			
3.	De åtkomsträttigheter som bör tas bort eller anpassas omfattar fysisk och logisk åtkomst, nycklar, ID-kort, informationsbehandlingsresurser (se också 11.2.4), prenumerationer och borttagande av all dokumentation som identifierar dem som aktuell medarbetare i organisationen. Kommentar:			
4.	Om en anställd, uppdragstagare eller tredjepartsanvändare lämnar sin befattning och har kännedom om lösenord för fortfarande aktiva konton bör dessa lösenord ändras när anställning upphör eller förändras, eller när avtal eller överenskommelser upphör att gälla. Kommentar:			
5.	Åtkomsträtt till informationstillgångar och informationsbehandlingsresurser bör begränsas eller dras in innan anställningsförhållandet upphör eller ändras beroende på värderingen av riskfaktorer såsom: a) om anställningens avslutande eller förändring har initierats av den anställde, uppdragstagaren eller tredje-partsanvändanvändaren eller av ledningen och anledningen till avslutandet;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
6.	b) den anställdes, uppdragstagare eller annan användares aktuella ansvar; Kommentar:			
7.	c) värdet av de vid tillfället åtkomliga tillgångarna. Kommentar:			

Övrig information

I vissa fall kan åtkomsträtt tilldelas på så sätt att de ger tillgänglighet även till andra än den anställde, uppdragstagaren eller den tredjepartsanvändaren som slutar, t.ex. grupp-ID. I sådana fall bör personer som slutar tas bort från gruppåtkomstlistor och åtgärder bör vidtas för att meddela alla andra berörda anställda, uppdragstagare och tredjepartsanvändare att inte längre lämna ut den informationen till personen som slutar.

I fall där ledningen tagit initiativ till anställningen upphör kan missnöjda anställda, uppdragstagare eller tredjepartsanvändare avsiktligt förvanska information eller sabotera informationsbehandlingsresurser. När det gäller personer som säger upp sig kan de frestas att samla på sig information för framtida användning.

9. Fysisk och miljörelaterad säkerhet

9.1 Säkrade utrymmen

Mål: Att förhindra obehörigt fysiskt tillträde, skador och störningar i organisationens lokaler och information.

Kritiska eller känsliga informationsbehandlingsresurser bör inrymmas i säkra utrymmen inom ett avgränsat skalskydd med lämpliga säkerhetsavspärrningar och tillträdeskontroller. De bör fysiskt skyddas mot otillåten åtkomst, skada och störning.

Skyddet bör stå i proportion till de identifierade riskerna.

9.1.1 Skalskydd

	Nivå
Skalskydd (barriärer som väggar, kortstyrda entréer eller bemannade receptioner) bör användas för att skydda utrymmen där information och informationsbehandlingsresurser finns. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan skalskydd exponeras system och (informations-) tillgångar och kan lättare stjälas, skadas eller manipuleras.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Följande riktlinjer bör övervägas och införas där det är lämpligt för det fysiska skalskyddet: a) skalskydd bör tydligt definieras och placeringen och styrkan hos varje sådant skalskydd bör anpassas till säkerhetskrav för tillgångarna inom skalskyddet och resultatet av en riskbedömning; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
2.	b) Skalskydd för en byggnad eller ett utrymme där informationsbehandlingsresurser installerats bör vara fysiskt heltäckande (t.ex. bör det inte finnas några luckor i skalskyddet eller områden där inbrott med lätthet kan ske). Ytterväggar bör ha solid konstruktion och alla yttre dörrar bör ha lämpligt skydd mot obehörigt tillträde med skyddande anordningar, t.ex. galler, larm, lås etc. Dörrar och fönster bör vara låsta när de är obevakade samt yttre skydd för fönster, särskilt på marknivå, bör övervägas; Kommentar:			
3.	c) en bemannad reception eller något annat sätt att kontrollera fysiskt tillträde till utrymmet eller byggnaden bör finnas; tillträde till utrymme eller byggnader bör begränsas till behörig personal; Kommentar:			
4.	d) fysiska avspärrningar bör, där så är lämpligt, byggas för att förhindra obehörigt fysiskt tillträde och nedsmutsning av miljön; Kommentar:			
5.	e) alla skalskyddets branddörrar bör vara larmade, övervakade och testade tillsammans med intilliggande väggar för att visa att de uppfyller krävd motståndsnivå i enlighet med lämpliga regionala, nationella och internationella standarder; De bör vara felsäkra i enlighet med lokala brandskyddsregler; Kommentar:			
6.	f) lämpliga larmsystem i enlighet med regionala, nationella och internationella standarder bör installeras och regelbundet provas. De bör omfatta alla ytterdörrar och åtkomliga fönster. Obemannade utrymmen bör vara ständigt larmade och även andra utrymmen, t.ex. datorhall eller kommunikationscentraler, bör förses med skydd. Kommentar:			
7.	g) informationsbehandlingsresurser som hanteras av organisationen bör fysiskt åtskiljas från sådana som hanteras av tredje part. Kommentar:			

Övrig information

Fysiskt skydd kan uppnås genom att skapa en eller flera fysiska skyddsspärrar runt organisationens lokaler och dess informationsbehandlingsresurser. Att använda flera skyddsspärrar ger ytterligare skydd då genombrott av en enda spärr inte innebär att säkerheten omedelbart äventyras.

Ett säkert område kan vara ett låsbart kontor, eller flera rum omgivna av en obruten intern fysisk skyddsbarriär. Ytterligare barriärer eller skalskydd för att kontrollera fysiskt tillträde kan behövas mellan områden med olika säkerhetskrav inom skalskyddet.

Särskild försiktighet i fråga om fysiskt tillträdesskydd bör iakttas i byggnader där flera organisationer är inhysta.

9.1.2 Tillträdeskontroll

	Nivå
Säkra utrymmen bör skyddas genom lämpliga tillträdeskontroller för att säkerställa att endast behörig personal får tillträde. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan tillträdeskontroll exponeras system och (informations-) tillgångar och kan lättare stjälas, skadas eller manipuleras.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer bör övervägas: a) datum och tidpunkt när besökare anländer respektive går bör noteras och alla besökare bör bevakas såvida inte deras tillträde har godkänts tidigare. De bör få tillträde endast för särskilda, godkända ändamål och få instruktioner om platsens säkerhetskrav och nödrutiner; Kommentar:			
2.	b) tillträde till utrymmen där känslig information bearbetas eller lagras bör styras och begränsas till behörig personal. Behörighetskontroll, t.ex. behörighetskort med PIN-kod, bör användas för godkännande och validering av varje tillträde; allt tillträde bör loggas och loggen förvaras säkert; Kommentar:			
3.	c) det bör krävas att alla anställda, uppdragstagare och tredje parts användare bär någon form av synlig identifikation och omedelbart informerar säkerhetspersonal om de möter en icke eskorterad person eller någon som inte bär synlig identifikation; Kommentar:			
4.	d) servicepersonal från tredje parts företag bör ges begränsat tillträde till säkra utrymmen eller känsliga informationsbehandlingsresurser och endast när så krävs. Denna typ av tillträde bör sanktioneras och övervakas; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	e) tillträdesrätt till säkra utrymmen bör regelbundet granskas och uppdateras och återkallas vid behov. Kommentar:			

9.1.3 Skydd av kontor, rum och faciliteter

	Nivå
Kontor, rum och faciliteter bör utformas med tanke på fysisk säkerhet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om platser för informationsbehandlingsaktiviteter avslöjas kan (informations-)tillgångar missbrukas av utomstående. Icke uppfyllda krav på hälso och säkerhetsföreskrifter kan leda till skador och* skadeståndskrav.	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer bör övervägas för att säkra kontor, rum och faciliteter: a) hänsyn bör tas till relevanta hälso- och säkerhetsföreskrifter och standarder; Kommentar:			
2.	b) viktiga faciliteter bör förläggas så att allmänhetens åtkomst undviks Kommentar:			
3.	c) där det är möjligt bör byggnader vara diskreta och ge minsta möjliga antydan om sitt användningsområde, utan uppenbar skyltning som inom eller utom byggnaden visar förekomsten av informationsbehandlingsaktiviteter; Kommentar:			
4.	d) adressförteckningar och interna telefonkataloger som anger platser med känsliga informationsbehandlingsresurser bör inte vara allmänt tillgängliga. Kommentar:			

9.1.4 Skydd mot externa hot och miljöhot

	Nivå
Fysiska skydd mot skada orsakad av brand, översvämning, jordbävning, explosion, upplopp och andra former av naturliga eller av människor orsakade katastrofer bör utformas och tillämpas. *Kritisk säkerhetsåtgärd: JA* *Risk: Bristfälligt skydd mot fysiska katastrofer innebär risk för skador på personal, utrustning, informationssystem och lokaler, vilket i sin tur kan leda till förlust av alla kritiska resurser och äventyra kontinuiteten i organisationens arbete.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Hänsyn bör tas till hot mot säkerheten som kan uppstå i angränsande utrymmen, t.ex. brand i en grannbyggnad, vattenläckage från tak eller i våningar under marknivå eller en explosion på gatan. Kommentar:			
2.	Följande riktlinjer bör beaktas för att undvika skador av brand, översvämning, jordbävning, upplopp och andra former av naturliga eller av människor orsakade katastrofer: a) farligt och brännbart material bör förvaras på betryggande avstånd från ett säkert utrymme. Skrymmande förråd av t.ex. blanketter bör inte förvaras inom ett säkert utrymme; Kommentar:			
3.	b) reservutrustning och media med säkerhetskopior bör förvaras på säkert avstånd för att undvika skador orsakad av en katastrof som drabbar ordinarie utrymme; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
4.	c) lämplig brandbekämpningsutrustning bör finnas placerad på lämplig plats. Kommentar:			

9.1.5 Arbete i säkra utrymmen

	Nivå
Fysiskt skydd och riktlinjer för arbete i säkra utrymmen bör utarbetas och tillämpas. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Oklara riktlinjer för arbete i säkra områden kan äventyra säkerheten för personal som arbetar där. Det ökar också risken för avslöjande av information, stöld, obehöriga ändringar i tillgångar och otillgänglighet av tillgångar.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Följande riktlinjer bör beaktas: a) personal bör ha kännedom om existensen av, eller verksamheten inom, ett säkrat utrymme endast om det är nödvändigt; Kommentar:			
2.	b) obevakat arbete inom säkra utrymmen bör undvikas både av säkerhetsskäl och för att förhindra tillfällen till skadlig verksamhet; Kommentar:			
3.	c) oanvända säkra utrymmen bör låsas fysiskt och kontrolleras regelbundet; Kommentar:			
4.	d) kamera, videokamera, bandspelare eller annan upptagningsutrustning som kameramobiler bör inte tillåtas utan särskilt tillstånd. Kommentar:			
5.	Arrangemangen gällande arbete inom säkra utrymmen innefattar säkerhetsåtgärder för de anställda, uppdragstagare och tredjepartsanvändare som arbetar i det säkra utrymmet, liksom även andra aktiviteter som tredje parter genomför där. Kommentar:			

9.1.6 Allmänhetens tillträdes, leverans- och lastutrymmen

	Nivå
Platser för tillträde som t.ex. leverans- och lastutrymmen och andra platser där obehöriga personer kan komma in i lokalerna bör övervakas och, om möjligt, avskärmas från informationsbehandlingsresurser för att undvika obehörigt tillträde. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om offentliga tillträdesplatser är oskyddade, kan de användas av obehöriga för att komma in i lokaler eller komma åt tillgångar i närheten.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer bör övervägas: a) tillträde till ett leverans- och lastområde från byggnadens utsida bör begränsas till identifierad och behörig personal; Kommentar:			
2.	b) leverans- och lastområde bör utformas så att gods kan lossas utan att leveranspersonalen får tillträde till andra delar av byggnaden; Kommentar:			
3.	c) ytterdörrar till ett leverans- och lastområde bör vara säkrade när innerdörrarna är öppna; Kommentar:			
4.	d) ankommande gods bör kontrolleras med avseende på tänkbara hot (se 9.2.1d) innan materialet flyttas från leverans- och lastområdet till platsen för dess användning; Kommentar:			
5.	e) ankommande gods bör registreras i enlighet med rutinerna för hantering av tillgångar (se också 7.1.1) när de förs in i anläggningen; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	f) ankommande och utgående leveranser bör åtskiljas fysiskt då det är möjligt. Kommentar:			

9.2 Skydd av utrustning

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

Utrustning bör skyddas mot fysiska hot och miljömässiga hot.

Skydd av utrustning (innefattandes sådan som används utanför organisationens lokaler, samt avlägsnande av egendom) krävs för att minska risken för obehörig åtkomst av information och skydda mot förlust och skada. Det bör också beaktas var utrustning installeras och hur den avvecklas. Särskilda säkerhetsåtgärder kan krävas för att skydda mot fysiska hot och för att skydda försörjningsutrustning, t.ex. elförsörjning och kablage

9.2.1 Placering och skydd av utrustning

	Nivå
Utrustning bör placeras eller skyddas för att minska risken för miljömässiga hot och faror och för möjligheten till obehörig åtkomst. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om utrustning inte är skyddad mot fysiska och miljömässiga hot kan den äventyras (även med avseende på informationsåtkomst), stjälas eller skadas.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer bör beaktas för att skydda utrustning: a) utrustning bör placeras så att onödigt tillträde till arbetsutrymmet minimeras; Kommentar:			
2.	b) informationsbehandlingsresurser som hanterar känsliga data bör placeras så att synfältet begränsas för att minska risken för att informationen blir synlig för obehöriga medan den används, och lagringsutrymmen bör säkras för att undvika obehörig åtkomst; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
3.	c) komponenter som kräver specialskydd bör isoleras för att minska den allmänt erforderliga skyddsnivån. Kommentar:			
4.	d) säkerhetsåtgärder bör användas för att minimera risken för tänkbara fysiska hot, t.ex. stöld, brand, explosioner, rök, vatten (eller vattenbrist), damm, vibration, kemisk påverkan, störning i elförsörjning, störning av kommunikationer, elektromagnetisk strålning och vandalism; Kommentar:			
5.	e) riktlinjer bör fastställas för hantering av mat, dryck och rökning i närheten av informationsbehandlingsresurser; Kommentar:			
6.	f) miljöförhållanden, såsom temperatur och luftfuktighet, bör övervakas med avseende på förhållanden som kan påverka driften av informationsbehandlingsresurser negativt; Kommentar:			
7.	g) alla byggnader bör förses med skydd mot åsknedslag och alla inkommande kraftledningar och kommunikationslinjer bör förses med transientskydd; Kommentar:			
8.	h) tillämpning av särskilda skyddsmetoder, som tangentbordsmembran, bör beaktas för utrustning i industriell miljö; Kommentar:			
9.	i) utrustning som bearbetar känslig information bör skyddas så att risken för informationsläckage på grund av röjande signaler minimeras. Kommentar:			

9.2.2 Tekniska försörjningssystem

	Nivå
Utrustning bör skyddas från elavbrott och andra störningar orsakade av avbrott i tekniska försörjningssystem. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om utrustning inte är tillräckligt skyddad mot störningar i tekniska försörjningssystem (till exempel elavbrott) kan den sluta fungera eller skadas. Det kan också leda till att system och information blir otillgängliga. Det finns också risk för ekonomiska påföljder.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Alla tekniska försörjningssystem, som t.ex. elektricitet, vattenförsörjning, avlopp, värme/ventilation och luftkonditionering bör vara tillräckliga för de system de stödjer. Kommentar:			
2.	Tekniska försörjningssystem bör inspekteras regelbundet och testas på lämpligt sätt för att säkerställa deras rätta funktion och minska risken för felfunktion eller avbrott. Kommentar:			
3.	En lämpligt elektrisk strömförsörjning som uppfyller specifikationerna från tillverkaren av utrustningen bör anskaffas. Kommentar:			
4.	En kontinuerlig strömförsörjning (UPS) som stöd för korrekt avstängning eller för kontinuerlig drift rekommenderas för utrustning som används för kritiska verksamhetstillämpningar. Kommentar:			
5.	Kontinuitetsplan vid elavbrott bör inkludera åtgärd vid UPS-avbrott. Installation av en reservgenerator bör övervägas om bearbetning måste fortgå även vid långvarigt strömavbrott. kommentar:			
6.	Ett tillräckligt bränsleförråd bör finnas för att säkerställa att generatorn kan köras en längre tid. UPS-utrustning och generatorer bör kontrolleras regelbundet för att säkerställa att de har tillräcklig kapacitet och testas i enlighet med tillverkarnas rekommendationer.			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
7.	Vidare kan användning av mer än en kraftkälla övervägas eller, om verksamheten är omfattande, en separat sekundärkraftstation. Kommentar:			
8.	Nödstopp för elförsörjningen bör finnas nära nödutgångar i utrymmen med utrustning för att underlätta snabbavstängning i en nödsituation. Kommentar:			
9.	Reservbelysning bör finnas för ifall normal elförsörjning bryts. Kommentar:			
10.	Vattentillgången bör vara stabil och tillräcklig för att försörja luftkonditionering, luftfuktare och brandbekämpningssystem (där sådant finns). Kommentar:			
11.	Felfunktion i vattenförsörjningen kan förstöra utrustning eller hindra brandbekämpning från att fungera verkningsfullt. Ett alarmsystem för att upptäcka felfunktion hos försörjningssystemen bör utvärderas och installeras om nödvändigt. Kommentar:			
12.	Telekommunikationsutrustning bör anslutas till teleoperatören via minst två olika vägar för att förhindra att avbrott i en av förbindelserna bryter all samtalskontakt. Kommentar:			
13.	Samtalstjänsten bör vara tillräcklig för att möta lokala legala krav på nödkommunikation. Kommentar:			

Övrig information

Ett alternativ för att upprätthålla kontinuitet i kraftförsörjningen är att ha multipla matarledningar för att undvika en känslig avbrottspunkt i kraftförsörjningen.

9.2.3 Kablageskydd

	Nivå
Starkströms- och telekommunikationskablar som används för datatrafik eller stödjer informationstjänster bör skyddas mot avlyssning och åverkan. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfälligt kablageskydd medför en ökad risk för störningar, överföringsfel och obehörig avlyssning.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Följande riktlinjer bör övervägas för kablageskydd: a) starkströms- och telekablar som är anslutna till databehandlingsresurser bör om möjligt grävas ned eller skyddas på annat sätt; Kommentar:			
2.	b) nätverkskablage bör skyddas mot obehörig avlyssning eller skada, t.ex. genom användning av skyddsrör eller genom att undvika dragning genom område som är tillgängligt för allmänheten; Kommentar:			
3.	c) starkströmskablar och kommunikationskablar bör dras skilda från varandra för att undvika interferens; Kommentar:			
4.	d) kablar och utrustning bör vara tydligt märkta för att minska handhavandefel som t.ex. sammankoppling av fel nätverkskablar av misstag; Kommentar:			
5.	e) en dokumenterad åtgärdslogg bör användas för att minska riskerna för fel; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	f) för känsliga eller kritiska system bör också övervägas: 1) installation av armerade skyddsrör och låsta rum eller boxar i inspektions- och anslutningspunkter; 2) användning av alternativa kabeldragningar och/eller transmissionsmedia som ger tillräcklig säkerhet; 3) användning av fiberoptiska kablar; 4) användning av elektromagnetisk avskärmning för att skydda kablarna; 5) initiering av teknisk avsökning och fysiska inspektioner av att obehöriga utrustningar inte ansluts till kablaget; 6) styrd åtkomst till reparationspaneler och kabelutrymmen. Kommentar:			

9.2.4 Underhåll av utrustning

	Nivå
Utrustning bör underhållas på korrekt sätt för att säkerställa dess fortsatta tillgänglighet och systemets integritet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfällig service och underhåll av utrustning kan leda till avbrott och haveri.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer för utrustningens underhåll bör beaktas: a) utrustning bör underhållas enligt leverantörens rekommenderade serviceintervall och specifikationer; Kommentar:			
2.	b) endast auktoriserad underhållspersonal bör utföra reparationer och service på utrustning; Kommentar:			
3.	c) förteckning bör föras över alla misstänkta eller konstaterade fel och över allt förebyggande och avhjälpande underhåll; Kommentar:			
4.	d) lämpliga säkerhetsåtgärder bör införas när utrustning är avsedd att underhållas och då ta hänsyn till om detta underhåll utförs av personal på platsen eller externt. Om nödvändigt bör känslig information tas bort från utrustningen eller så bör underhållspersonalen ha genomgått tillräckliga säkerhetskontroller; Kommentar:			
5.	e) alla krav som ställs i försäkringsvillkor bör uppfyllas. Kommentar:			

9.2.5 Säkerhet för utrustning utanför egna lokaler

	Nivå
Säkerhet beträffande utrustning utanför egna lokaler bör utformas med de olika risker som är förknippade med att arbeta utanför organisationens lokaler i åtanke. *Kritisk säkerhetsåtgärd: Nej* *Risk: Utan regler för hantering av utrustningen utanför de egna lokalerna ökar risken för informationsförlust, informationsspridning eller skada på utrustningen.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Användning av informationsbehandlingsresurser utanför organisationens lokaler bör godkännas av ledningen, oavsett ägare. Kommentar:			
2.	Följande riktlinjer bör övervägas för skyddet av utrustning utanför egna lokaler: a) utrustning och media som medförs utanför egna lokaler bör inte lämnas obevakade på allmän plats. Bärbara datorer bör fraktas som handbagage och döljas under resor när det är möjligt; Kommentar:			
3.	b) tillverkarens instruktioner beträffande skydd av utrustning bör alltid följas, t.ex. vad gäller skydd mot starka elektromagnetisk fält; Kommentar:			
4.	c) säkerhetsåtgärder vid distansarbete bör avgöras genom en riskbedömning, och lämpliga åtgärder vidtas, t.ex. låsta förvaringsskåp, städat skrivbord, kontroll av åtkomst till datorer och säker kommunikation med kontoret (se även ISO/IEC 18028 Network Security); Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	d) tillräckligt försäkringsskydd bör finnas för att skydda utrustning utanför organisationens lokaler. Kommentar:			
6.	Säkerhetsrisker, t.ex. för skada, stöld eller avlyssning kan variera avsevärt mellan olika platser, något som bör beaktas när de lämpligaste säkerhetsåtgärderna bestäms. Kommentar:			

Övrig information

Utrustning för lagring och bearbetning av information omfattar alla former av persondatorer, planeringskalendrar, mobiltelefoner, aktiva kort, pappersdokument etc. som används för distansarbete eller förs ut från den normala arbetsplatsen.

Mera information om andra aspekter på skyddet av mobil utrustning finns i 11.7.1.

9.2.6 Säker avveckling eller återanvändning av utrustning

	Nivå
Alla utrustningsenheter som är försedda med lagringsmedia bör kontrolleras för att säkerställa att alla känsliga data och licensierade program har tagits bort eller överskrivits på ett säkert sätt innan utrustningen avvecklas. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan lämpliga metoder för avveckling av lagringsmedia, ökar risken att känslig information hamnar i fel händer, till exempel om saker säljs eller kastas i papperskorgen.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Enheter som innehåller känslig information bör fysiskt förstöras, alternativt bör informationen förstöras, utplånas eller överskrivas genom användning av teknik som omöjliggör rekonstruktion i stället för att använda standardfunktioner för att radera informationen eller utföra formatering. Kommentar:			

Övrig information
En riskbedömning kan behövas för skadade lagringsmedia som innehåller känsliga data för att avgöra om de fysiskt bör förstöras hellre än repareras eller kasseras.

Information kan äventyras genom oförsiktig avyttrande eller återanvändning av utrustning (se också 10.7.2).

9.2.7 Avlägsnande av egendom

	Nivå
Utrustning, information eller programvara bör inte avlägsnas från organisationens lokaler utan föregående tillstånd. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Otydliga regler för avlägsnande av (informations-) tillgångar eller dåligt upprätthållande av reglerna ökar risken för avslöjande av information, för juridiska krav (till exempel licenser) och för (ekonomisk) förlust av tillgångar.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande vägledning bör övervägas: a) utrustning, information eller programvara bör inte avlägsnas från organisationens lokaler utan föregående tillstånd; Kommentar:			
2.	b) anställda, uppdragstagare och tredjepartsanvändare som har tillstånd att ta med tillgångar utanför organisationens lokaler bör vara tydligt identifierbara; Kommentar:			
3.	c) tidsgränser för avlägsnande av utrustning bör anges och kontrolleras vid återlämnandet; Kommentar:			
4.	d) där det är nödvändigt och lämpligt bör utrustning som flyttas ut ur lokalerna registreras, liksom återlämnande av utrustningen. Kommentar:			

Övrig information

Stickprovskontroller som vidtas för att upptäcka obehörigt avlägsnande av egendom kan också genomföras för att upptäcka obehörig inspelningsutrustning, vapen etc. och förhindra att de förs in i lokalen. Sådana stickprover bör utföras i enlighet med relevanta författningar. Personal bör göras uppmärksam på att stickprover utförs och kontrollen bör endast utföras med behörighet anpassad till krav i författningar.

10. Styrning av kommunikation och drift

10.1 Driftsrutiner och driftansvar

Mål: Att säkerställa korrekt och säker drift av informationsbehandlingsresurser.

Ansvar och rutiner för styrning och drift av alla informationsbehandlingsresurser bör fastställas. Detta innefattar utveckling av lämpliga driftsrutiner.

Dualitet gällande arbetsuppgifter bör i förekommande fall tillämpas för att minska risken för försummelse eller avsiktligt missbruk av system.

10.1.1 Dokumenterade driftsrutiner

	Nivå
Driftsrutiner bör dokumenteras, underhållas och göras tillgängliga för alla användare som behöver dem. *Kritisk säkerhetsåtgärd: JA* *Risk: Bristfälliga driftsrutiner ökar risken för mänskligt fel (i synnerhet där det råder hög personalomsättning och snabba ansvarsförändringar) vid systemdrift. Det kan också leda till störningar och försämrad incidenthantering.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Dokumenterade rutiner bör tas fram för systemaktiviteter kopplade till informations- och kommunikationstillgångar såsom start- och avstängningsrutiner för datorer, säkerhetskopiering, underhåll av utrustning, mediahantering, datorrums- och posthantering och säkerhet. Bevisas genom: Uppvisande av driftinstruktioner och dessa kvalitetsgranskas mot punkt 2a-h. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
2.	Driftrutinerna bör omfatta detaljerade instruktionerna för att utföra varje arbetsuppgift inklusive: a) bearbetning och hantering av information; Kommentar:			
3.	b) säkerhetskopiering (se 10.5); Kommentar:			
4.	c) krav på ordningsföljd, innefattande beroenden av andra system, tidigaste starttid och senaste tid då viss körning skall vara avslutad; Kommentar:			
5.	d) instruktioner för hantering av fel och andra exceptionella förhållanden som kan uppstå under körningen, inklusive restriktioner i användningen av hjälpprogram (se 11.5.4); Kommentar:			
6.	e) lista över kontaktpersoner vid oväntade driftsstörningar eller tekniska svårigheter; Kommentar:			
7.	f) särskilda instruktioner för hantering av utdata och media som t.ex. användning av särskilt skrivmateriel eller hanteringsregler för konfidentiella utdata, inklusive rutiner för att på ett säkert sätt ta hand om utdata från misslyckade körningar (se 10.7.2 och 10.7.3); Kommentar:			
8.	g) återstart- och återställningsrutiner att användas vid eventuellt systemfel; Kommentar:			
9.	h) hantering av revisionsspår och systemens logg-information (se 10.10). Kommentar:			
10.	Driftrutiner och dokumenterade rutiner för systemaktiviteter bör behandlas som formella dokument där ändringar bör godkännas av			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	ledningen. Bevisas genom: IT-chefen ska ha godkänt dokumentet och det ska vara ändringshanterat. Kommentar:			
11.	Där det är tekniskt lämpligt bör informationssystem hanteras konsekvent med användning av samma rutiner, verktyg och hjälpprogram. Kommentar:			

10.1.2 Ändringshantering

	Nivå
Förändringar av informationsbehandlingsresurser och –system bör styras. *Kritisk säkerhetsåtgärd: JA* *Risk: Bristfälliga rutiner för ändringshantering medför ökad risk för instabilitet under normala (och oförutsedda) omständigheter. Riskens omfattning beror på systemets tillgänglighetskrav. Följdeffekter kan också bli att andra kritiska drifttjänster och system blir otillgängliga eller att vissa säkerhetskontroller inaktiveras vilket ökar risken för angrepp.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	System och tillämpningar i drift bör vara föremål för noggrann styrning gällande ändringshantering. Bevisas genom: Dokumenterad ändringshanteringsprocess och att den är införd enligt punkt 2a-f. Kommentar:			
2.	Särskilt bör följande punkter iakttas: a) identifiering och registrering av viktiga ändringar; Kommentar:			
3.	b) planering och test av ändringar; Kommentar:			
4.	c) bedömning av tänkbara effekter, inklusive effekten på säkerheten, av sådana ändringar; Kommentar:			
5.	d) rutin för formellt godkännande av föreslagna ändringar; Kommentar:			
6.	e) detaljerad information om ändringar till all relevanta personer; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	f) reservrutiner, inklusive rutiner och ansvar för att avbryta och återställa efter misslyckade ändringar och oförutsedda händelser. Kommentar:			
8.	Formellt ledningsansvar och rutiner bör finnas för att säkerställa godtagbar hantering av ändringar i utrustning, program och rutiner. När ändringar görs bör en revisionslogg omfattande all relevant information bevaras. Bevisas genom: Upprättad logg över godkända ändringar. Kommentar:			

Övrig information

Otillräcklig styrning av ändringar gällande informationsbehandlingsresurser och -system är en vanlig orsak till systemfel eller säkerhetsbrister. Ändringar i driftmiljön kan påverka tillförlitlighet hos tillämpningar, särskilt när ett system överförs från utveckling till drift (se också 12.5.1).

Ändringar av system i drift bör bara göras när det finns en godtagbar anledning för organisationen t.ex. vid ökad risk för systemet. Att uppdatera system med senaste operativsystemversion eller tillämpning är inte alltid i organisationens intresse, eftersom det kan leda till ökad sårbarhet och instabilitet jämfört med den aktuella versionen. Det kan också uppstå ett behov av mer utbildning, ökade licenskostnader, mer stöd, underhåll och administrativa kostnader och ny hårdvara, särskilt under övergångsskedet.

.

10.1.3 Uppdelning av arbetsuppgifter

	Nivå
Arbetsuppgifter och ansvar bör åtskiljas för att minska tillfällen till obehörig eller oavsiktlig förändring eller missbruk av organisationens tillgångar. *Kritisk säkerhetsåtgärd: JA* *Risk: Allmänt: Utan uppdelning av arbetsuppgifter ökar risken att fel som begåtts av en enskild individ orsakar brister i säkerhetsskyddet.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Uppdelning av arbetsuppgifter (dualitet) är en metod för att minska risken för oavsiktligt och avsiktligt missbruk av system. Kommentar:			
2.	Det bör undvikas att en och samma person kan få åtkomst till, modifiera eller använda tillgångar utan behörighet eller upptäckt. Initiering av en händelse bör skiljas från att ge behörighet till den. Bevisas genom: Analys av behovet och vidtagna åtgärder. Kommentar:			
3.	När säkerhetsåtgärder utformas bör risken för otillåten verksamhet i maskopi beaktas. Kommentar:			
4.	Små organisationer kan finna det svårt att åstadkomma dualitet, men principen bör tillämpas så långt det är praktiskt möjligt. Kommentar:			
5.	När det uppstår svårigheter att dela upp arbetsuppgifter bör andra åtgärder övervägas såsom uppföljning av verksamheten, revisionsspår och övervakning från ledningens sida. Bevisas genom: Dokumentation av dessa åtgärder. Kommentar:			
6.	Det är viktigt att säkerhetsgranskningen förblir oberoende. Kommentar:			

10.1.4 Uppdelning av utvecklings- test- och driftresurser

	Nivå
Utvecklings-, test- och driftresurser bör åtskiljas för att minska risken för obehörig åtkomst till eller ändringar i driftsystem. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan en avgränsad testmiljö ökar risken för instabil drift. Risken beror på hur kritiskt systemet är. Brist på tydlig uppdelning och indikation på huruvida en användare arbetar i test eller produktionsmiljö kan leda till att en transaktion av misstag registrerats och valideras i produktionsmiljö.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Den nivå på separeringen mellan drift, test, och utvecklingsmiljöer som är nödvändig för att förhindra driftproblem bör fastställas och ändamålsenliga säkerhetsåtgärder införas. Bevisas genom: Regelverk för detta som omfattar punkt 2a-f. Kommentar:			
2.	Följande punkter bör övervägas: a) regler för att överföra programvara från utvecklingsstatus till driftsstatus bör fastställas och dokumenteras; Kommentar:			
3.	b) utvecklings- och driftprogramvara bör köras på skilda system eller processorer och i skilda domäner eller katalogtjänster; Kommentar:			
4.	c) kompilatorer, editorer och andra utvecklingsverktyg eller systemverktyg bör inte vara åtkomliga från system i drift om ej nödvändigt; Kommentar:			
5.	d) testmiljön bör efterlikna driftmiljön så nära som möjligt; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	e) användare bör använda olika användarprofiler för drift- respektive testsystem och menyer bör visa lämpliga identifieringsmeddelanden för att minska risken för misstag; Kommentar:			
7.	f) känsliga data bör inte kopieras in i testmiljön (se 12.4.2). Kommentar:			

Övrig information

Utvecklings- och testaktiviteter kan orsaka allvarliga problem, t.ex. oönskad förändring av filer, systemmiljö eller systemfel. I detta fall finns behov av en känd och stabil miljö i vilken meningsfull testverksamhet kan utföras och som förhindrar olämplig åtkomst från utvecklare.

Där utvecklings- och testpersonal har åtkomst till driftsystem och dess information kan de ha möjlighet att införa obehörig och icke testad kod eller ändra driftdata. I vissa system skulle denna möjlighet kunna missbrukas för att genomföra bedrägerier eller för att föra in icke testad eller skadlig kod vilket kan orsaka allvarliga driftproblem.

Utvecklare och testpersonal utgör också ett hot mot driftinformationens konfidentialitet. Utvecklings- och testaktiviteter kan orsaka ej avsedda förändringar i program eller information om de delar samma datormiljö. Att åtskilja utvecklings-, test- och driftresurser från varandra är därför önskvärt för att minska risken för oavsiktlig ändring av och obehörig åtkomst till programvara i drift och verksamhetsdata (se också 12.4.2 om skyddet av testdata).

10.2 Hantering av tredjepartsleverantör av tjänster

Mål: Att införa och bibehålla lämplig nivå på informationssäkerhet och utförande av tjänster enligt överenskommelse om tjänsteleverans med tredje part.

Organisationen bör kontrollera implementeringen av avtal, följa upp överensstämmelsen med avtalen och hantera ändringar för att säkerställa att utförda tjänster uppfyller alla krav avtalade med den tredje parten.

10.2.1 Tjänsteleverans

	Nivå
Det bör säkerställas att säkerhetsåtgärder, definitioner av tjänsten och leveransnivån enligt avtalet med den tredje parten införs, drivs och upprätthålls av parten ifråga. *Kritisk säkerhetsåtgärd: JA* *Risk: Brist på SLA kan innebära till att systemägarens förväntningar inte uppfylls av IT-avdelningen, vilket kan leda till att för många eller för få tjänster levereras. Det sistnämnda kan resultera i att säkerhetskraven inte uppfylls (särskild i förhållande till konfidentialitet, riktighet och tillgänglighet).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Tjänster utförda av tredje part bör innefatta avtalade säkerhetsarrangemang, tjänstedefinitioner och tjänstehanteringens olika aspekter. Kommentar:			
2.	När det är fråga om utläggning bör organisationen planera den nödvändiga överföringen (av information, resurser för informationsbehandlingsresurser och annat som behöver flyttas) och bör försäkra sig om att säkerheten bibehålls under hela överföringsperioden. Kommentar:			
3.	Organisationen bör säkerställa att den tredje parten upprätthåller tillräcklig kapacitet rörande sina tjänster tillsammans med realistiska planer för att säkerställa att avtalad överenskommen			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	kontinuitetsnivå för tjänsterna upprätthålls efter omfattande eller allvarliga avbrott i tjänsten eller katastrof (se 14.1). Kommentar:			

10.2.2 Övervakning och granskning av tjänster från tredje part

	Nivå
De tjänster, rapporter och redovisningar som presteras av tredje part bör regelbundet övervakas och granskas och revisioner bör göras regelbundet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Dålig övervakning på överenskommen SLA kan leda till överfakturering och försämrat utförande av tjänster. Det sistnämnda kan resultera i att säkerhetskrav inte uppfylls (särskild i förhållande till konfidentialitet, riktighet och tillgänglighet).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Övervakning och granskning av tjänster från tredje part bör säkerställa att villkor och förhållanden för informationssäkerhet enligt avtalet uppfylls och att informationssäkerhetsincidenter och -problem hanteras på lämpligt sätt. Kommentar:			
2.	Detta bör innefatta en relation och process för tjänstehantering mellan organisationen och den tredje parten för att: a) övervaka prestandanivåerna på tjänsten för att kontrollera efterlevnaden av avtalet; Kommentar:			
3.	b) granska tjänsterapporter från tredje parten och ordna regelbundna uppföljningsmöten enligt kraven i avtalet; Kommentar:			
4.	c) tillhandahålla information om informationssäkerhetsincidenter och granska denna information från den tredje parten och från organisationen enligt avtalets krav och eventuella kompletterande riktlinjer och rutiner; Kommentar:			
5.	d) granska den tredje partens revisionsspår och redovisning över säkerhetshändelser, driftproblem, fel, hur fel spåras och avbrott i den levererade tjänsten;			

Nivåstyrande frågor		JA	NEJ	VET EJ
	Kommentar:			
6.	e) lösa och hantera identifierade problem. Kommentar:			
7.	Ansvaret för att hantera relationen till en tredje part bör ges till en utsedd person eller en grupp med ansvar för samordning av tjänster. Kommentar:			
8.	Vidare bör organisationen säkerställa att den tredje parten utser ansvarig för kontroll av efterlevnad och uppfyllande av avtalskraven. Kommentar:			
9.	Det bör finnas tillräcklig teknisk kunskap och resurser för att övervaka att avtalskraven (se 6.2.3) följs, särskilt informationssäkerhetskraven. Kommentar:			
10.	När det uppstår brister i leveransen av tjänsten bör lämpliga åtgärder vidtas. Kommentar:			
11.	Organisationen bör hålla tillräcklig övergripande styrning och insyn i alla säkerhetsaspekter för känslig eller kritisk information eller informationsbehandlingsresurser som används, bearbetas eller hanteras av tredje part.. Kommentar:			
12.	Organisationen bör säkerställa att insyn i säkerhetsaktiviteter bibehålls, t.ex. hantering av ändringar, identifiering av sårbarhet samt rapportering och åtgärder vid informationssäkerhetsincidenter genom ett klart definierat rapporteringsförfarande, inklusive format och struktur. Kommentar:			

Övrig information

Organisationen måste vara medveten om att den bibehåller det slutliga ansvaret för information bearbetad av tredje parts part vid utläggning.

10.2.3 Ändringshantering av tjänster från tredje part

	Nivå
Ändring avseende utförande av tjänster, inklusive att upprätthålla och förbättra befintliga policyer, rutiner och säkerhetsåtgärder för informationssäkerhet, bör hanteras med hänsyn till hur kritiska verksamhetssystem och processer är och till förnyad bedömning av risker. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfällig ändringshantering för utförande av tjänster kan leda till störningar, incidenter och inaktiverade säkerhetskontroller. Det sistnämnda kan resultera i att säkerhetskrav inte uppfylls (särskild i förhållande till konfidentialitet, riktighet och tillgänglighet).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Processen för ändringshantering av tjänster från tredje part behöver ta hänsyn till: a) förändringar som görs av organisationen för att införa: 1) förbättringar av det aktuella tjänsteutbudet; 2) utveckling av eventuella nya tillämpningar och system; 3) modifiering eller uppdatering av organisationens policyer och rutiner; 4) nya säkerhetsåtgärder för att lösa informationssäkerhetsincidenter och förbättra säkerheten; Bevisas genom: Livscykelprocess för ändringshantering och dokumentation av denna enligt 1a-b. Länk: Exempel på en livscykel för ändringshantering och kontroll av informationssäkerhet i system. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
2.	b) ändring av tjänster från tredje part för att införa: 1) ändringar och förbättringar i nätverk; 2) användning av nya tekniker; 3) införande av nya produkter eller nyare versioner/utgåvor; 4) nya utvecklingsverktyg och -miljöer; 5) ändring i tjänsteresursernas fysiska placering; 6) byte av leverantörer. Kommentar:			

10.3 Systemplanering och systemgodkännande

Mål: Att minimera risken för systemfel.

Planering och förberedelse krävs i förväg för att säkerställa att tillgänglig kapacitet och resurser finns för att leverera den systemprestanda som krävs.

Planläggning för framtida kapacitetskrav bör göras för att minska risken för överbelastning av system.

Driftkraven hos nya system bör fastställas, dokumenteras och testas innan de godkänds och används.

10.3.1 Kapacitetsplanering

	Nivå
Resursanvändningen bör övervakas, justeras, och prognoser bör göras av framtida kapacitetskrav för att säkerställa den erforderliga prestandan i systemen. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfällig kapacitetsplanering kan resultera i otillräckliga dator- och nätverksresurser (till exempel lagringsutrymme), otillgänglighet eller prestandaproblem. Eftersom de flesta system idag har stor reservkapacitet är detta vanligtvis inget akut problem, men det bör finnas med i beräkningarna.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	För varje ny och pågående aktivitet bör kapacitetskraven identifieras. Bevisas genom: Angivande av kapacitetskrav i SLA. Kommentar:			
2.	Justering och uppföljning av systemen bör utföras för att säkerställa och när så är nödvändigt, förbättra systemens tillgänglighet och effektivitet. Kommentar:			
3.	Upptäckande säkerhetsåtgärder bör införas för att indikera problem i tid.			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	Prognoser gällande framtida kapacitetskrav bör ta hänsyn till nya verksamhets- och systemkrav samt nuvarande och förväntade trender avseende organisationens informationsbehandlingsförmåga. Kommentar:			
5.	Särskild uppmärksamhet behöver ägnas åt resurser med långa ledtider eller höga kostnader för inköp; ansvariga bör därför övervaka användningsgraden av viktiga systemresurser Kommentar:			
6.	De bör identifiera hur användningen utvecklas, särskilt när det gäller verksamhetstillämpningar eller verktyg för ledningens informationssystem. Kommentar:			
7.	Ledningen bör använda denna information för att identifiera och undvika tänkbara flaskhalsar och beroende av nyckelpersoner som kan utgöra ett hot mot systemsäkerheten, eller tjänster, samt för att planera lämpliga åtgärder. Kommentar:			

10.3.2 Systemgodkännande

	Nivå
Kriterier för godkännande av nya och uppgraderade informationssystem liksom för nya versioner bör fastställas och lämpliga tester av system(en) utföras under utvecklingen och före godkännande. *Kritisk säkerhetsåtgärd: JA* *Risk: Bristfälliga acceptanstest baserade på fastställda krav kan leda till felaktig funktionalitet – till exempel bristande säkerhet. Det kan innebära att information blir felaktig, avslöjas eller att systemet slutar fungera.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Ledningen bör säkerställa att krav och kriterier för godkännande av nya system är tydligt definierade, överenskomna, dokumenterade och testade. Kommentar:			
2.	Nya och uppgraderade informationssystem och nya versioner bör inte tas i produktion förrän efter formellt godkännande. Bevisas genom: Uppvisande av beslut för systemgodkände innehållande delar av punkt 3a-j. Kommentar:			
3.	Följande punkter bör beaktas innan det formella godkännandet ges: a) prestanda- och kapacitetskrav för datorer; Kommentar:			
4.	b) rutiner för återställande av fel och för återstart, samt avbrottsplaner; Kommentar:			
5.	c) utformning och test av normala drifstrutiner enligt gällande standarder; Kommentar:			
6.	d) överenskommen uppsättning säkerhetsåtgärder på plats; Kommentar:			
7.	e) verkningsfulla manuella rutiner;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
8.	f) kontinuitetsplaner (se 14.1); Kommentar:			
9.	g) belägg för att installation av det nya systemet inte kommer att inverka negativt på befintliga system, särskilt vid hög belastning som t.ex. vid månadsslut; Kommentar:			
10.	h) belägg för att effekten av det nya systemet på organisationens totala säkerhet har beaktats; Kommentar:			
11.	i) praktisk utbildning gällande drift eller användning av nya system; Kommentar:			
12.	j) användarvänlighet, då det påverkar effektiviteten och minskar risken för misstag. Kommentar:			
13.	När det gäller nya, större system bör driftfunktionen och användare konsulteras under alla stadier i utvecklingsprocessen för att säkerställa driftseffektiviteten för den föreslagna systemutformningen. Kommentar:			
14.	Lämpliga tester bör genomföras för att bekräfta att alla kriterier för godkännande har uppfyllts i sin helhet. Bevisas genom: Upprättande av testrapport innan systeminförande. Kommentar:			

Övrig information

Godkännande kan omfatta en formell certifierings- och ackrediteringsprocess för att verifiera att säkerhetskraven har blivit rätt hanterade.

10.4 Skydd mot skadlig och mobil kod

Mål: Att säkerställa systemintegritet för programvara och riktighet i information.

Försiktighetsåtgärder krävs för att förhindra och upptäcka att skadlig kod och icke godkänd mobil kod installeras.

Programvara och informationsbehandlingsresurser är sårbara för att skadlig kod, såsom virus, maskar, Trojanska hästar och logiska bomber. Användare bör uppmärksammas på farorna med skadlig kod. Där det är lämpligt, bör ledningen införa säkerhetsåtgärder för att skydda mot, upptäcka och rensa bort skadlig kod liksom för att styra mobil kod.

10.4.1 Säkerhetsåtgärder mot skadlig kod

	Nivå
Upptäckande, förebyggande och återställande säkerhetsåtgärder bör införas för att skydda mot skadlig kod och lämpliga rutiner bör införas för att uppmärksamma användarna. *Kritisk säkerhetsåtgärd: JA* *Risk: Otillräckligt skydd mot skadlig kod innebär en risk att informationssystem blir angripna av virus eller trojaner vilket kan leda till störningar eller att information går förlorad.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Skydd mot skadlig kod bör baseras på programvara för upptäckt och reparation, säkerhetsmedvetande, och lämpliga säkerhetsåtgärder för åtkomst av system och ändringshantering. Bevisas genom: Beskrivning av hur skyddet mot skadlig kod är infört enligt punkt 2a-h. Upprättade riktlinjer och regler för användare. Länk: Exempel på riktlinje. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
2.	Följande vägledning bör beaktas: a) att fastställa en formell policy som förbjuder användning av ej godkänd programvara (se 15.1.2); Kommentar:			
3.	b) Att fastställa en formell policy för skydd mot riskerna förknippade med att hämta hem datafiler och programvara antingen från eller via externa nätverk eller från annat medium och som anger vilka säkerhetsåtgärder som bör vidtas); Kommentar:			
4.	c) Att utföra regelbundna granskningar av programvara och datainnehåll i system som stödjer kritiska verksamhetsprocesser. Förekomsten av icke godkända filer eller obehöriga förändringar bör formellt utredas; Kommentar:			
5.	d) Att installera och regelbundet uppdatera programvara för att upptäcka och reparera skadlig kod och som läser av datorer och media i förebyggande syfte eller rutinmässigt. De kontroller som utförs bör omfatta: 1) kontroll av alla datafiler på elektroniska eller optiska media och filer mottagna via nätverk med avseende på skadlig kod före användning; 2) Kontroll av nedladdade data och filer som är bifogade e-postmeddelanden med avseende på skadlig kod före användning. Kontrollen bör utföras på olika ställen, t.ex. på e-postservrar, i persondatorer eller när meddelande förs in i organisationens nätverk; 3) kontroll av webbsidor med avseende på skadlig kod; Kommentar:			
6.	e) att fastställa ledningsrutiner och ansvar för skydd mot skadlig kod i system, för praktisk utbildning i hantering av dem, liksom för rapportering och återställning efter en attack av skadlig kod (se 13.1 och 13.2); Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
7.	f) Att utarbeta lämpliga kontinuitetsplaner för verksamheten för återställning efter attack av skadlig kod, inklusive säkerhetskopiering av alla nödvändiga data och program samt rutiner som behövs för återställande (se avsnitt 14); Kommentar:			
8.	g) Att införa rutiner för att regelbundet samla information såsom prenumeration på e-postutskick och/eller bevakning av webbsidor som informerar om skadlig kod; Kommentar:			
9.	h) Att införa rutiner för att verifiera information om skadlig kod och säkerställa att varningsmeddelanden är korrekta och informativa. Ledningen bör säkerställa att kvalificerade källor, t.ex. välrenommerade tidskrifter, tillförlitliga Internet-källor eller leverantörer av programvara som skyddar mot skadlig kod används för att skilja mellan falsk och verklig skadlig kod. Alla användare bör informeras om problemet med falsk skadlig kod och vad som bör göras om sådan tas emot. Kommentar:			

Övrig information

Användning av två eller flera programvaruprodukter från olika leverantörer som skyddar mot skadlig kod över hela informationsbehandlingsmiljön, kan öka verkan hos skyddet mot skadlig kod.

Programvara för skydd mot skadlig kod kan installeras för att tillhandahålla automatisk uppdatering av definitionsfiler och sökmotorer för att säkerställa att skyddet hålls uppdaterat. Sådan programvara kan installeras på varje persondator för att göra automatiska kontroller.

Särskilda åtgärder bör övervägas för skydd mot att skadlig kod införs under underhålls- och reservrutiner som kan förbigå normala skyddsrutiner mot skadlig kod.

10.4.2 Säkerhetsåtgärder mot mobil kod

	Nivå
Där användning av mobil kod är tillåten bör konfigurationen säkerställa att godkänd mobil kod fungerar enligt en tydligt definierad säkerhetspolicy och att exekvering av icke godkänd mobil kod förhindras. *Kritisk säkerhetsåtgärd: JA* *Risk: Otillräckligt skydd mot mobil kod innebär risk för att otillåten kod kan exekveras vilket kan leda till driftsavbrott och att information blir felaktig eller förloras.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande åtgärder bör övervägas som skydd mot att mobil kod utför obehöriga aktiviteter: a) mobil kod exekveras i en logiskt isolerad miljö; Kommentar:			
2.	b) spärra all användning av mobil kod; Kommentar:			
3.	c) spärra mottagning av mobil kod; Kommentar:			
4.	d) aktivering av de tekniska åtgärder som är tillgängliga i ett visst system för att säkerställa hanteringen av mobil kod; Kommentar:			
5.	e) styrning av de resurser som är tillgängliga för åtkomst via mobil kod; Kommentar:			
6.	f) kryptografiska säkerhetsåtgärder för att unikt autentisera mobil kod. Kommentar:			

Övrig information

Mobil kod är programvarukod som överförs från en dator till en annan och sedan exekveras automatiskt och utför en särskild funktion med obetydlig eller ingen användarmedverkan. Mobil kod används av ett antal mellanprogramstjänster (middleware).

Förutom att säkerställa att mobil kod inte innehåller skadlig kod, är kontroll av mobil kod helt nödvändig för att undvika otillåten användning eller störning av system, nätverk eller tillämpningsresurser eller andra avvikelser från informationssäkerheten.

10.5 Säkerhetskopiering

Mål: Att bevara informationens och informationsbehandlingsresursers riktighet respektive systemintegritet samt tillgänglighet.

Rutinåtgärder bör etableras för att införa den beslutade policyn och strategin för säkerhetskopiering av data (se också 14.1) och för att öva återställande av data inom rimlig tid.

10.5.1 Säkerhetskopiering av information

	Nivå
Säkerhetskopior av information och programvara bör tas och testas regelbundet i enlighet med den beslutade policyn för säkerhetskopiering. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan väl fungerande rutiner för säkerhetskopiering ,eller bristfälliga tester för återställning, ökar risken för att systemet (och informationen) inte kan nås inom utsatt tid.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Lämplig utrustning för säkerhetskopiering bör finnas för att säkerställa att all viktig information och programvara kan återskapas efter en olyckshändelse eller fel på media. Kommentar:			
2.	Följande punkter gällande säkerhetskopiering bör beaktas: a) erforderlig nivå på säkerhetskopiering av information bör definieras; Kommentar:			
3.	b) korrekta och fullständiga förteckningar över säkerhetskopior och dokumenterade återställningsrutiner bör utarbetas; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
4.	c) Säkerhetskopieringens omfattning (t.ex. fullständig eller selekterad kopiering) och frekvens bör spegla organisationens krav, säkerhetskraven på den berörda informationen och hur kritisk informationen är för organisationens fortsatta drift; Kommentar:			
5.	d) den säkerhetskopierade informationen bör förvaras på avlägsen plats på tillräckligt avstånd för att undgå skada vid en olyckshändelse på det ordinarie driftstället; [3] Kommentar:			
6.	e) Den säkerhetskopierade informationen bör ges en lämplig nivå på fysiskt skydd och miljöskydd (se avsnitt 9) i överensstämmelse med gällande standard på ordinarie driftställe. De säkerhetsåtgärder som tillämpas för media på ordinarie driftställe bör också gälla på den plats där säkerhetskopior förvaras; Kommentar:			
7.	f) media för säkerhetskopior bör testas regelbundet för att säkerställa att de är pålitliga när de behövs i en akut situation; Kommentar:			
8.	g) Återställningsrutiner bör kontrolleras och testas regelbundet för att säkerställa att de är verkningsfulla och att de kan utföras inom den tid som är avsatt i driftsrutinerna för återhämtning; Kommentar:			
9.	h) I situationer där konfidentialitet är viktig bör säkerhetskopior skyddas genom kryptering. Kommentar:			
10.	Arrangemang för säkerhetskopiering av enskilda system bör testas regelbundet för att säkerställa att de klarar kontinuitetsplanernas krav (se avsnitt 14). För kritiska system bör arrangemangen för säkerhetskopiering täcka all systeminformation, tillämpningar och data nödvändiga för att återställa systemet i sin helhet om en olycka inträffar. Kommentar:			

[3] Kommentar: Tillräckligt avstånd är för kritisk verksamhet minst 2 mil och för övriga att samma händelse inte ska påverka verksamhetens säkerhetskopia.

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
11.	Tiden för bevarande av väsentlig information liksom också krav på permanent lagring av arkivkopior bör bestämmas (se 15.1.3). Kommentar:			

Övrig information

Arrangemang för säkerhetskopiering kan automatiseras för att underlätta säkerhetskopierings- och återställningsprocessen. Sådana automatiska lösningar bör testas i tillräcklig utsträckning före införande och med regelbundna intervall.

10.6 Hantering av säkerhet i nätverk

Mål: Att säkerställa skyddet av information i nätverk och i tillhörande infrastruktur.

Säker hantering av nätverk, vilka kan sträcka sig över organisationsgränser, kräver noggrann hänsyn till dataflöde, legala konsekvenser, övervakning och skydd.

Ytterligare åtgärder kan krävas för skyddet av känsliga data som överförs via allmänna nät.

10.6.1 Säkerhetsåtgärder för nätverk

	Nivå
Nätverk bör vara adekvat administrerade och övervakade, för att vara skyddade från hot, och för att upprätthålla säkerhet för system och tillämpningar som nyttjar nätverket, innefattandes även information under överföring. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Otillräcklig övervakning av nätverk kan leda till försämrad tillgänglighet, obehörig åtkomst eller avlyssning av information.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Nätverksansvariga bör införa säkerhetsåtgärder för att åstadkomma säkerhet för information i nätverk och för att skydda anslutna tjänster mot obehörig åtkomst. Bevisas genom: En riskanalys och beskrivning av säkerhetsåtgärder som bör minst innehålla punkt 2a-e. Kommentar:			
2.	Särskilt bör följande punkter bör beaktas: a) där det är möjligt bör driftansvaret för nätverk vara skilt från ansvaret för datordrift (se 10.1.3); Kommentar:			
3.	b) ansvar och rutiner bör fastställas för hantering av externt placerad utrustning, inklusive utrustning installerad hos användarna;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Bevisas genom: Instruktion till användarna om placering av utrustning. Kommentar:			
4.	c) särskilda säkerhetsåtgärder bör införas för att skydda konfidentialitet och riktighet när data passerar allmänna nät eller via trådlösa nätverk, och för att skydda anslutna system och tillämpningar (se 11.4 och 12.3), särskilda åtgärder kan också krävas för att upprätthålla tillgänglighet till nätverkstjänster och anslutna datorer; Kommentar:			
5.	d) erforderlig loggning och övervakning bör tillämpas för att möjliggöra registrering av säkerhetsrelevanta händelser; Kommentar:			
6.	e) administrativa aktiviteter bör noga samordnas både för att optimera tjänsten i förhållande till organisationen såväl som för att tillse att säkerhetsåtgärder är konsekvent tillämpade över hela infrastrukturen för informationsbehandling. Kommentar:			

Övrig information

Ytterligare information om nätverkssäkerhet finns i ISO/IEC 18028, Information technology – Security techniques – IT network security.

10.6.2 Säkerhet i nätverkstjänster

	Nivå
Säkerhetsfunktioner, tjänstenivåer och förvaltningskrav för alla nätverkstjänster bör klarläggas och ingå i varje överenskommelse om nätverkstjänster, oavsett om dessa tjänster utförs inom organisationen eller är utlagda. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Se 10.6.1. Bristfällig hantering av nätverkssäkerhet kan leda till försämrad tillgänglighet, obehörig åtkomst eller avlysning av information.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Förmågan hos leverantören av nätverkstjänster att hantera avtalade tjänster på ett säkert sätt bör bedömas och regelbundet kontrolleras, och rätten att få utföra revision bör avtalas. Bevisas genom: Att det finns ett avtal som stödjer detta samt plan för revision. Kommentar:			
2.	De säkerhetsarrangemang som är nödvändiga för vissa tjänster såsom säkerhetsegenskaper, tjänstenivåer och ledningens krav bör fastställas. Bevisas genom: Fastställt dokument. Kommentar:			
3.	Organisationen bör säkerställa att leverantören av nätverkstjänster inför dessa åtgärder. Kommentar:			

Övrig information

Nätverkstjänster innefattar att tillhandahålla förbindelser, privata nätverkstjänster och nät med värdeskapande tjänster och säkerhetslösningar för nätverk såsom brandväggar och system för intrångsdetektering. Dessa tjänster kan sträcka sig från vanlig oövervakad bandbredd till komplexa värdeskapande erbjudanden.

Nätverkstjänsternas säkerhetsfunktioner kan vara:

a) teknik tillämpad för säkra nätverkstjänster, såsom autenticering, kryptering och nätverkssegmentering

b) tekniska parametrar som krävs för säkrad förbindelse med nätverkstjänsterna i enlighet med reglerna för säkerhet och nätverksåtkomst

c) rutiner för användning av nätverkstjänst i syfte att begränsa åtkomst till nätverkstjänster eller applikationer, vid behov.

10.7 Hantering av media

Mål: Att förhindra obehörigt avslöjande, förändring, borttagning eller förstörande av tillgångar samt avbrott i verksamhet.

Lagringsmedia bör vara föremål för kontroll och fysiskt skydd.

Lämpliga driftsrutiner bör upprättas för att skydda dokument, datamedia (t.ex. band och diskar), in- och utdata och systemdokumentation, från obehörigt avslöjande, förändring, borttagande och förstöring.

10.7.1 Hantering av flyttbara datamedia

	Nivå
Det bör finnas rutiner för hantering av flyttbara datamedia. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan riktlinjer för hantering av flyttbar lagringsmedia (till exempel USB-minnen), ökar risken för att information lämnar företaget, både avsiktligt och oavsiktligt.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Följande riktlinjer för hantering av flyttbara datamedia bör övervägas: a) när det inte behövs längre bör innehållet i ett återanvändbart medium som ska avlägsnas från organisationen göras omöjligt att återställa; Bevisas genom: Rutin och metod för att förstöra datamedia. Kommentar:			
2.	b) Där det är nödvändigt och praktiskt möjligt, bör tillstånd krävas för att avlägsna media från organisationen och avlägsnade media bör noteras för att bibehålla spårbarhet; Bevisas genom: Instruktion om hur media får hanteras. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
3.	c) alla media bör förvaras på säker plats och i lämplig miljö enligt tillverkarens specifikationer; Kommentar:			
4.	d) information som lagrats på media och som kräver tillgänglighet längre än medias livstid (i enlighet med tillverkarens specifikationer) bör också lagras på annan plats för att undvika informationsförlust på grund av att media gradvis förstörs; Kommentar:			
5.	e) registrering av flyttbara media bör övervägas för att begränsa möjligheterna till dataförlust; Kommentar:			
6.	f) flyttbara enheter för media bör aktiveras endast om det finns verksamhetsbehov av att göra så. Kommentar:			
7.	Alla rutiner och behörighetsnivåer bör tydligt dokumenteras. Kommentar:			

Övrig information

Flyttbara media inkluderar band, diskar, minneskort, flyttbara hårddiskar, CD, DVD och tryckta media.

10.7.2 Avveckling av media

	Nivå
Media bör avvecklas på ett säkert och ofarligt sätt enligt en formell rutin när de inte längre behövs. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfälliga eller ineffektiva rutiner för säker avveckling av media innebär en ökad risk för spridning av känslig information.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	För att minimera risken för att information läcker ut till obehöriga bör formella regler tillämpas för avveckling av media. Bevisas genom: Framtagen regel för mediahantering som omfattar punkt 2,3a-e. Kommentar:			
2.	Rutinerna för säker avveckling av media som innehåller känslig information bör vara i nivå med informationens känslighet. Kommentar:			
3.	Följande punkter bör beaktas: a) Lagringsmedia som innehåller känslig information bör förvaras och avvecklas på ett säkert och ofarligt sätt, t.ex. genom att brännas eller strimlas alternativt rensas från data om mediet i fråga är avsett att användas inom annan tillämpning inom organisationen; Kommentar:			
4.	b) Rutiner bör finnas för att identifiera sådana enheter som kan kräva säker avveckling; Kommentar:			
5.	c) Det kan vara enklare att samla in samtliga mediaenheter som ska avvecklas och avveckla alla på ett säkert sätt hellre än att försöka skilja ut särskilt känsliga mediaenheter; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	d) många företag åtar sig att insamla och bortskaffa papper, utrustning och lagringsmedia. Försiktighet bör iakttas så att ett lämpligt företag som har lämplig hantering och erfarenhet väljs;			
7.	e) Där så är möjligt bör avveckling av känsligt material loggas i syfte att få spårbarhet. Kommentar:			
8.	När media för avveckling samlas in bör effekten av aggregering beaktas som kan få till följd att en stor mängd icke känslig information sammantaget blir känslig. Kommentar:			

Övrig information

Känslig information kan avslöjas genom oförsiktig avveckling av media (se också 9.2.6 rörande information om avveckling av utrustning).

10.7.3 Rutiner för informationshantering

	Nivå
Rutiner bör upprättas för hantering och förvaring av information i syfte att skydda sådan information mot obehörigt avslöjande eller användning. *Kritisk säkerhetsåtgärd: JA* *Risk: Brist på sekretess- och klassificeringspolicy och riktlinjer för genomförande innebär en ökad risk för att känslig information avslöjas. Känsliga dokument kan till exempel lämnas ut till leverantörer på grund av att de är felaktigt klassificerade.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Rutiner bör utformas för att hantera, bearbeta, lagra och kommunicera information i enlighet med dess klassificering (se 7.2). Bevisas genom: Framtagna rutiner för hantering av information enligt punkt 2a-l. Länk: Informationsklassningsdokument, modell och metod. Kommentar:			
2.	Följande punkter bör beaktas: a) hantering och märkning av alla media enligt dess angivna klassificeringsnivå; Kommentar:			
3.	b) åtkomstrestriktioner för att förhindra åtkomst från obehörig personal; Kommentar:			
4.	c) upprättande och underhåll av formellt register över behöriga mottagare av data; Kommentar:			
5.	d) säkerställande av att inmatade data är fullständiga, att bearbetning genomförs korrekt och att validering av utdata genomförs;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
6.	e) skydd av mellanlagrade data i väntan på slutlig utdataproduktion på en nivå som är anpassad efter deras känslighet; Kommentar:			
7.	f) förvaring av media i enlighet med tillverkarnas specifikationer; Kommentar:			
8.	g) begränsning av spridningen av data till ett minimum.; Kommentar:			
9.	h) tydlig märkning av alla kopior av media avsedda för behöriga mottagare; Kommentar:			
10.	i) regelbunden granskning av sändlistor och listor över behöriga mottagare. Kommentar:			

Övrig information

Dessa rutiner gäller information i dokument, datasystem, nätverk, mobila datorer, mobil kommunikation, elektronisk post, röstmeddelanden, röstkommunikation i allmänhet, multimedia, posttjänster, användning av faxmaskiner och allt annat som kan vara känsligt, som t.ex. ej ifyllda checkar, fakturor.

10.7.4 Säkerhet för systemdokumentation

	Nivå
Systemdokumentation bör skyddas mot obehörig åtkomst. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfälligt skydd av känslig (system) dokumentation kan leda till att den sprids till obehöriga, vilket kan underlätta för en angripare att få åtkomst till systemet.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	För att skydda systemdokumentationen bör följande punkter beaktas: a) systemdokumentationen bör förvaras säkert; Kommentar:			
2.	b) listan över dem som har tillgång till systemdokumentation bör omfatta så få namn som möjligt och godkännas av systemägaren; Kommentar:			
3.	c) systemdokumentation som finns åtkomlig på eller hämtas via publikt nät bör skyddas på lämpligt sätt. Kommentar:			

Övrig information
Systemdokumentation kan innehålla åtskilligt med känslig information, t.ex. beskrivning av tillämpningars processer, rutiner, datastrukturer, behörighetsprocesser.

10.8 Utbyte av information

Mål: Att bibehålla säkerheten för information och programvara som utbyts inom organisationen och med externa enheter.

Utbyte av information och programvara mellan organisationer bör baseras på en formell utbytespolicy genomförd enligt överenskommelser om utbyte, samt bör vara i överensstämmelse med relevant lagstiftning (se avsnitt 15).

Rutiner och regler bör fastställas för att skydda information och fysiska media innehållandes information under befordran.

10.8.1 Policyer och rutiner för informationsutbyte

	Nivå
Formella policyer, rutiner och säkerhetsåtgärder för informationsutbyte bör finnas för att skydda utbyte av information via alla typer av kommunikationsvägar. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Informationsutbyte med motparter är normalt av konfidentiell karaktär och bör inte innehålla känslig information. Det finns dock en liten risk att känslig information förmedlas av misstag. I olyckliga fall kan Tredje part ta del av informationen vilket skulle kunna leda till negativ publicitet.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	De rutiner och åtgärder som bör följas när elektroniska kommunikationsvägar används för informationsutbyte bör beakta följande punkter: a) rutiner utformade för att skydda informationsutbytet från avlyssning, kopiering, modifiering, feldirigering och förstöring; Bevisas genom: Upprättad rutinbeskrivning och åtgärder för informationsutbyte enligt punkt 1a-o. Kommentar:			
2.	b) rutiner för upptäckt av och skydd mot skadlig kod som kan skickas genom att använda elektronisk kommunikation (se avsnitt 10.4.1);			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
3.	c) rutiner för att skydda kommunicerad känslig elektronisk information som är i form av en bilaga; Kommentar:			
4.	d) policy eller riktlinjer som anger godtagbar användning av elektroniska kommunikationsutrustning (se 7.1.3); Kommentar:			
5.	e) rutiner för utnyttjande av trådlös kommunikation där hänsyn tas till de särskilda riskerna som det innebär; Kommentar:			
6.	f) anställds, uppdragstagares och annan användares ansvar att inte äventyra organisationen t.ex. genom förtal, trakasserier, imitation, vidarebefordran av kedjebrev, otillåtna inköp, etc; Kommentar:			
7.	g) användning av krypteringsteknik t.ex. för att skydda informationens konfidentialitet, riktighet och autenticitet (se avsnitt 12.3); Kommentar:			
8.	h) riktlinjer för bevarande och förstöring av all affärskorrespondens, inklusive meddelanden, i enlighet med relevant nationell lagstiftning och lokala föreskrifter; Kommentar:			
9.	i) säkerhetsåtgärder och restriktioner i fråga om kommunikationsutrustning för vidarebefordran, t.ex. automatisk vidarebefordran av e-post till externa e-postadresser; Kommentar:			
10.	j) säkerhetsåtgärder och restriktioner i fråga om kommunikationsutrustning för vidarebefordran, t.ex. automatisk vidarebefordran av e-post till externa adresser;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
11.	k) påminnelse till personalen om att de bör vidta lämpliga försiktighetsåtgärder, t.ex. för att inte avslöja känslig information, genom att undvika att bli avlyssnade eller få informationen uppsnappad när man telefonerar genom: 1) folk i deras omedelbara närhet, särskilt vid samtal i mobiltelefon; 2) telefonavlyssning och andra former av tjuvlyssnande genom fysisk åtkomst av telefonapparat eller telefonlinje eller användning av sökande mottagare; 3) personer på mottagarsidan: Kommentar:			
12.	l) att inte lämna meddelanden med känslig information på telefonsvarare eftersom de kan spelas upp av obehörig person, eller, lagras på allmänna system eller lagras inkorrekt som resultat av felslagning av numret; Kommentar:			
13.	m) påminnelse till personalen om problemen vid användning av faxmaskiner, såsom; 1) obehörig åtkomst till inbyggd meddelandelagring för att ta fram meddelanden; 2) avsiktlig eller oavsiktlig programmering av maskiner att sända meddelanden till särskilda nummer; 3) att sända meddelanden till fel nummer antingen genom felslagning eller genom att välja fel lagrat nummer; Kommentar:			
14.	n) påminnelse till personal att inte registrera demografiska data som t.ex. e-postadresser eller annan personlig information, i någon som helst programvara för att undvika insamling för obehörig användning; Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
15.	o) påminnelse till personal att moderna faxmaskiner och fotokopiatorer har buffertminnen och lagrar sidor vid eventuellt pappers- eller överföringsfel och kommer att trycka sidan så snart felet är avhjälpt. Kommentar:			
16.	Personal bör också påminnas om att de inte bör föra samtal om konfidentiella ämnen på allmän plats eller kontorslandskap och mötesplatser utan ljudisolerade väggar. Kommentar:			
17.	Resurser för informationsutbyte bör uppfylla tillämpliga författningskrav (se avsnitt 15). Kommentar:			

Övrig information

Information kan utbytas genom användning av ett antal olika typer av kommunikationsvägar, t.ex. e-post, röst, fax och video.

Utbyte av programvara kan ske genom ett antal olika media inklusive nerladdning från Internet och inköp från företag som säljer standardprodukter.

Verksamhetsanknutna, legala och säkerhetsmässiga konsekvenser vid elektroniskt datautbyte (EDI), elektronisk handel och annan elektronisk kommunikation samt krav på säkerhetsåtgärder bör övervägas.

Information kan äventyras på grund av brist på kunskap, policy eller rutiner i fråga om användning av resurser för informationsutbyte, t.ex. att bli avlyssnad vid användning av mobiltelefon på allmän plats, felsändning av ett e-postmeddelande, avlyssning av en telefonsvarare, obehörig åtkomst till uppkopplad röstpostlåda eller faxmeddelande som av misstag sänds till fel faxutrustning.

Organisationens verksamhet kan störas och information kan äventyras vid fel på kommunikationsutrustning, om den är överbelastad eller avbryts (se 10.3 och avsnitt 14). Information kan äventyras om obehöriga användare kommer åt den (se avsnitt 11).

10.8.2 Överenskommelser om överföring

	Nivå
Överenskommelser om utbyte av information och programvara mellan organisationen och externa parter bör upprättas. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Avtal om utbyte och överenskommelser som inte tillräckligt inriktar sig på säkerhetsfrågor ökar risken att tredje part inte hanterar säkerhetskrav eller att tredje parts tjänster inte överensstämmer med säkerhetskraven.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	I avtal om utbyte bör följande säkerhetsvillkor beaktas: a) administrativt ansvar för att kontrollera och meddela överföring, avsändning och mottagning; Kommentar:			
2.	b) rutiner för att meddela sändare om överföring, avsändning och mottagning: Kommentar:			
3.	c) rutiner för att säkerställa spårbarhet och oavvislighet; Kommentar:			
4.	d) lägsta tekniska standarder för paketering och sändning; Kommentar:			
5.	e) depositionsavtal; Kommentar:			
6.	f) regler för identifiering av budfirmor; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	g) ansvar och skyldigheter i händelse av informationssäkerhetsincidenter som t.ex. dataförlust; Kommentar:			
8.	h) användning av överenskommet system för märkning av känslig eller kritisk information och säkerställande att betydelsen av märkningen är omedelbart begriplig och att informationen är lämpligt skyddad; Kommentar:			
9.	i) ägande och ansvar för dataskydd, upphovsrätt, efterlevnad beträffande programvarulicenser och liknande överväganden (se 15.1.2 och 15.1.4); Kommentar:			
10.	j) tekniska standarder för registrering och läsning av information och programvara;			
11.	k) eventuella särskilda säkerhetsåtgärder som kan behövas för att skydda känsliga data som t.ex. kryptonycklar (se 12.3). Kommentar:			
12.	Policyer, rutiner och standarder bör fastställas och bibehållas för att skydda information och fysiska media vid överföring (se också 10.8.3) och bör anges i sådana överenskommelser om utbyte. Kommentar:			
13.	Säkerhetsbestämmelserna i en överenskommelse bör spegla känsligheten hos den berörda informationen. Kommentar:			

Övrig information

Överenskommelser kan vara elektroniska eller manuella och förekomma i form av formella avtal eller villkor i ett anställningsavtal. När det gäller känslig information bör de särskilda metoder som används för överföring av sådan information vara konsekventa för alla organisationer och alla typer av överenskommelser.

10.8.3 Fysiska media under transport

Media som innehåller information bör skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport utanför en organisations fysiska gränser. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan tillräckligt skydd av fysisk media under transport, finns det en risk att försändelsen blir skadad, stulen eller manipulerad under transporten.*	**Nivå**

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer bör beaktas för att skydda media som transporteras mellan olika platser: a) tillförlitliga transportörer eller bud bör anlitas; Bevisas genom: Upprättad riktlinje för skydd av datamedia vid transport enligt punkt 1a-e. Kommentar:			
2.	b) en förteckning över godkända budfirmor bör överenskommas med ledningen; Kommentar:			
3.	c) en rutin bör införas för identitetskontroll av bud; Kommentar:			
4.	d) emballaget bör vara tillräckligt robust för att skydda innehållet mot sådan fysisk skada som med viss sannolikhet kan inträffa under transport och som uppfyller krav i tillverkares specifikationer (t.ex. för programvara) t.ex. skydda mot eventuella miljöfaktorer som kan minska medias återställningseffektivitet som t.ex. exponering för värme, fukt eller elektromagnetiska fält; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	e) om det är nödvändig bör säkerhetsåtgärder vidtas för att skydda känslig information mot obehörigt avslöjande eller förändring; t.ex. genom: 1) användning av låsta transportbehållare 2) personlig leverans 3) förpackning som avslöjar manipulering (som avslöjar eventuella försök att komma åt innehållet) 4) i extremfall dela försändelsen i mer än en leverans och skicka dem olika vägar Kommentar:			

Övrig information

Information kan vara sårbar för obehörig åtkomst, missbruk eller förvanskning under fysisk transport t.ex. när media sänds med posten eller med bud.

10.8.4 Elektroniska meddelanden

	Nivå
Information som hanteras som elektroniskt meddelande bör skyddas på lämpligt sätt. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan tillräckligt skydd av elektroniskt meddelande finns det en risk att meddelandet förlorar konfidentialitet, tillgänglighet eller riktighet .*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Överväganden i fråga om säkerhet för elektroniska meddelanden bör omfatta följande: a) skydd av meddelanden mot obehörig åtkomst, förändring eller tillgänglighetsförlust; Kommentar:			
2.	b) att säkerställa korrekt adressering och transport av meddelandet; Kommentar:			
3.	c) tjänstens allmänna tillförlitlighet och tillgänglighet Kommentar:			
4.	d) legala överväganden, t.ex. krav på elektroniska signaturer; Kommentar:			
5.	e) att erhålla godkännande före användning av publika tjänster såsom snabbmeddelanden eller fildelning; Kommentar:			
6.	f) starkare autentiseringsnivåer som styr åtkomst till publika nät. Kommentar:			

Övrig information

Elektroniska meddelanden som e-post, Electronic Data Interchange (EDI) och snabbmeddelanden spelar en allt viktigare roll organisationer emellan. Elektroniska meddelanden medför andra risker än pappersbaserad kommunikation.

10.8.5 Verksamhetsrelaterade informationssystem

	Nivå
Policyer och rutiner bör utvecklas och införas för att skydda information i samband med sammankoppling av verksamhetsrelaterade informationssystem. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Otillräckligt skydd vid sammankoppling av verksamhetsrelaterade informationssystem kan leda till obehörig åtkomst och manipulering av information och transaktioner (transaktionsbedrägeri).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Överväganden med avseende på säkerhet och konsekvenser för organisationen av att integrera sådana resurser bör omfatta: a) kända sårbarheter i de administrativa systemen och bokföringssystemen där informationen delas mellan olika delar av organisationen; Bevisas genom framtagen policy och rutin för sammankoppling av verksamhetsrelaterade informationssystem. Kommentar:			
2.	b) informationens sårbarhet i verksamhetens kommunikationssystem, t.ex. inspelning av telefon- eller konferenssamtal, samtalens konfidentialitet, lagring av faxmeddelanden, postöppning, postdistribution; Kommentar:			
3.	c) policy och lämpliga säkerhetsåtgärder för att hantera informationsdelning; Kommentar:			
4.	d) Att undanta för vissa kategorier av känslig information och hemliga dokument om systemet inte klarar tillräcklig skyddsnivå; Kommentar:			
5.	e) begränsning av åtkomst till kalenderinformation avseende vissa personer, t.ex. personal som arbetar med känsliga projekt (se 7.2);			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
6.	f) kategorier av personal, uppdragstagare och partners vars åtkomst till systemet kan beviljas och de platser från vilka åtkomst kan ske (se 6.2 och 6.3); Kommentar:			
7.	g) begränsa utvalda resurser till specifika användarkategorier; Kommentar:			
8.	h) identifiering av användares status i register, t.ex. organisationens anställda eller uppdragstagare till nytta för andra användare; Kommentar:			
9.	i) bevarande och säkerhetskopiering av systemets information (se 10.5.1);			
10.	j) reservarrangemang och krav (se 14). Kommentar:			

Övrig information

Kontorssystem innebär möjligheter för snabbare spridning och att ta del av verksamhetsrelaterad information genom att utnyttja en kombination av: dokument, datorer, bärbara datorer, mobil kommunikation, post, röstpost, röstkommunikation i allmänhet, multimedia, posttjänster/utrustning och faxmaskiner.

10.9 Elektronisk handel

Mål: : Att tillgodose säkerheten för e-handelstjänster, samt deras säkra användning.

Säkerhetskonsekvenserna förenade med nyttjande av e-handelstjänster, inklusive on-linetransaktioner, samt kraven gällande säkerhetsåtgärder, bör beaktas. Riktigheten och tillgängligheten hos information som publiceras elektroniskt via allmänt tillgängliga system bör också beaktas.

10.9.1 Elektronisk handel

	Nivå
Information inbegripen i elektronisk handel som skickas över allmänt tillgängliga nätverk bör skyddas mot bedrägliga förfaranden, avtalstvister, samt obehörigt avslöjande, och modifiering. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan tillräcklig säkerhet, vid e-handel, finns det risk för otillåten avlyssning eller förändring av information, bedrägeri eller konflikter, som kan få både juridiska och ekonomiska följder.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Överväganden när det gäller säkerheten vid e-handel bör innefatta följande: a) den förtroendenivå vardera parten kräver vad gäller varandras uppgivna identitet t.ex. genom autenticering; Kommentar:			
2.	b) behörighetsrutiner i fråga om vem som sätter priser och vem som utfärdar eller signerar viktiga affärsdokument; Kommentar:			
3.	c) att säkerställa att handelspartners är fullständigt informerade om sina behörigheter;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	d) att bestämma och uppfylla krav på konfidentialitet, riktighet, bevis på avsändning och mottagning av nyckeldokument och oavvislighet för avtal, t.ex. i samband med offerter och avtalshantering; Kommentar:			
5.	e) behov av förtroende för riktigheten i annonserade prislistor; Kommentar:			
6.	f) konfidentialitet hos känsliga data eller information; Kommentar:			
7.	g) konfidentialitet och riktighet i ordertransaktioner, betalinformation, detaljer i leveransadresser och bekräftelse av mottagning; Kommentar:			
8.	h) nivå på lämplig verifiering för att kontrollera betalningsinformation som lämnas av en kund; Kommentar:			
9.	i) val av lämpligaste betalningsform för skydd mot bedrägeri; Kommentar:			
10.	j) erforderlig skyddsnivå som krävs för att bevara orderinformationens konfidentialitet och riktighet; Kommentar:			
11.	k) undvikande av förlust eller duplicering av transaktionsinformation; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
12.	l) skuldfråga vid eventuell bedräglig transaktion. Kommentar:			
13.	m) försäkringskrav. Kommentar:			
14.	Många av de ovanstående övervägandena kan hanteras genom att nyttja kryptering (se 12.3), varvid hänsyn tas till legala krav (se 15.1, särskilt 15.1.6 om lagstiftning om kryptering). Kommentar:			
15.	E-handelsarrangemang mellan handelsparter bör stödjas av ett dokumenterat avtal som binder båda parter till de överenskomna handelsvillkoren inklusive behörighetskontrolldetaljer (se b) ovan. Kommentar:			
16.	Andra överenskommelser med leverantörer av informationstjänster och nät med kompletterande tjänster (value added networks) kan vara nödvändiga. Kommentar:			
17.	Publika handelssystem bör meddela kunderna sina affärsvillkor. Kommentar:			
18.	Vid e-handel bör hänsyn tas till värdsystemets eller värdsystemens återhämtningsförmåga efter en attack och säkerhetskonsekvenserna av uppkoppling av nätverk som krävs för att införa e-handelstjänster (se 11.4.6). Kommentar:			

Övrig information

E-handel är sårbar för ett antal nätverkshot som kan resultera i bedrägeri, avtalstvist och avslöjande eller modifiering av information.

E-handel kan byggas upp med säkra autenticeringsmetoder t.ex. använda öppen-nyckelkryptering och digitala signaturer (se också 12.3) för att minska riskerna. Vidare, betrodda tredje parter kan användas där sådana tjänster behövs.

10.9.2 Direktanslutna transaktioner

	Nivå
Information i direktanslutna (on-line) transaktioner bör skyddas för att förhindra ofullständig överföring, feladressering, obehörig ändring av meddelande, obehörigt avslöjande, obehörig duplicering eller repetition av meddelande. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan tillräcklig säkerhet i direktanslutna (on-line) transaktioner finns det risk för att system utsätts för obehörigt avslöjande, manipulering, bedrägeri eller konflikter som kan ge både juridiska och ekonomiska följder.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Säkerhetsöverväganden för direktanslutna transaktioner bör omfatta följande: a) användning av elektroniska signaturer av var och en av de medverkande parterna i transaktionen; Kommentar:			
2.	b) alla aspekter på transaktionen d.v.s. säkerställa att: 1) alla användares behörigheter är giltiga och verifierade; 2) transaktionen förblir konfidentiell; 3) alla deltagande parters integritet bibehålls; Kommentar:			
3.	c) kommunikationsvägen mellan alla inblandade parter är krypterad; Kommentar:			
4.	d) de protokoll som utnyttjas för kommunikation mellan alla inblandade parter är säkra; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	e) säkerställa att lagringen av transaktionernas innehåll finns utanför allmänt åtkomliga miljöer t.e.x på en lagringsplattform på organisationens intranät och inte bevaras och exponeras på ett lagringsmedium som är direkt åtkomligt från Internet; Kommentar:			
6.	f) där en betrodd instans används (t.ex. för att ge ut och hantera digitala signaturer och/eller digitala certifikat) är säkerheten integrerad och innefattar hela hanteringskedjan av certifikat/signatur från början till slut. Kommentar:			

Övrig information

Omfattningen av tillämpade säkerhetsåtgärder behöver stå i proportion till risknivån vid varje typ av direktansluten transaktion.

Transaktioner kan behöva leva upp till lagar, regler och föreskrifter inom den jurisdiktion från vilken transaktionen utgår, bearbetas via, fullbordas i och/eller lagras.

Många typer av transaktioner kan utföras med direktanslutning, t.ex. avtalsrelaterade transaktioner, finansiella transaktioner etc.

10.9.3 Offentlig tillgänglig information

	Nivå
Riktigheten hos information som görs tillgänglig i ett för allmänheten tillgängligt system bör skyddas för att förhindra obehörig modifiering. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan tillräcklig säkerhet för publicerad information finns det risk för att information manipuleras eller görs otillgänglig.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Programvara, data och annan information som har höga krav på riktighet och som görs tillgängliga i allmänt tillgängliga system bör skyddas med lämpliga metoder, t.ex. digitala signaturer (se 12.3). Kommentar:			
2.	System med allmän tillgänglighet bör testas mot svagheter och fel innan informationen görs tillgänglig. Kommentar:			
3.	Det bör finnas ett formellt förfarande för godkännande innan informationen görs allmänt tillgänglig. Kommentar:			
4.	Dessutom bör alla indata som kommer utifrån till systemet vara verifierade och godkända. Kommentar:			
5.	Elektroniska publiceringssystem, särskilt sådana som tillåter återkoppling och direktinmatning av information bör noga styras så att: a) information erhålls i enlighet med förekommande lagstiftning om dataskydd (se 15.1.4); Kommentar:			
6.	b) information som matas in i och bearbetas av publiceringssystemet blir fullständigt och riktigt bearbetad inom avsedd tid; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	c) känslig information skyddas under insamling, bearbetning och lagring; Kommentar:			
8.	d) åtkomst till utgivningssystemet inte tillåter oavsiktlig åtkomst till det nätverk som systemet är anslutet. Kommentar:			

Övrig information

Information på ett för allmänheten tillgängligt system t.ex. en webbserver som kan nås via Internet kan behöva överensstämma med lagar, regler och föreskrifter inom den jurisdiktion inom vilken systemet är beläget, där handeln äger rum eller där ägaren eller ägarna är bosatta. Obehörig modifiering av publicerad information kan skada den ansvariga organisationens rykte.

10.10 Övervakning

Mål: : Att upptäcka obehöriga informationsbehandlingsaktiviteter.

System bör övervakas och informationssäkerhetshändelser bör registreras. Operatörs- och felloggar bör användas för att säkerställa att problem med informationssystem upptäcks.

Organisationen bör följa alla relevanta lagkrav som är tillämpliga på dess övervakning och loggning.

Systemövervakning bör användas för att kontrollera verkan av de säkerhetsåtgärder som används och verifiera att en modell för åtkomstpolicy följs.

10.10.1 Revisionsloggning

	Nivå
Revisionsloggar som registrerar användaraktiviteter, undantag, och informationssäkerhetshändelser bör föras och bevaras under en bestämd tidsperiod för att vara till hjälp vid framtida undersökningar och övervakning av åtkomstkontroll. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfällig hantering av revisionsloggar gör det svårare att identifiera och utreda säkerhetsincidenter.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

	Nivåstyrande frågor	JA	NEJ	VET EJ
1.	Där det är relevant, bör revisionsloggar innefatta: a) användaridentitet; Kommentar:			
2.	b) datum, tidpunkter och detaljer om viktiga händelser, t.ex. på- och avloggning; Kommentar:			
3.	c) om möjligt, terminalidentitet eller -placering;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	d) registrering av lyckade och avvisade försök till systemåtkomst; Kommentar:			
5.	e) registrering av lyckade respektive avvisade data och andra försök till åtkomst; Kommentar:			
6.	f) ändringar i systemkonfiguration; Kommentar:			
7.	g) användning av av särskild åtkomsträtt; Kommentar:			
8.	h) användning av systemverktyg och systemtillämpningar; Kommentar:			
9.	i) anropade filer och typ av åtkomst; Kommentar:			
10.	j) nätverksadresser och protokoll; Kommentar:			
11.	k) larm från åtkomstkontrollsystemet; Kommentar:			
12.	l) aktivering och avstängning av skyddssystem, såsom anti-virussystem och intrångsdetekteringssystem. Kommentar:			

Övrig information

Revisionsloggarna kan innehålla påträngande och konfidentiella persondata. Lämpliga åtgärder för skydd av personlig integritet bör vidtas (se också 15.1.4). Där det är möjligt bör systemadministratörer inte ha behörighet att radera eller deaktivera loggning av egna aktiviteter (se 10.1.3).

10.10.2 Övervakning av systemanvändning

	Nivå
Rutiner för övervakning av informationsbehandlingsresursernas användning bör upprättas och övervakningsresultaten granskas regelbundet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Otillräcklig övervakning ökar risken för att säkerhetsbrister som påverkar konfidentialitet, riktighet och tillgänglighet inte upptäcks och åtgärdas i tid.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Den nivå av övervakning som krävs för olika resurser bör dimensioneras utifrån riskbedömning. Kommentar:			
2.	En organisation bör följa alla relevanta legala krav som är tillämpliga på dess övervakningsaktiviteter. Kommentar:			
3.	Områden som bör övervägas omfattar: a) behörig åtkomst inklusive detaljer som: 1) användaridentitet; 2) datum och tidpunkt för viktiga händelser; 3) händelsetyper; 4) anropade filer; 5) använda program/verktyg; Kommentar:			
4.	b) alla privilegierade aktiviteter, såsom.: 1) användning av privilegierade konton, t.ex. supervisor, root, administratör 2) start och stopp av system 3) in- och urkoppling av I/O-enheter; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	c) obehöriga åtkomstförsök, såsom: 1) misslyckade eller avvisade användaraktiviteter 2) misslyckade eller avvisade aktiviteter som berör data och andra resurser 3) avvikelse från åtkomstpolicy och meddelanden från nätbryggor och brandväggar 4) larm från proprietära intrångsdetekteringssystem; Kommentar:			
6.	d) systemlarm eller fel såsom: 1) konsollarm eller –meddelanden; 2) undantagsmeddelanden från systemlogg; 3) larm från nätet; 4) larm från åtkomstkontrollsystemet; Kommentar:			
7.	e) ändringar eller försök till ändringar av systemets säkerhetsuppsättningar och säkerhetsåtgärder. Kommentar:			
8.	Hur ofta resultaten från övervakningsaktiviteter granskas bör baseras på förekommande risker. Bland riskfaktorer som bör övervägas ingår: a) hur kritisk tillämpningsprocessen är; Kommentar:			
9.	b) värde, känslighet och hur kritisk den berörda informationen är; Kommentar:			
10.	c) tidigare erfarenhet av systeminfiltration och missbruk och hur ofta sårbarheter utnyttjas; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
11.	d) i vilken utsträckning system är sammankopplade (särskilt öppna nät); Kommentar:			
12.	e) urkoppling av loggningsresurser. Kommentar:			

Övrig information

Rutiner för att övervaka användningen är nödvändiga för att säkerställa att användare endast utför aktiviteter som är explicit godkända.

En loggranskning kräver förståelse av hoten mot systemet och det sätt på vilket de kan uppstå. Exempel på händelser som kan kräva vidare undersökning vid informationssäkerhetsincidenter ges i 13.1.1.

10.10.3 Skydd av logginformation

	Nivå
Loggningsresurser och logginformation bör skyddas mot manipulering och obehörig åtkomst. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfälligt skydd av loggar ökar risken för att logginformation går förlorad (till exempel att loggar skrivs över) eller manipuleras vilket gör det svårare att utreda händelser i systemet.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Säkerhetsåtgärder bör inriktas mot att skydda mot obehöriga ändringar och driftproblem med loggningsresurserna inklusive: a) förändring av meddelandetyperna som registreras; Kommentar:			
2.	b) loggfiler som ändras eller raderas; Kommentar:			
3.	c) att loggfilens lagringskapacitet överskrids vilket resulterar antingen i att registrering av händelser misslyckas eller att tidigare registrerade händelser överskrivs. Kommentar:			
4.	Vissa revisionsloggar kan behöva arkiveras som del av en policy som rör bevarande av dokument eller på grund av krav på att insamla och spara bevis (se också 13.2.3). Kommentar:			

Övrig information

Systemloggar innehåller ofta stora informationsvolymer av vilket mycket är ovidkommande för säkerhetsövervakning. Till hjälp för att identifiera signifikanta händelser för säkerhetsövervakningen bör det övervägas att automatiskt kopiera lämpliga meddelandetyper till en andra logg och/eller använda lämpliga hjälpprogram eller revisionshjälpmedel för undersökning av till filerna och för rationalisering.

Systemloggar behöver skyddas eftersom om data kan ändras eller raderas i dem, kan deras existens skapa en falsk känsla av säkerhet.

10.10.4 Administratörs- och operatörsloggar

	Nivå
Systemadministratörers och systemoperatörers aktiviteter bör loggas. *Kritisk säkerhetsåtgärd: JA* *Risk: Bristfällig loggning av aktiviteter gör det svårare att identifiera och utreda säkerhetshändelser.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Loggarna bör innehålla: a) tidpunkt vid vilken en händelse (lyckad eller misslyckad) inträffade; Kommentar:			
2.	b) information om händelsen (t.ex. hanterade filer) eller misslyckande (t.ex. fel som inträffat och vidtagen korrigerande åtgärd); Kommentar:			
3.	c) vilket konto och vilken administratör eller operatör som var involverad; Kommentar:			
4.	d) vilka processer som var involverade. Kommentar:			
5.	Systemadministratörs- och operatörsloggar bör granskas regelbundet. Kommentar:			

Övrig information
Ett intrångsdetekteringssystem som hanteras utanför system- och nätverksadministratörernas kontroll kan användas för att övervaka efterlevnaden i system- och nätadministrationens verksamhet.

10.10.5 Loggning av fel

	Nivå
Fel bör loggas, analyseras och lämpliga åtgärder vidtas. *Kritisk säkerhetsåtgärd: NEJ* *Risk:*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Fel som rapporteras av användare eller av systemprogram avseende problem med i informationsbehandlings eller kommunikationssystem bör loggas. Kommentar:			
2.	Det bör finnas tydliga regler för att hantera rapporterade fel, inklusive de följande: a) granskning av felloggar i syfte att säkerställa att fel har blivit åtgärdade på ett tillfredsställande sätt; Kommentar:			
3.	b) granskning av korrigerande åtgärder för att säkerställa att säkerhetsåtgärder inte äventyrats och att vidtagen åtgärd är godkänd. Det bör säkerställas att felloggning är aktiverad om den funktionen finns tillgänglig i systemet. Kommentar:			

Övrig information

Loggning av misstag och fel kan påverka ett systems prestanda. Denna typ av loggning bör aktiveras av kvalificerad personal. Nivån av loggning som krävs för enskilda system bör avgöras genom riskbedömning, där hänsyn tas till prestandaförlusten.

10.10.6 Klocksynkronisering

	Nivå
Klockor i alla relevanta informationsbehandlingssystem inom en organisation eller en säkerhetsdomän bör synkroniseras med en överenskommen korrekt tidsangivelse. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Felaktiga tidstämplar gör det svårare att utreda säkerhetshändelser och att säkerställa spårbarheten.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	I de fall en dator eller en kommunikationsenhet kan driva en realtidsklocka, bör denna klocka ställas in mot en överenskommen standard t.ex. Coordinated Universal Time (UTC) eller lokal standardtid. Kommentar:			
2.	Eftersom det är känt att vissa klockor drar sig med tiden bör det finnas en rutin som kontrollerar och korrigerar alla signifikanta avvikelser. Kommentar:			
3.	Den korrekta tolkningen av formatet för datum/tid är viktig för att säkerställa att tidsstämpeln återspeglar den verkliga datumet/tiden. Hänsyn bör tas till lokala avvikelser (t.ex. sommartid). Kommentar:			

Övrig information

Att ställa datorklockor rätt är viktigt för att säkerställa revisionsloggarnas riktighet vilket kan krävas för undersökningar eller som bevis i legala eller disciplinära fall. Felaktiga revisionsloggar kan förhindra sådana undersökningar och skada trovärdigheten hos ett sådant bevis. En klocka kopplad till radiotid utsänd från ett nationellt atomur kan användas som referensklocka i loggningssystem. Ett nätverkstidsprotokoll kan användas för att hålla alla serverar synkroniserade med referensklockan.

11. Styrning av åtkomst

11.1 Verksamhetskrav på styrning av åtkomst

Mål: Att styra åtkomst till information.

Åtkomst till information, informationsbehandlingsresurser och verksamhetsprocesser bör styras på grundval av verksamhets- och säkerhetskrav.

Regler för styrning av åtkomst bör ta hänsyn till policyer för spridning och behörighet till information.

11.1.1 Åtkomstpolicy

	Nivå
En åtkomstpolicy bör fastställas, dokumenteras och granskas baserat på verksamhets- och säkerhetskrav gällande åtkomst. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan åtkomstkontrollpolicy, ökar risken att användare tilldelas eller bibehåller högre rättigheter än de behöver, vilket leder till obehörig åtkomst och ökar potentiell effekt av en attack.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Regler för styrning av åtkomst och rättigheter för varje användare eller grupp av användare bör tydligt fastställas i en åtkomstpolicy. Kommentar:			
2.	Säkerhetsåtgärder för åtkomst kan vara både logiska och fysiska (se också avsnitt 9) och dessa bör beaktas tillsammans. Kommentar:			
3.	Användare och uppdragstagare av tjänster bör få klart uttalat de verksamhetskrav som styrningen av åtkomst skall uppfylla.			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	Policyn bör ta hänsyn till följande: a) säkerhetskrav på varje enskild verksamhetstillämpning; Kommentar:			
5.	b) identifiering av all information som rör verksamhetstillämpningarna och de risker som finns för informationen; Kommentar:			
6.	c) policyer för informationsspridning och rättigheter, t.ex. ”behov-att-känna-till”-principen, säkerhetsnivåer och informationsklassificering (se 7.2); Kommentar:			
7.	d) konsekvens mellan riktlinjer för styrning av åtkomst och policyer för informationsklassificering hos olika system och nätverk; Kommentar:			
8.	e) relevanta rättsregler och eventuella avtalsrättsliga skyldigheter beträffande åtkomstskydd av data eller tjänster (se 15.1); Kommentar:			
9.	f) enhetliga åtkomstprofiler för användare med vanligt förekommande befattningar i organisationen; Kommentar:			
10.	g) hantering av åtkomsträttigheter i distribuerade miljöer och i nätverksmiljöer där hänsyn tas till alla tillgängliga typer av uppkopplingar; Kommentar:			
11.	h) åtskillnad av roller vid styrning av åtkomst, t.ex. åtkomstbegäran, åtkomsttillstånd, åtkomstadministration; Kommentar:			
12.	i) krav på formellt godkännande av begäran om åtkomst (se 11.2.1);			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
13.	j) krav på periodisk granskning av styrningen av åtkomst (se 11.2.4); Kommentar:			
14.	k) borttagning av åtkomsträtt (se 8.3.3). Kommentar:			

Övrig information

Noggrannhet bör iakttagas när åtkomstregler specificeras varvid bör beaktas:

a) att skilja mellan regler som alltid måste följas och riktlinjer som är valfria eller villkorliga;

b) att fastställa regler baserade på förutsättningen ”Allt är förbjudet som inte är uttryckligen tillåtet” snarare än den svagare regeln ”Allt är tillåtet som inte uttryckligen är förbjudet”;

c) ändrad märkning av information (se 7.2) som åsätts automatiskt av informationsbehandlingsresurser respektive sådan som användare kan göra själv;

d) ändring av användartillstånd som automatiskt åsätts av informationssystemet respektive sådana som en administratör initierar;

e) regler som kräver godkännande innan de verkställs respektive de som inte kräver det.

Regler för styrning av åtkomst bör stödjas av formella rutiner och klart definierat ansvar (se t.ex. 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Styrning av användares åtkomst

Mål: Att säkerställa behörig användares åtkomst och förhindra obehörig åtkomst till informationssystem.

Formella rutiner bör finnas för att styra tilldelningen av åtkomsträttigheter till informationssystem och tjänster.

Rutinerna bör täcka alla stadier i användaråtkomstens livscykel, från den första registreringen av nya användare till slutlig avregistrering av användare som inte längre behöver åtkomst till informationssystem och tjänster. Särskild försiktighet bör iakttas, där det är lämpligt, i fråga om behovet av att styra tilldelning av privilegierade åtkomsträttigheter som tillåter användare att förbigå normala systemspärrar.

11.2.1 Användarregistrering

	Nivå
Det bör finnas en formell rutin för registrering och avregistrering för att medge och återkalla åtkomst till alla informationssystem och tjänster. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan formella rutiner för registrering och avregistrering av användare ökar risken för att felaktiga rättigheter ges. Inaktiva användarkonton som finns kvar i systemet gör det lättare för en angripare. Generiska konton gör det svårare att säkerställa spårbarhet och tillförlitlighet. Utan spårbarhet kan det vara omöjligt att utreda vem som gjort vad, och om denne i så fall haft rättighet göra detta.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Rutinen för registrering och avregistrering av användare bör innefatta: a) användning av unik användar-id för att möjliggöra för användare att bli knutna till och göras ansvariga för sina åtgärder. Användning av grupp-id bör tillåtas endast där det är nödvändigt av verksamhets- eller driftskäl och bör då godkännas och dokumenteras; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
2.	b) kontroll av att användaren har systemägarens tillstånd att utnyttja informationssystemet eller tjänsten; särskilt godkännande fån ledningen för åtkomst kan också vara tillämpligt; Kommentar:			
3.	c) kontroll av att den tilldelade åtkomstnivån är anpassad till verksamhetens ändamål (se 11.1) och överensstämmer med organisationens säkerhetspolicy t.ex. så att segregering av arbetsuppgifter inte äventyras (se 10.1.3); Kommentar:			
4.	d) ge skriftligt besked till användarna om tilldelade rättigheter till åtkomst; Kommentar:			
5.	e) krav på att användare undertecknar förbindelse som visar att de förstår reglerna för åtkomst; Kommentar:			
6.	f) säkerställa att tjänsteuppdragstagare inte tillåter åtkomst förrän tillståndsrutinen fullgjorts; Kommentar:			
7.	g) upprätta ett formellt register över alla personer med åtkomsttillstånd; Kommentar:			
8.	h) omgående ta bort eller blockera åtkomsträtten för användare som har bytt roller eller arbetsuppgifter eller lämnat organisationen; Kommentar:			
9.	i) periodiskt kontrollera och avlägsna eller blockera redundanta användar-id och konton (se 11.2.4); Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
10.	j) säkerställa att inaktuella användaridentiteter inte tilldelas andra användare. Kommentar:			

Övrig information

Organisationen bör överväga att fastställa användares roller vad avser åtkomst baserade på verksamhetskrav där ett antal åtkomsträtter förs samman till standardprofiler för användaråtkomst. Begäran om åtkomst och granskning (se 11.2.4) är lättare att hantera med en sådan utgångspunkt än om individuella rättigheter ges.

Klausuler i anställningsavtal och tjänsteavtal bör övervägas som preciserar sanktioner om obehöriga åtkomstförsök görs av egen eller tjänsteleverantörs personal (se också 6.1.5, 8.1.3 och 8.2.3).

11.2.2 Hantering av särskilda rättigheter

	Nivå
Tilldelning och användning av privilegierad åtkomsträtt bör begränsas och styras. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan rutiner för att hantera åtkomsträttigheter ökar risken för att användare får högre rättigheter än de behöver.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Fleranvändarsystem som ställer krav på skydd mot obehörig åtkomst bör styras med avseende på tilldelade privilegier genom en formell process. Kommentar:			
2.	Följande steg bör övervägas: a) åtkomstprivilegier som avser enskilda system, t.ex. operativsystem, databassystem och individuella tillämpningar och de användare till vilka de bör hänföras, bör fastställas; Kommentar:			
3.	b) privilegier bör tilldelas användare efter behov (”behov att känna till”) och för enstaka händelser i linje med åtkomstpolicyn (11.1.1), d.v.s. minimikraven för deras arbetsuppgifter och endast när det behövs; Kommentar:			
4.	c) en rutin för tilldelning av behörighet och ett register över alla meddelade privilegier bör hållas aktuellt. Särskilda rättigheter bör inte beviljas förrän tillståndsrutinen är färdig; Kommentar:			
5.	d) utveckling och användning av systemrutiner bör föredras för att undvika behov av att medge särskilda rättigheter till användare; Kommentar:			
6.	e) utveckling och användning av program som undviker behovet att utnyttja privilegier bör främjas; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	f) privilegier bör tilldelas med användning av annan användaridentitet än den som utnyttjas i den normala verksamheten. Kommentar:			

Övrig information

Olämplig användning av administratörsrättigheter för system (egenskap eller resurser hos ett informationssystem som möjliggör för användaren att förbigå system- eller tillämpningskontroller) kan vara en viktig bidragande faktor till fel eller intrång i system.

11.2.3 Lösenordshantering

	Nivå
Tilldelning av lösenord bör styras genom en formell administrativ process. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan en formell process för tilldelning av lösenord ökar risken för att lösenord "stjäls" och används på ett skadligt sätt.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Rutinen bör omfatta följande krav: a) det bör krävas att användare undertecknar en förbindelse att hålla personliga lösenord hemliga och grupplösenord enbart inom gruppen; en sådan signerad förklaring kan tas in bland anställningsvillkoren (se 8.1.3); Kommentar:			
2.	b) när det krävs av användarna att förvalta sina egna personliga lösenord bör de först förses med ett säkert tillfälligt lösenord (se 11.3.1), som de är tvingade att omedelbart ändra; Kommentar:			
3.	c) inför rutiner för att kontrollera en användares identitet innan ett nytt, ett ersättnings- eller ett temporärt lösenord tilldelas; Kommentar:			
4.	d) tillfälliga lösenord bör tilldelas användare på ett säkert sätt; användning av tredje parts eller oskyddat (klartext) e-postmeddelande bör undvikas; Kommentar:			
5.	e) tillfälliga lösenord bör vara unika för personen och inte möjliga att gissa; Kommentar:			
6.	f) användare bör kvittera mottagande av lösenord; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	g) lösenord bör aldrig registreras i datorsystem i oskyddad form; Kommentar:			
8.	h) av leverantör tilldelat tillfälligt lösenord bör ändras så snart systemet eller programmet installerats. Kommentar:			

Övrig information

Lösenord är en vanlig metod att verifiera en användares identitet för rätt till åtkomst till ett informationssystem eller en tjänst i enlighet med användarens behörighet. Andra tekniker för identifiering och autenticering av användare som biometriska metoder t.ex. verifiering genom fingeravtryck, signaturverifiering och användning av hårdvarunycklar, t.ex. aktiva kort finns och bör övervägas om det är lämpligt.

11.2.4 Granskning av användares åtkomsträttigheter

	Nivå
Ansvariga chefer bör granska användares åtkomsträttigheter med jämna mellanrum genom en formell process. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan regelbunden granskning av åtkomsträttigheter ökar risken att användare får behålla onödigt hög behörighet. Oanvända användarkonton som finns kvar i systemet kan också användas av angripare.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

	Nivåstyrande frågor	JA	NEJ	VET EJ
1.	Vid granskning av åtkomsträtter bör följande riktlinjer beaktas: a) användares åtkomstmöjligheter bör granskas med regelbundna intervall, t.ex. var sjätte månad och efter förändring, såsom befordran, degradering eller avslut av anställning (se 11.2.1); Kommentar:			
2.	b) användares åtkomsträtt bör granskas och omfördelas när en anställd flyttar från en befattning till en annan inom samma organisation; Kommentar:			
3.	c) behörighet för särskild, privilegierad åtkomsträtt (se 11.2.2) bör granskas med tätare tidsintervall, t.ex. var tredje månad; Kommentar:			
4.	d) fördelning av särskilda rättigheter bör kontrolleras med jämna mellanrum för att säkerställa att rättigheterna inte har erhållits obehörigt; Kommentar:			
5.	e) ändring av konton med särskilda rättigheter bör loggas för periodisk granskning. Kommentar:			

Övrig information
Det är nödvändigt att regelbundet granska användares åtkomsträtter för att bibehålla effektiv kontroll över åtkomst till data och informationstjänster.

11.3 Användares ansvar

Mål: Att förhindra obehörig användaråtkomst och kompromettering eller stöld av information och informationsbehandlingsresurser.

De behöriga användarnas medverkan är väsentlig för en effektiv säkerhet.

Användarna bör göras medvetna om sitt ansvar för att upprätthålla en effektiv styrning av åtkomst särskilt när det gäller användning av lösenord och säkerheten för användarutrustning.

En policy som kräver ”renstädat skrivbord och tom bildskärm” bör införas för att minska risken för otillåten åtkomts till eller skada på pappersdokument, media och informationsbehandlingsresurser.

11.3.1 Användning av lösenord

	Nivå
Användare bör följa god säkerhetssed vid val och användning av lösenord. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan god säkerhetssed vid val av lösenord ökar risken för otillåtna inloggningar och försämrad tillförlitlighet (användning av ”stulna” inloggningsuppgifter).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Alla användare bör rådas att: a) hålla lösenord hemliga; Kommentar:			
2.	b) undvika att dokumentera lösenord (på t.ex. papper, i datafiler, eller handburna enheter) om de inte kan förvaras helt säkert och metoden för förvaring har godkänts; Kommentar:			
3.	c) genast ändra lösenord när det finns indikation om att system- eller lösenordssäkerheten möjligen har äventyrats;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	d) välja bra lösenord med tillräcklig minimumlängd som: 1) är lätta att komma ihåg 2) inte har något samband med något som någon annan lätt kan gissa sig till eller härleda ur information med anknytning till innehavaren, t.ex. namn, telefonnummer, födelsedatum etc. 3) inte är sårbart för ordboksattacker (d.v.s. inte består av ord som finns i ordböcker) 4) inte innehåller identiska tecken i följd eller är helt numeriska eller helt alfabetiska. Kommentar:			
5.	e) ändra lösenord regelbundet eller på grundval av användningsfrekvens (lösenord för privilegierad åtkomst bör ändras oftare än ”normala” lösenord) och undvika att återanvända lösenord eller cykliskt förändra lösenord; Kommentar:			
6.	f) ändra tillfälliga lösenord vid första påloggningen; Kommentar:			
7.	g) att inte lägga in lösenordet i något automatiskt påloggningsförfarande, t.ex. lagrad i ett makro eller i en funktionstangent; Kommentar:			
8.	h) inte dela personliga lösenord till någon annan; Kommentar:			
9.	i) inte använda samma lösenord för organisationens ändamål som för privata ändamål. Kommentar:			
10.	Om användare behöver åtkomst till flera tjänster, system eller plattformar och därför måste ha flera lösenord bör de ges rådet att de får använda ett enda lösenord av bra kvalitet (se d) ovan) för alla tjänster där användaren är övertygad om att en rimlig skyddsnivå har upprättas för lagringen av lösenordet inom varje tjänst, system eller plattform.			

Nivåstyrande frågor		JA	NEJ	VET EJ
	Kommentar:			

Övrig information
Hantering av system med supportfunktion för förlorade eller bortglömda lösenord kräver särskild omsorg eftersom det också kan innebära en metod att angripa lösenordssystemet.

11.3.2 Obevakad användarutrustning

	Nivå
Användare bör säkerställa att obemannad utrustning har tillräckligt skydd. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Ökad risk för obehörig åtkomst till system och information och även för förlust av eller skada på utrustning.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Alla användare bör uppmärksammas på säkerhetskraven och rutinerna för att skydda obevakad utrustning liksom även på sitt ansvar för att införa sådant skydd. Kommentar:			
2.	Användare bör rådas att: a) avsluta aktiva program när användningen upphör såvida programmen inte kan låsas på lämpligt sätt, t.ex. genom lösenordsskyddad skärmsläckare; Kommentar:			
3.	b) logga av stordatorer, servrar och kontorsdatorer när bearbetningssessionen avslutats (d.v.s. inte bara stänga av persondatorns bildskärm eller terminalen); Kommentar:			
4.	c) skydda persondatorer och terminaler mot obehörig åtkomst, när de inte används, med fysiskt lås eller motsvarande skydd, t.ex. lösenord (se även 11.3.3). Kommentar:			

Övrig information

Utrustning installerad i användares utrymmen, t.ex. arbetsstationer eller servrar, kan behöva särskilt skydd mot obehörig åtkomst när de lämnas utan tillsyn under en längre tid.

11.3.3 Policy för renstädat skrivbord och tom bildskärm

	Nivå
En policy, för renstädat skrivbord utan pappersdokument och flyttbara datamedia liksom en policy för tom bildskärm för informationsbehandlingsresurser, bör antas. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan en policy för rent skrivbord och ren bildskärm ökar risker för att någon obehörig tar del av, förvanskar eller förstör information. Detta gäller både under och efter normal arbetstid. Datamedia som ligger löst på skrivbordet är oskyddad mot katastrofer som en brand, jordbävning, översvämning eller explosion.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Policyn för renstädat skrivbord och tom bildskärm bör ta hänsyn till informationsklassificeringen (se 7.2), legala krav och avtalskrav (se 15.1), och de tillhörande riskerna och organisationskulturen.			
2.	Följande riktlinjer bör övervägas: a) för verksamheten känslig eller kritisk information, t.ex. på pappersdokument eller elektroniska lagringsmedia bör låsas in (helst i kassaskåp eller brandskyddat skåp eller annan typ av säkerhetsmöbel) när den inte behövs, särskilt när kontoret är obemannat; Kommentar:			
3.	b) datorer och terminaler bör lämnas avloggade eller skyddade med låsmekanism för bildskärm och tangentbord skyddade med lösenord, aktivt kort eller liknande autenticeringsfunktion när de är obevakade och bör skyddas av nyckellås, lösenord eller andra medel när de inte är i bruk; Kommentar:			
4.	c) platser för inkommande och utgående post liksom obemannade fax-maskiner bör skyddas;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
5.	d) obehörig användning av kopieringsmaskiner och annan reproduktionsteknologi (t.ex. scanners, digitalkameror) bör förhindras; Kommentar:			
6.	e) dokument innehållande känslig eller hemlig information bör avlägsnas ur skrivare omedelbart efter utskrift. Kommentar:			

Övrig information

En policy för renstädat skrivbord och tom bildskärm minskar risken för obehörig åtkomst, förlust och skada på information under och utanför normal arbetstid. Kassaskåp eller annan form av säker förvaring kan också skydda information lagrad i dem mot olyckor som brand, jordbävning, översvämning eller explosion.

Överväg att använda skrivare med en funktion som kräver en personlig kod så att upphovsmännen till dokumentet är de enda som kan få utskrifter och endast när de befinner sig intill skrivaren.

11.4 Styrning av åtkomst till nätverk

Mål: Att förhindra obehörig åtkomst till nätverkstjänster.

Åtkomst till både interna och externa nätverkstjänster bör styras.

Användaråtkomst till nätverk och nätverkstjänster bör inte äventyra nätverkstjänsternas säkerhet, genom att säkerställa:

a) att det finns lämpliga gränssnitt mellan organisationens nätverk och nätverk som ägs av andra organisationer och publika nät

b) att lämpliga autenticeringsmetoder används för användare och utrustningar

c) att kontroll av användares åtkomst till informationstjänster är i funktion.

11.4.1 Policy för användning av nätverkstjänster

	Nivå
Användare bör förses med åtkomst endast till de tjänster som de särskilt fått behörighet att använda. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan en tydlig policy för nätverkstjänster ökar risken för obehöriga och osäkra anslutningar. Detta innebär hög risk för nätverksanslutningar till känsliga eller kritiska företagsapplikationer eller för användare på riskfyllda platser, t.ex. offentliga eller externa områden.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	En policy bör utformas för användning av nätverk och nätverkstjänster. Den bör omfatta: a) nätverk och nätverkstjänster till vilka åtkomst medges; Kommentar:			
2.	b) behörighetsrutin för att avgöra vem som medges åtkomst till vilka nätverk eller vilka nätverkstjänster; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
3.	c) Säkerhetsåtgärder och rutiner för att skydda åtkomst till nätverksanslutningar och nätverkstjänster; Kommentar:			
4.	d) de metoder som används för åtkomst till nätverk och nätverkstjänster (t.ex. villkoren för att tillåta uppringd åtkomst till en leverantör av Internettjänster eller ett fjärrsystem). Kommentar:			
5.	Policyn för användning av nätverkstjänster bör vara förenlig med verksamhetens åtkomstpolicy (se 11.1). Kommentar:			

Övrig information

Obehöriga och osäkra uppkopplingar till nätverkstjänster kan påverka hela organisationen. Denna säkerehtsåtgärd är särskilt viktig för nätverksanslutning av känsliga eller kritiska verksamhetstillämpningar liksom av användare i högrisklokaler, t.ex. dit allmänheten har tillträde eller yttre utrymmen där säkerheten inte hanteras och styrs av organisationen.

11.4.2 Autenticering av användare vid extern anslutning

	Nivå
Lämpliga autenticeringsmetoder bör användas för att styra fjärranvändares åtkomst. *Kritisk säkerhetsåtgärd: JA* *Risk: Externa anslutningar gör det möjligt för obehöriga att komma åt företagsinformation.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Autenticering av externa användare kan göras t.ex. genom krypteringsteknik, aktivt kort eller ett anrops/svarsprotokoll. Möjliga tillämpningar av sådana tekniker finns i olika virtuella privata nätverkslösningar (VPN). Dedicerade privata linjer kan också användas för att säkerställa anslutningens ursprung. Kommentar:			
2.	Motringningsrutiner och -åtgärder, t.ex. genom motringningsmodem kan erbjuda skydd mot obehörig anslutning till en organisations informationsbehandlingsresurser. Denna typ av åtgärd autenticerar användare som försöker ansluta till en organisations nätverk externt. När denna metod används bör en organisation inte använda nätverkstjänster som omfattar vidarebefordran av anrop, eller om de gör så, bör de koppla ur användningen av sådana egenskaper för att undvika svagheter som hänger samman med vidarebefordran. Motringningsförfarandet bör säkerställa att nedkoppling på organisationens sida sker. I annat fall skulle den yttre användaren kunna hålla förbindelsen öppen och simulera att verifiering av motringning har skett. Rutiner och åtgärder för motringning bör av detta skäl testas noga. Kommentar:			
3.	Autenticering av nod kan också tjäna som en alternativ autenticeringsmetod för grupper av externanslutna användare om de är anslutna till en säker, gemensam datorresurs. Krypteringsteknik, t.ex. baserad på maskincertifikat, kan utnyttjas för autenticering av nod. Detta är en del av flera VPN-baserade lösningar. Kommentar:			
4.	Ytterligare säkerhetsåtgärder för autenticeringen bör införas för att styra åtkomst till trådlösa nätverk. Särskild omsorg är i synnerhet			

Nivåstyrande frågor		JA	NEJ	VET EJ
	nödvändig vid val av säkerhetsåtgärder för trådlösa nätverk beroende på de större möjligheterna till oupptäckt uppsnappande och tillägg av nätverkstrafik. Kommentar:			

Övrig information

Externa anslutningar erbjuder möjlighet till obehörig åtkomst till verksamhetsinformation, t.ex. genom uppringningsmetoder. Det finns olika typer av metoder för autenticering, vissa av dem ger högre grad av skydd än andra t.ex. så kan metoder baserade på krypteringsteknik ge stark autenticering. Det är viktigt att bestämma erforderlig skyddsnivå med hjälp av riskbedömning. Detta behövs för att välja lämplig autenticeringsmetod.

Möjligheten till automatisk uppkoppling till en extern dator kan medföra obehörig åtkomst till en tillämpning. Detta är särskilt viktigt att beakta om anslutningen utnyttjar ett nätverk där säkerheten inte hanteras och styrs av organisationen.

11.4.3 Identifiering av utrustning i nätverk

	Nivå
Automatisk identifiering av utrustning bör övervägas som en metod att autenticera anslutningar från olika platser och utrustningar. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om utrustningen inte identifieras, kan det leda till obehörig åtkomst till nätverk, system eller information.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Identifiering av utrustning kan användas om det är viktigt att kommunikationen endast kan initieras från en speciell plats eller utrustning. En identifierare i eller ansluten till utrustningen kan användas för att indikera om utrustningen tillåts ansluta till nätverket. Dessa identifierare bör klart visa till vilket nätverk utrustningen tillåts ansluta om det finns mer än ett nätverk och särskilt om nätverken har olika känslighet. Det kan vara nödvändigt att överväga fysiskt skydd av utrustningen för att bibehålla utrustningsidentifierarens säkerhet. Kommentar:			

Övrig information

Denna säkerhetsåtgärd kan kompletteras med andra tekniker för att autenticera utrustningens användare (se 11.4.2). Utrustningsidentifierare kan användas som tillägg till användarautenticering.

11.4.4 Skydd av extern diagnos- och konfigurationsport

	Nivå
Fysisk och logisk åtkomst till diagnos- och konfigurationsportar bör styras. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om dessa portar lämnas oskyddade utgör de en risk för obehörig åtkomst.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Tänkbara säkerhetsåtgärder för att styra åtkomst till diagnos- och konfigurationsportar innefattar användning av nyckellås och stödrutiner för att styra den fysiska åtkomsten till porten. Ett exempel på en sådan stödrutin är att säkerställa att diagnos- och konfigurationsportar endast är åtkomliga genom överenskommelse mellan den ansvarige för datortjänsten och den servicepersonal för datortjänsten och program som behöver åtkomst. Kommentar:			
2.	Portar, tjänster och liknande resurser som är installerade på en dator eller nätverksutrustning och som inte särskilt krävs för verksamheten bör stängas av eller tas bort. Kommentar:			

Övrig information
Många datorsystem, nätverkssystem och kommunikationssystem har installerats med en diagnostik- eller konfigurationsanordning att användas externt av servicetekniker. Om de är oskyddade utgör dessa portar ett medel för obehörig åtkomst.

11.4.5 Nätverkssegmentering

	Nivå
Grupper av informationstjänster, användare och informationssystem bör åtskiljas i nätverk. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan nätverkssegmentering ökar risken för attacker mellan olika typer av användare och system. Anslutningar till andra nätverk kan öka risken för obehörig åtkomst i existerande informationssystem som använder nätverket, av vilka vissa kan kräva skydd från andra nätverksanvändare på grund av att systemen är känsliga eller kritiska.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Ett sätt att styra säkerheten i stora nätverk är att dela dem i separata logiska nätverksdomäner, t.ex. en organisations externa respektive interna domän, var och en skyddad av en definierad yttre säkerhetsanordning. En graderad uppsättning säkerhetsåtgärder kan tillämpas i olika logiska nätverksdomäner för att ytterligare skilja de olika nätverkssäkerhetsmiljöerna åt, t.ex. öppna system, interna nätverk och kritiska tillgångar. Domänerna bör definieras med utgångspunkt från en riskbedömning och de olika säkerhetskraven inom var och en av domänerna. Kommentar:			
2.	Ett sådant perimeterskydd för nätverk kan åstadkommas genom att installera en säker brygga mellan två nätverk som ska sammankopplas för att kontrollera åtkomst och informationsflöden mellan de två domänerna. Denna brygga bör konfigureras så att den filtrerar trafik mellan dessa domäner (se 11.4.6 och 11.4.7) och blockerar obehörig åtkomst i enlighet med organisationens policy för åtkomstkontroll. (se 11.1). Ett exempel på en sådan typ av brygga är det som vanligen benämns brandvägg. En annan metod för att skilja separata logiska domäner är att begränsa nätverksåtkomst genom att använda virtuella privata nätverk för användargrupper inom organisationen. Kommentar:			
3.	Nätverk kan också skiljas åt genom att använda nätverksfunktioner, t.ex. IP-switching. Separata domäner kan då användas genom att styra nätverkets dataflöde via användning av routnings-/omkopplingsmöjligheter som t.ex. listor för styrning av åtkomst.			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	Kriterierna för att dela upp nätverk i domäner bör baseras på åtkomstpolicyn och åtkomstkraven (se 10.1), och även ta hänsyn till den relativa kostnaden och inverkan på prestanda av att införa lämplig teknik för dirigering av trafik eller nätverksbryggor (se 11.4.6 och 11.4.7) Kommentar:			
5.	Dessutom bör uppdelning av nätverk baseras på värde och klassificering av den information som lagras eller bearbetas i nätverket, förtroendenivåer eller verksamhetsområden i syfte att reducera den totala påverkan från en störning av tjänsten. Kommentar:			
6.	Uppdelning av trådlösa nätverk från interna och privata nätverk bör övervägas. Eftersom säkerhetsgränserna i trådlösa nätverk inte är väl definierade bör en riskbedömning göras i sådana fall för att fastställa vilka medel som behövs för att bibehålla uppdelningen mellan nätverk (t.ex. stark autenticering, krypteringsmetoder och frekvensval). Kommentar:			

Övrig information

Eftersom samarbeten etableras mellan organisationer utsträcks nätverk i allt högre grad utanför traditionella organisationsgränser. Detta kan kräva att utrustning för informationsbehandling och nätverksresurser sammankopplas eller används gemensamt. Den sortens utvidgning av nätverk kan öka risken för obehörig åtkomst i existerande informationssystem som använder nätverket, av vilka vissa kan kräva skydd från andra nätverksanvändare på grund av att systemen är känsliga eller kritiska.

11.4.6 Styrning av nätverksanslutning

	Nivå
När det gäller delade nätverk, särskilt sådana som sträcker sig över organisationsgränser, bör användares möjligheter att ansluta sig till nätverket begränsas i enlighet med åtkomstpolicyn och verksamhetstillämpningarnas krav (se 11.1). *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan åtkomstpolicy, ökar risken för att användare besitter högre rättigheter än de behöver, vilket leder till obehörig åtkomst och kan förvärra skadan av en attack.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Användares rätt till nätverksåtkomst bör upprätthållas och uppdateras i enlighet med åtkomstpolicyn (se 11.1.1). Kommentar:			
2.	Användares uppkopplingsmöjligheter kan begränsas genom nätverksportar som filtrerar trafiken genom fördefinierade tabeller eller regler. Exempel på tillämpningar där restriktioner bör finnas är: a) meddelandehantering, t.ex. elektroniskpost; Kommentar:			
3.	b) filöverföring; Kommentar:			
4.	c) interaktiv åtkomst; Kommentar:			
5.	d) tillämpningsåtkomst. Att koppla åtkomsträtt för nätverk till vissa tidpunkter under dagen eller vissa dagar bör övervägas. Kommentar:			

Övrig information

Åtkomstpolicyn till delade nätverk, särskilt de som sträcker sig över organisationsgränser, kan kräva att säkerhetsåtgärder införs för att begränsa användarnas uppkopplingsmöjlighet.

11.4.7 Styrning av routning

	Nivå
Säkerhetsåtgärder för routning bör införas för nätverk för att säkerställa att datoruppkopplingar och informationsflöden inte bryter mot åtkomstpolicyn till verksamhetstillämpningarna. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan åtkomstpolicy ökar risken att användare besitter högre rättigheter än de behöver, vilket kan leda till obehörig åtkomst och kan förvärra skadan av en attack.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Säkerhetsåtgärder för routning bör baseras på kontrollmekanismer för positiva avsändar- och destinationsadresser. Kommentar:			
2.	Säkerhetsportar kan utnyttjas för att validera avsändar- och destinationsadresser vid interna och externa kontrollpunkter i nätet om proxy och/eller tekniker för översättning av nätverksadresser används De som inför sådana lösningar bör vara medvetna om styrka och svagheter hos den valda metoden. Kraven på styrning av routning i nätverk bör baseras på åtkomstpolicyn (se 11.1). Kommentar:			

Övrig information
Delade nätverk och då särskilt sådana som sträcker sig över organisationsgränser kan ställa krav på ytterligare styrning av routning. Detta gäller särskilt när nätverk delas med tredjepartanvändare (ej tillhörande organisationen).

11.5 Styrning av åtkomst till operativsystem

Mål: Att förhindra obehörig åtkomst till operativsystem.

Säkerhetsanordningar bör användas för att begränsa åtkomsten till operativsystem till endast behöriga användare. Dessa anordningar bör kunna klara av följande:

a) autenticera behöriga användare i enlighet med en definierad åtkomstpolicy

b) registrera lyckade och misslyckade försök till autenticering av system

c) registrera användningen av särskilda systemrättigheter

d) slå larm vid avvikelser från systemsäkerhetspolicyer

e) tillhandahålla lämpliga medel för autenticering

f) i tillämpliga fall begränsa användarens uppkopplingstid.

11.5.1 Säker påloggningsrutin

	Nivå
Åtkomst till operativsystem bör styras genom en säker påloggningsrutin. *Kritisk säkerhetsåtgärd: JA* *Risk: Om inga säkra påloggningsrutiner finns, kan en obehörig användare komma åt företagets information och system.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Rutinen för påloggning till ett operativsystem bör utformas för att minimera möjligheterna till obehörig åtkomst. Påloggningsrutinen bör därför avslöja ett minimum av information om systemet för att undvika att en obehörig användare får onödig hjälp. En bra påloggningsrutin bör: a) inte visa identitetsbegrepp för system eller tillämpningar förrän en lyckad påloggning slutförts; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
2.	b) visa en allmän kommentar som varnar för att endast behöriga användare bör ha åtkomst till datorn; Kommentar:			
3.	c) inte lämna hjälpmeddelanden under påloggningsrutinen som skulle kunna hjälpa en obehörig användare; Kommentar:			
4.	d) validera påloggningsinformationen först sedan alla data inmatats. Om ett fel uppstår bör systemet inte avslöja vilka data som är riktiga respektive felaktiga; Kommentar:			
5.	e) begränsa det tillåtna antalet misslyckade påloggningsförsök till t.ex. tre försök och överväga att: 1) registrera misslyckade och lyckade försök; 2) lägga in en tidsfördröjning innan nya påloggningsförsök tillåts, eller avvisa ytterligare försök utan särskild behörighet; 3) koppla ner förbindelsen; 4) sända ett larmmeddelande till systemkonsolen om det maximala antalet påloggningsförsök har nåtts; 5) bestämma antalet lösenordsförsök i kombination med lösenordets minsta längd och värdet av det system som skyddas; Kommentar:			
6.	f) begränsa längsta och kortaste tid som tillåts för påloggningsrutinen. Om den överskrids bör systemet avsluta påloggningen; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
7.	g) visa följande information sedan lyckad påloggning skett: 1) tidpunkt och datum för närmast föregående lyckade påloggningen; 2) detaljer om eventuella misslyckade påloggningsförsök efter senaste lyckade påloggning; Kommentar:			
8.	h) inte visa lösenordet som införs eller överväga att gömma lösenordstecknen med symboler; Kommentar:			
9.	i) inte överföra lösenord i klartext över ett nätverk. Kommentar:			

Övrig information
Om lösenord sänds i klartext under påloggning över ett nätverk kan det snappas upp av ett ”avlyssnings”-program på nätet.

11.5.2 Identifiering och autenticering av användare

	Nivå
Varje användare bör ha en unik identifikation (användar-ID) enbart för deras personliga användning och en lämplig autenticeringsteknik bör väljas för att styrka användarens uppgivna identitet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan lämplig autentiseringsteknik ökar möjligheten för obehörig åtkomst och möjligheter att kringgå segregering av uppgifter.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Denna säkerhetsåtgärd bör tillämpas för alla typer av användare (inklusive teknisk supportpersonal, operatörer, nätverksadministratörer, programmerare och databasadministratörer). Kommentar:			
2.	Användar-ID bör användas för att spåra aktiviteter till den ansvariga individen. Normala användaraktiviteter bör inte utföras från konton med särskilda rättigheter. Kommentar:			
3.	I mycket speciella fall där det innebär en klar fördel för verksamheten, kan användningen av delad användar-ID tillämpas för en grupp användare eller för en särskild arbetsuppgift. Ledningens godkännande bör i dessa fall inhämtas och dokumenteras. Ytterligare säkerhetsåtgärder kan krävas för att klargöra ansvarsförhållanden. Kommentar:			
4.	Generiska användar-ID för användning av en individ bör endast tillåtas antingen när de funktioner som kan nås eller åtgärder utföras av en sådan ID inte behöver kunna spåras (t.ex. endast läsåtkomst) eller när det finns andra säkerhetsåtgärder (t.ex. lösenord för ett generiskt användar-ID som lämnas till en anställd åt gången och då loggning sker). Kommentar:			
5.	När stark autenticering och identitetsverifiering krävs bör andra autenticeringsmetoder än lösenord användas, såsom kryptering, smarta kort eller andra identifieringsbevis, eller biometriska			

Nivåstyrande frågor		JA	NEJ	VET EJ
	metoder. Kommentar:			

Övrig information

Lösenord (se också 11.3.1 och 11.5.3) är en mycket vanlig metod för att ge identifiering och autenticering baserad på en hemlighet som endast användaren känner till. Detsamma kan även uppnås med krypteringsmetoder och autenticeringsprotokoll. Tillvägagångssättet för användaridentifikation och autenticering bör vara anpassat till känsligheten hos den aktuella informationen.

Föremål som t.ex. smarta kort eller andra hårdvaruföremål användaren innehar kan också användas för identifiering och autenticering. Biometriska autenticeringstekniker som utnyttjar karaktäristika eller egenskaper hos en person kan också användas för att bekräfta personens identitet. En kombination av tekniker och mekanismer kombinerade på ett säkert sätt ger starkare autenticering.

11.5.3 Lösenordsrutin

	Nivå
System för att hantera lösenord bör vara interaktiva och bör säkerställa lösenord av god kvalitet. *Kritisk säkerhetsåtgärd: Nej* *Risk: Om inte lösenordspolicyn tillämpas automatiskt av systemet ökar risken att något använder ett lösenord som är känt eller av dålig kvalité, vilket kan leda till obehörig åtkomst och dålig spårbarhet (användare använder andra användares uppgifter).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Ett system för hantering av lösenord bör: a) tvinga till användning av personliga användaridentiteter och lösenord för att fastställa ansvarighet; Kommentar:			
2.	b) tillåta användare att välja och ändra sina egna lösenord och innehålla en rutin för bekräftelse för att tillåta felaktig inmatning; Kommentar:			
3.	c) framtvinga val av lösenord av god kvalitet (se 11.3.1); Kommentar:			
4.	d) tvinga till lösenordsändringar (se 11.3.1); Kommentar:			
5.	e) tvinga användare att ändra tillfälliga lösenord vid första påloggning (se 11.2.3); Kommentar:			
6.	f) föra ett register över tidigare använda lösenord och hindra återanvändning;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
7.	g) inte visa lösenord på skärmen när det skrivs in; Kommentar:			
8.	h) lagra lösenordsregistret skilt från tillämpningssystemets data; Kommentar:			
9.	i) lagra och överföra lösenord i skyddad form (t.ex. krypterad eller som hashvärde). Kommentar:			

Övrig information

Lösenord är ett av de viktigaste sätten att validera en användares rätt till åtkomst till en datorbaserad tjänst.

Vissa tillämpningar kräver att användares lösenord tilldelas av ett oberoende organ. I sådana fall är inte punkterna b), d) och e) ovan tillämpliga. I de flesta fall väljs och hanteras lösenord av användare. Se avsnitt 11.3.1 för vägledning gällande användning av lösenord.

11.5.4 Användning av systemverktyg

	Nivå
Användning av hjälpprogram som kan förbigå system- och tillämpningsspärrar bör användas restriktivt och styras noga. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Systemets hjälpprogram kan förbigå system och applikationskontroller och därmed möjliggöra obehörig åtkomst.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

	Nivåstyrande frågor	JA	NEJ	VET EJ
1.	Följande riktlinjer för användning av systemverktyg bör övervägas: a) användning av identifiering, autenticering och behörighetsrutiner för systemhjälpmedel; Kommentar:			
2.	b) att skilja systemverktyg från tillämpningsprogram; Kommentar:			
3.	c) att begränsa användningen av systemverktyg till så få pålitliga användare som möjligt (se också 11.2.2); Kommentar:			
4.	d) att ge behörighet för tillfällig användning av systemverktyg ; Kommentar:			
5.	e) att begränsa tillgången till systemverktyg, t.ex. till den tid det tar att genomföra en behörig ändring; Kommentar:			
6.	f) loggning av all användning av systemverktyg; Kommentar:			
7.	g) definition och dokumentation av behörighetsnivåer för systemverktyg;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
8.	h) ta bort eller stänga av alla onödiga systemprogram och programbaserade hjälpmedel; Kommentar:			
9.	i) att inte göra systemverktyg tillgängliga för användare som har tillgång till tillämpningar på system där uppdelning av arbetsuppgifter krävs. Kommentar:			

Övrig information

De flesta datorinstallationer har ett eller flera systemverktyg som kan åsidosätta skydd för system- och tillämpningar.

11.5.4 Tidsfördröjd nedkoppling

	Nivå
Inaktiva sessioner bör kopplas ned efter en fastställd period av inaktivitet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om sessioner inte kopplas ner automatiskt blir det möjligt för obehöriga att utföra överbelastningsattacker (Denial of Service).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	En mekanism för time-out bör rensa sessionsdata från skärmen och också, möjligen senare, släcka ner både tillämpnings- och nätverkssessioner efter en fastställd period av inaktivitet. Tidsfördröjningen för time-out bör återspegla säkerhetsrisken på platsen, den hanterade informationen och de använda tillämpningarna, klassificering och de risker som är knutna till utrustningens användare. Kommentar:			
2.	En begränsad variant av funktionen för tidsfördröjd nedkoppling kan tillhandahållas för vissa system. Den rensar skärmen och förhindrar obehörig åtkomst, men avslutar inte pågående tillämpnings- och nätverkssessioner. Kommentar:			

Övrig information

Denna säkerhetsåtgärd är av särskild vikt på platser med hög risk inklusive allmänna och externa områden utanför organisationens säkerhetskontroll. Sessionerna bör kopplas ner för att förhindra åtkomst av obehöriga personer och tillgänglighetsattacker.

11.5.5 Begränsning av uppkopplingstid

	Nivå
Begränsning i uppkopplingstid bör användas för att ge ytterligare säkerhet vid högrisktillämpningar. *Kritisk säkerhetsåtgärd: NEJ* *Risk:*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Styrning av uppkopplingstid bör övervägas för känsliga datortillämpningar, särskilt från högriskplatser t.ex. på publik eller extern plats där organisationen inte har kontroll över säkerheten. Exempel på sådana begränsningar är: a) användning av fördefinierade tidsfönster, t.ex. för att sända fil-batchar eller för regelbundna, kortvariga, interaktiva sessioner; Kommentar:			
2.	b) begränsning av uppkopplingstider till normal kontorstid om det inte finns krav på övertid eller drift utanför normal kontorstid; Kommentar:			
3.	c) överväga åter-autenticering med visst tidsintervall. Kommentar:			

Övrig information

Att begränsa den tidsperiod under vilken uppkoppling till datortjänster tillåts minskar tidsfönstret för obehörig åtkomst. Att begränsa varaktigheten av aktiva sessioner hindrar användare från att hålla sessioner öppna och därmed förhindra re-autenticering.

11.6 Styrning av åtkomst till information och tillämpningar

Mål: Att förhindra obehörig åtkomst av information i tillämpningssystem.

Säkerhetsmekanismer bör nyttjas för att begränsa åtkomst till och inom tillämpningssystem.

Logisk åtkomst till tillämpningsprogram och data bör begränsas till behöriga användare. Tillämpningssystem bör:

a) styra användares åtkomst till information och funktioner i tillämpningssystem enligt definierad åtkomstpolicy

b) ge skydd mot obehörig åtkomst via systemhjälpmedel och operativsystemprogram och mot skadlig programvara som har funktioner för att åsidosätta eller gå förbi systemets eller tillämpningssystemets styrning

c) inte äventyra säkerheten i andra system med vilka informationsresurser delas.

11.6.1 Begränsning av åtkomst till information

	Nivå
Användares och underhållspersonals åtkomst till information och tillämpningssystemens funktioner bör begränsas i enlighet med den definierade åtkomstpolicyn. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan tillräcklig applikationssäkerhet kan en obehörig användare komma åt företagsinformation och system.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Åtkomstbegränsning bör grundas på kraven i enskild verksamhetstillämpningar. Åtkomtspolicyn bör också överensstämma med organisationens åtkomstpolicy (se avsnitt 11.1). Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
2.	Tillämpning av följande riktlinjer bör övervägas som stöd för krav på begränsad åtkomst: a) sätta upp menyer för att styra åtkomst av tillämpningssystemets funktioner; Kommentar:			
3.	b) styra användarnas åtkomstmöjligheter, t.ex. läsa, skriva, radera och exekvera; Kommentar:			
4.	c) Styra åtkomsträttigheter gällande andra tillämpningar; Kommentar:			
5.	d) Säkerställa att det i resultat från tillämpningssystem som bearbetar känslig information endast ingår information relevant för användning av resultaten samt att data endast sänds till behöriga terminaler och platser. Detta bör innefatta regelbunden granskning av sådana resultat för att säkerställa att överflödig information tas bort. Kommentar:			

11.6.2 Isolering av känsliga system

Säkerhetsåtgärd

	Nivå
Känsliga system bör ha en dedikerad (isolerad) IT-miljö. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan isolering av känsliga system ökar risken för angrepp mellan olika kategorier av användare och system. Vidare kan en störning i ett system eller komponent påverka alla system som delar komponenten.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Följande punkter bör övervägas för isolering av känsliga system: a) ett tillämpningssystems känslighet bör explicit definieras och dokumenteras av tillämpningens ägare (se 7.1.2); Kommentar:			
2.	b) när ett känsligt system är avsett att köras i en delad miljö bör de tillämpningssystem med vilket resurser kommer att delas och motsvarande risker identifieras och godtas av den känsliga tillämpningens ägare. Kommentar:			

Övrig information

Vissa tillämpningssystem är tillräckligt känsliga för tänkbara förluster att de kräver särbehandling. Känsligheten kan visa att tillämpningssystemet:

a) bör köras på en dedikerad dator eller

b) endast dela resurser med tillförlitliga tillämpningssystem.

Isolering kan uppnås med fysiska eller logiska metoder (se också 11.4.5).

11.7 Mobil datoranvändning och distansarbete

Mål: Att säkerställa informationssäkerheten vid användning av mobil utrustning och utrustning för distansarbete.

Det skydd som krävs bör stå i proportion till de risker dessa särskilda arbetsmetoder orsakar. Vid mobil bearbetning bör risker med att arbeta i en oskyddad miljö beaktas och lämpligt skydd användas. Vid distansarbete bör organisationen använda skydd för arbetsplatsen och säkerställa att lämpliga anordningar är installerade för detta arbetssätt.

11.7.1 Mobil datoranvändning och kommunikation

	Nivå
En formell policy bör finnas och lämpliga säkerhetsåtgärder tillämpas för att skydda mot riskerna vid användning av mobil bearbetnings- och kommunikationsutrustning. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan fungerande policy för användandet av mobil utrustning ökar risken för att information avslöjas (till exempel någon som tjuvtittar på skärmen) eller stjäls. Det finns också risk för virusangrepp på till exempel bärbara datorer utan regelbundna anti-virus uppdateringar.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	När mobil utrustning för datorbehandling och kommunikation används, t.ex. notebooks, handdatorer, bärbara datorer och mobiltelefoner måste särskild försiktighet iakttas för att säkerställa att verksamhetsinformation inte äventyras. Policyn för mobil databehandling bör ta hänsyn till riskerna med att arbeta med utrustning för mobil databehandling i oskyddade miljöer. Kommentar:			
2.	Policyn för mobil databehandling bör omfatta krav på fysiskt skydd, styrning av åtkomst, krypteringsteknik, säkerhetskopiering och virusskydd. Denna policy bör också omfatta regler och råd vid uppkoppling av mobil utrustning till nätverk och vägledning för användning av dessa resurser på allmän plats. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
3.	Försiktighet bör iakttas när mobil datorutrustning används på allmän plats, i sammanträdesrum och på andra oskyddade platser utanför organisationens lokaler. Skydd bör finnas för att undvika obehörig åtkomst till eller avslöjande av information som lagras och behandlas av sådan utrustning t.ex. genom att använda krypteringsteknik (se 12.3). Kommentar:			
4.	Användare av mobil datorutrustning på allmän plats bör tänka på att undvika risken för obehöriga personers insyn. Rutiner för skydd mot skadliga program bör finnas och hållas uppdaterade (se 10.4). Kommentar:			
5.	Säkerhetskopior av verksamhetskritisk information bör tas regelbundet. Utrustning bör finnas tillgänglig för att möjliggöra snabb och enkel säkerhetskopiering av information. Dessa säkerhetskopior bör ges adekvat skydd mot t.ex. stöld eller informationsförlust. Kommentar:			
6.	Lämpligt skydd bör finnas vid användning av mobil utrustning ansluten till nätverk. Extern åtkomst till verk-samhetsinformation över öppna nät när mobil utrustning används bör endast ske efter positiv identifiering och autenticering och med lämplig mekanism för styrning av åtkomst installerad (se 11.4). Kommentar:			
7.	Mobil datorutrustning bör också skyddas fysiskt mot stöld särskilt om den lämnas utan tillsyn i t.ex. bilar och andra transportmedel, hotellrum, konferenscentra och möteslokaler. En särskild rutin som tar hänsyn till legala krav, försäkringskrav och andra säkerhetskrav inom organisationen bör upprättas för fall av stöld eller förlust av den mobila utrustningen. Utrustning som innehåller viktig, känslig och/eller kritisk verksamhetsinformation bör inte lämnas obevakad och, där det är möjligt, fysiskt låsas in eller låsas med speciallås för att säkra utrustningen (se 9.2.5). Kommentar:			
8.	Praktisk utbildning bör ordnas för personal som använder mobil databehandling för att öka deras kunskap om de ytterligare risker som uppstår vid detta sätt att arbeta och de säkerhetsåtgärder som bör införas. Kommentar:			

Övrig information

Trådlös anslutning till mobila nätverksresurser liknar andra typer av nätverksanslutningar men det finns viktiga skillnader som bör beaktas när medel för skydd fastställs. Typiska skillnader är

a) vissa protokoll avseende trådlös säkerhet är outvecklade och har kända svagheter;

b) information lagrad i mobila datorer kan ibland inte gå att säkerhetskopiera beroende på att nätverket har begränsad bandbredd och/eller därför att mobil utrustning inte är uppkopplad vid den tidpunkt när säkerhetskopieringen är inplanerad.

11.7.2 Distansarbete

	Nivå
Policy, driftsplan och rutiner bör utvecklas och införas för distansarbetsaktiviteter. *Kritisk säkerhetsåtgärd: Nej* *Risk: Utan fungerande policy för användandet av mobil utrustning ökar risken för att information avslöjas (till exempel någon som tjuvtittar på skärmen) eller stjäls. Det finns också risk för virusangrepp på till exempel bärbara datorer utan regelbundna anti-virus uppdateringar.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Organisationer bör endast tillåta distansarbete om de är säkra på att lämpliga säkerhetsanordningar och säkerhetsåtgärder finns på plats och att dessa överensstämmer med organisationens säkerhetspolicy. Kommentar:			
2.	Lämpligt skydd av distansarbetsplatsen bör finnas mot t.ex. stöld av utrustning och information, obehörigt avslöjande av information, obehörig extern åtkomst till organisationens interna system eller missbruk av resurser. Distansarbete bör vara både godkänt och styrt av ledningen och det bör säkerställas att lämpliga arrangemang vidtagits för detta sätt att arbeta. Kommentar:			
3.	Följande bör övervägas: a) den befintliga fysiska säkerheten hos distansarbetsplatsen med beaktande av byggnadens och den lokala miljöns fysiska säkerhet; Kommentar:			
4.	b) distansarbetsplatsens föreslagna fysiska miljö; Kommentar:			
5.	c) kommunikationssäkerhetskraven med beaktande av behovet av extern åtkomst till organisationens interna system, känsligheten hos den information till vilken åtkomst kommer att ske och som kommer att vidarebefordras via kommunikationslänken, samt känsligheten hos det interna systemet;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
6.	d) hotet avseendeobehörig åtkomst till information eller resurser från andra personer som finns på platsen, t.ex. familj och vänner; Kommentar:			
7.	e) användningen av hemmanätverk och krav eller begränsningar vad avser konfigurationen av trådlös nätverkstjänst; Kommentar:			
8.	f) policyer och rutiner för att förhindra tvist om rättigheter till immateriell egendom utvecklad på privatägd utrustning; Kommentar:			
9.	g) åtkomst till privatägd utrustning (för att kontrollera utrustningssäkerheten eller under en utredning), för vilken juridiska hinder kan föreligga; Kommentar:			
10.	h) programvarulicensavtal utformade så att organisationen kan bli skyldig att betala licens för klientprogram på arbetsstationer som ägs privat av anställda, uppdragstagare eller tredjepartsanvändare; Kommentar:			
11.	i) krav på virusskydd och brandväggar. Kommentar:			
12.	Riktlinjer och arrangemang att överväga bör omfatta: a) att tillhandahålla lämplig utrustning och förvaringsmöbler för distansarbete, då användning av privatägd utrustning utanför organisationens kontroll inte är tillåten; Kommentar:			
13.	b) en definition av tillåtet arbete, arbetstiden och klassificering av information som distansarbetare får förfoga över och de interna system och tjänster som distansarbetaren har behörighet till; Kommentar:			
14.	c) tillgång till lämplig kommunikationsutrustning innefattande metoder för att säkra extern åtkomst;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
15.	d) fysisk säkerhet; Kommentar:			
16.	e) regler och vägledning för familjens och besökares åtkomst till utrustning och information; Kommentar:			
17.	f) tillgång till stöd och underhåll av maskin- och programvara; Kommentar:			
18.	g) tillgång till försäkring; Kommentar:			
19.	h) rutiner för säkerhetskopiering och kontinuitet i verksamheten; Kommentar:			
20.	i) revision och säkerhetsövervakning; Kommentar:			
21.	j) återkallande av befogenheter och åtkomsträttigheter liksom återlämnande av utrustning när distansarbetsuppgifterna upphör. Kommentar:			

Övrig information

Vid distansarbete används kommunikationsteknik för att göra det möjligt att arbeta på en bestämd plats utanför organisationens lokaler.

12. Anskaffning, utveckling och underhåll av informationssystem

12.1 Säkerhetskrav på informationssystem

Mål: Att säkerställa att säkerheten är en integrerad del av informationssystem.

Informationssystem omfattar operativsystem, infrastruktur, verksamhetstillämpningar, inköpta standardprodukter, tjänster och användarutvecklade tillämpningar. Utformningen och införandet av informationssystem som stödjer verksamhetsprocessen kan vara avgörande för säkerheten. Säkerhetskrav bör identifieras och beslutas innan utveckling och/eller införande av informationssystem sker.

Alla säkerhetskrav bör identifieras under ett projekts kravspecifikationsfas och motiveras, beslutas och dokumenteras som ett led i den överordnade nyttoanalysen för ett informationssystem.

12.1.1 Analys och specifikation av säkerhetskrav

	Nivå
Uttalanden om verksamhetens krav på nya informationssystem eller förbättring av befintliga informationssystem bör specificera kraven gällande säkerhetsåtgärder. *Kritisk säkerhetsåtgärd: JA* *Risk: Dålig hantering av systemskydd kan leda till säkerhetsincidenter. Utan dokumenterade säkerhetskrav i början av ett systemutvecklingsprojekt, ökar risker för högre kostnader och förseningar.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	När kraven gällande säkerhetsåtgärder specificeras bör de automatiska funktioner som kan ingå i informationssystemet övervägas liksom behovet av stödjande manuella säkerhetsåtgärder. Liknande överväganden bör tillämpas vid utvärdering av			

Nivåstyrande frågor		JA	NEJ	VET EJ
	programvarupaket, utvecklade eller inköpta, för verksamhetstillämpningar. Kommentar:			
2.	Säkerhetskrav och säkerhetsåtgärder bör återspegla värdet av de berörda informationstillgångarna (se också 7.2) och den tänkbara skada på verksamheten som kan bli resultatet av felaktigheter eller brist på säkerhet. Kommentar:			
3.	Systemkrav ifråga om informationssäkerhet och processer för att införa säkerhet bör ingå i de tidiga faserna av informationssystemprojekt. Säkerhetsåtgärder som införs vid systemutformningen blir betydligt billigare att införa och underhålla än sådana som införs under eller efter systemets implementering. Kommentar:			
4.	Om produkter inköps bör en formell test- och anskaffningsrutin följas. I kontraktet med leverantören bör de fastställda säkerhetskraven tas upp. Där säkerhetsfunktionerna i en föreslagen produkt inte tillfredsställer de specificerade kraven bör den tillkommande risken och tillhörande säkerhetsfunktioner övervägas på nytt innan produkten inköps. Om funktioner utöver de begärda levereras och orsakar en säkerhetsrisk bör de stängas av eller också bör den föreslagna kontrollstrukturen granskas för att avgöra om den utökade funktionalitet som är tillgänglig kan bli till nytta. Kommentar:			

Övrig information

Om det bedöms lämpligt, t.ex. av kostnadsskäl, kan ledningen välja att använda oberoende evaluerade och certifierade produkter. Mera information om evalueringskriteria för IT-säkerhetsprodukter finns i ISO/IEC 15408 eller andra förekommande evaluerings- eller certifieringsstandarder.

ISO/IEC TR 13335-3 ger vägledning i fråga om användning av riskhanteringsprocesser för att identifiera krav beträffande säkerhetsåtgärder.

12.2 Korrekt bearbetning i tillämpningar

Mål: Att förhindra fel, förlust, obehörig förändring eller missbruk av information i tillämpningssystem.

Lämpliga säkerhetsåtgärder bör byggas in i tillämpningssystem, inklusive användarutvecklade tillämpningar, för att säkerställa korrekt bearbetning. Dessa säkerhetsåtgärder bör innefatta validering av indata, intern bearbetning och utdata.

Ytterligare säkerhetsåtgärder kan krävas för system som bearbetar eller kan påverka känslig, värdefull eller kritisk information. Sådana säkerhetsåtgärder bör beslutas på grundval av säkerhetskrav och riskbedömning.

12.2.1 Validering av indata

	Nivå
Indata till tillämpningssystem bör valideras för att säkerställa att de är riktiga och relevanta. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan automatisk kontroll och validering av indata, ökar risken för fel och sårbarhet för attacker såsom buffertöverskridning (buffer overflow) och olovlig körning av kod (code injection).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Kontroller bör tillämpas avseende; inmatning av affärstransaktioner, fasta data (t.ex. namn och adress, kreditgränser, kundnummer) och parametertabeller (t.ex. försäljningspriser, valutakurser, skattesatser). Följande riktlinjer bör beaktas: a) dubbel inmatning eller andra indatakontroller, t.ex. gränsvärden eller begränsning av fält till givna värdeintervall för indata, för att upptäcka följande fel: 1) värden utanför förväntat intervall 2) ogiltiga tecken i datafält 3) saknade eller ofullständiga data			

Nivåstyrande frågor		JA	NEJ	VET EJ
	4) överskridande av övre eller lägre gränser för datavolym 5) oauktoriserade eller inkonsekventa kontrolldata; Kommentar:			
2.	b) regelbunden granskning av nyckelfält eller datafiler för att bekräfta deras validitet och riktighet; Kommentar:			
3.	c) granskning av pappersbundna indatadokument för att upptäcka eventuella obehöriga förändringar (alla förändringar av indatadokument bör godkännas); Kommentar:			
4.	d) rutiner för att reagera på valideringsfel; Kommentar:			
5.	e) rutiner för rimlighetstest av indata; Kommentar:			
6.	f) definition av ansvar för all personal som arbetar med indatabehandling; Kommentar:			
7.	g) skapa en logg över aktiviteterna i indataprocessen (se 10.10.1). Kommentar:			

Övrig information

Där det är tillämpligt kan automatisk granskning och validering av indata övervägas för att minska risken för fel och förhindra vanligt förekommanden attacker inklusive överskridande av tillåten data-/fältstorlek och infogande av kod.

12.2.2 Styrning av intern bearbetning

	Nivå
Valideringskontroller bör läggas in i systemen för att upptäcka eventuella förvanskningar av informationen som sker genom bearbetningsfel eller med avsikt. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Bristfällig kontroll av intern databearbetning kan leda till förvanskad data på grund av hårdvarufel, bearbetningsfel eller genom avsiktliga handlingar.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Utformning och införande av tillämpningssystem bör säkerställa att risken för bearbetningsfel som leder till att integriteten förloras minimeras. Särskilda områden att tänka på innefattar: a) användning av funktioner för att lägga till, ändra och radera, för att införa förändringar i data; Kommentar:			
2.	b) rutiner för att förhindra att program körs i fel ordning eller efter fel i föregående bearbetning (se också 10.1.1); Kommentar:			
3.	c) användning av lämpliga program för återställning efter fel för att säkerställa korrekt bearbetning av data; Kommentar:			
4.	d) skydd mot attacker som använder överskridande av tillåten data-/fältstorlek. Kommentar:			
5.	En lämplig checklista bör upprättas, aktiviteter dokumenteras och resultaten bör skyddas. Exempel på kontroller som kan läggas in innefattar följande: a) sessions- eller batch-kontroller för att stämma av filbalanser efter transaktionsuppdatering; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	b) saldokontroll för att kontrollera öppningssaldo mot föregående slutsaldo såsom: 1) kontroll från ett bearbetningstillfälle till nästa; 2) fil-uppdateringstotaler; 3) program-till-program-kontroller; Kommentar:			
7.	c) validering av systemgenererade indata (se 12.2.1); Kommentar:			
8.	d) kontroll av riktighet, autenticitet eller annan säkerhetsegenskap hos data eller programvara, ner- eller uppladdade, mellan centrala anslutna datorer ; Kommentar:			
9.	e) kontroller för att säkerställa att tillämpningsprogram körs vid rätt tidpunkt; Kommentar:			
10.	f) kontroller för att säkerställa att program körs i rätt ordning, avslutas vid eventuellt fel och att fortsatt bearbetning avbryts till dess att problemet lösts; Kommentar:			
11.	g) Skapa en logg över aktiviterna involverade i bearbetningen (se 10.10.1). Kommentar:			

Övrig information

Data som har matats in korrekt kan förstöras genom hårdvarufel, bearbetningsfel eller genom avsiktliga handlingar. De valideringskontroller som krävs beror på typ av tillämpning och betydelsen för verksamheten vid eventuell förstöring av data.

12.2.3 Meddelandeintegritet

	Nivå
Krav på att säkerställa autenticitet och skydda meddelandes riktighet i tillämpningar bör fastställas och lämpliga säkerhetsåtgärder fastställas och införas. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om meddelandets riktighet inte är säkerställd kan det vara förfalskat eller förändrat, vilket kan resultera i ekonomiska förluster och påverka beslutsfattandet.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	En bedömning av säkerhetsrisker bör göras för att bestämma hur betydelsefull meddelandets riktighet är och fastställa den lämpligaste skyddsmetoden att införa. Kommentar:			

Övrig information

Krypteringsteknik (se 12.3) kan användas som en lämplig metod att införa autenticering av meddelanden.

12.2.4 Validering av utdata

	Nivå
Utdata från ett tillämpningssystem bör valideras för att säkerställa att bearbetning av lagrad information är korrekt och lämplig med hänsyn till omständigheterna. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om inte utdata valideras kan den bli felaktig, vilket kan leda till ekonomiska förluster eller försämrat beslutsfattande.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

	Nivåstyrande frågor	JA	NEJ	VET EJ
1.	Utdatavalidering kan innefatta: a) rimlighetskontroller för att testa om utdata är rimliga; Kommentar:			
2.	b) avstämningar för att säkerställa att alla data bearbetats; Kommentar:			
3.	c) att lämna tillräcklig information så att en läsare eller ett efterföljande bearbetningssystem kan avgöra informationens riktighet, fullständighet, precision och klassificering;			
4.	d) rutiner för att reagera på valideringstest av utdata;			
5.	e) definition av ansvar för all personal som är involverad i utdataprocessen; Kommentar:			
6.	f) att skapa en aktivitetslogg i rutinen för utdatavalidering. Kommentar:			

Övrig information
Vanligtvis bygger system och tillämpningar på förutsättningen att efter erforderlig validering, verifiering och test kommer utdata alltid att vara

korrekta. Dock är denna förmodan inte alltid giltig. System som har testats kan fortfarande producera felaktiga utdata under vissa omständigheter.

12.3 Kryptering

Mål: Att skydda konfidentialiteten, autenticiteten eller riktigheten i information genom kryptering.

En policy bör utvecklas för användningen av kryptofgrafiska säkerhetsåtgärder. Nyckelhantering bör finnas för att stödja användningen av krypteringsteknik.

12.3.1 Krypteringspolicy

	Nivå
En policy för användning av kryptografiska säkerhetsåtgärder för informationsskydd bör utvecklas och införas. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan policy för kryptografiska säkerhetsåtgärder, finns det risk för att information går förlorad, konflikter med andra säkerhetssystem som behöver komma åt den krypterade informationen, eller att lösningen inte ger tillräckligt skydd.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Vid utveckling av en krypteringspolicy bör följande beaktas: a) ledningens inställning till att använda kryptering i organisationen inklusive de allmänna principerna för hur verksamhetens information bör skyddas (se också 5.1.1); Kommentar:			
2.	b) baserat på en riskbedömning bör den skyddsnivå som krävs fastställas med hänsyn tagen till typ, styrka och kvalitet hos den krypteringsalgoritm som krävs; Kommentar:			
3.	c) användning av kryptering för skydd av känslig information överförd av mobila eller flyttbara media, enheter eller över kommunikationsförbindelser; Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
4.	d) sättet för nyckelhantering inklusive metoder för att behandla skyddet av krypteringsnycklar och återvinning av krypterad information om nycklarna förloras, påverkas eller förstörs; Kommentar:			
5.	e) roller och ansvar, t.ex. vem som ansvarar för: 1) implementering av policyn; 2) nyckelhantering, inklusive nyckelgenerering (se också 12.3.2); Kommentar:			
6.	f) de standarder som bör tillämpas för ett verkningsfullt införande i hela organisationen (vilken lösning används för vilka verksamhetsprocesser); Kommentar:			
7.	g) effekten av säkerhetsåtgärder som förlitar sig på innehållsgranskning (t.ex. upptäckt av virus) av att använda krypterad information. Kommentar:			
8.	När organisationens krypteringspolicy införs bör hänsyn tas till de bestämmelser och nationella begränsningar som kan gälla för användning av kryptering på olika håll i världen och till frågor om att sända krypterad information över nationsgränser (se också 15.1.6). Kommentar:			
9.	Kryptering kan utnyttjas för att uppnå olika säkerhetsmål, t.ex.: a) konfidentialitet; användning av kryptering för att skydda känslig eller kritisk information, antingen lagrad eller under överföring; Kommentar:			
10.	b) riktighet/autenticitet; användning av digitala signaturer eller koder för meddelandeautenticering för att skydda autenticitet och riktighet hos lagrad eller överförd information som är känslig eller kritisk; Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
11.	c) oavvislighet; användning av krypteringsteknik för att erhålla bevis för inträffad alternativt inte inträffad händelse eller handling. Kommentar:			

Övrig information

Att fatta beslut om en krypteringslösning är lämplig bör ses som ett led i en mer omfattande process rörande riskbedömning och val av säkerhetsåtgärder. Denna bedömning kan sedan ligga till grund för att avgöra om en krypteringsåtgärd är lämplig, vilken typ av åtgärd som bör väljas samt för vilket ändamål och för vilka verksamhetsprocesser.

En krypteringspolicy är nödvändig för att maximera fördelarna och minimera riskerna med användning av krypteringstekniker och för att undvika olämplig eller felaktig användning. När digitala signaturer används bör relevant lagstiftning beaktas, särskilt lagstiftning som beskriver villkoren för att digital signatur blir juridiskt bindande (se15.1).

Specialistråd bör inhämtas för att fastställa lämplig skyddsnivå och välja lämpliga specifikationer som ger det skydd som krävs och som stödjer införande av ett säkert nyckelhanteringssystem (se också 12.3.2).

ISO/IEC JTC 1/SC 27 har utvecklat ett flertal standarder som behandlar kryptering. Mer information finns också i IEEE P1363 och i OECD Guidelines on Chryptography.

12.3.2 Nyckelhantering

	Nivå
Ett nyckelhanteringssystem bör finnas för att stödja organisationens användning av krypteringsteknik. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan nyckelhantering ökar risken för att krypteringslösningar inte fungerar (oskyddad eller otillgänglig information). Det finns också en risk för förfalskning av digital signatur genom att ersätta användarens publika nyckel.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Alla krypteringsnycklar bör skyddas mot förändring, förlust och förstöring. Hemliga och privata nycklar behöver också skydd mot obehörigt avslöjande. Fysiskt skydd bör användas för utrustning för framtagning, lagring och arkivering av nycklar. Kommentar:			
2.	Ett nyckelhanteringssystem bör baseras på en bestämd uppsättning standarder, rutiner och säkra metoder för att: a) framställa nycklar för olika krypteringssystem och skilda tillämpningar; Kommentar:			
3.	b) skapa och erhålla öppna-nyckelcertifikat; Kommentar:			
4.	c) distribuera nycklar till avsedda användare inklusive uppgift om hur nycklarna bör aktiveras när de tas emot; Kommentar:			
5.	d) lagra nycklar inklusive uppgift om hur behöriga användare kan få åtkomst till nycklar; Kommentar:			
6.	e) ändra eller uppdatera nycklar inklusive regler för när och hur nycklar bör ändras			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
7.	f) hantera nycklar vars säkerhet äventyrats Kommentar:			
8.	g) återkalla nycklar inklusive hur de bör dras in eller aktiveras när t.ex. nyckelns säkerhet äventyrats eller när en användare lämnar organisationen (då nyckeln också bör arkiveras) Kommentar:			
9.	h) som led i avbrottsplanen återvinna nycklar som förlorats eller äventyrats, t.ex. för att återvinna krypterad information; Kommentar:			
10.	i) arkivera nycklar t.ex. för arkiverad eller säkerhetskopierad information Kommentar:			
11.	j) förstöra nycklar. Kommentar:			
12.	För att minska sannolikheten för att de äventyras bör nycklar ha angivna aktiverings- och avaktiveringsdatum så att de kan användas endast under en begränsad tid. Längden på tidsperioden bör bero av omständigheter under vilka krypteringen används samt den förmodade risken. Kommentar:			
13.	Förutom säker hantering av hemliga och privata nycklar bör också autenticiteten hos öppna nycklar beaktas. Autenticeringsförfarandet kan ske med användning av öppen nyckelcertifikat. Det utfärdas normalt av en certifikatutfärdare som bör vara en erkänd organisation som infört lämpliga kontroller och rutiner för att uppfylla den grad av förtroende som krävs. Kommentar:			
14.	Innehållet i överenskommelser om tjänstenivå eller avtal med externa leverantörer av krypteringstjänster, t.ex. en certifikatutfärdare, bör omfatta bestämmelser om ansvar, tjänsternas tillförlitlighet och svarstider för att utföra tjänsten (se			

Nivåstyrande frågor		JA	NEJ	VET EJ
	6.2.3) Kommentar:			

Övrig information

Hanteringen av krypteringsnycklar är av avgörande betydelse för en effektiv användning av krypteringstekniker. ISO/IEC 11770 ger ytterligare information om nyckelhantering. De två typerna av krypteringsteknik är:

a) Symmetrisk nyckelteknik där två eller flera parter har samma nyckel som används både för att kryptera och dekryptera information. Denna nyckel måste vara hemlig eftersom var och en som har tillgång till den kan dekryptera all information som är krypterad med nyckeln eller lägga till obehörig information genom att använda nyckeln.

b) Asymmetrisk nyckelteknik där vardera parten har ett nyckelpar, en öppen nyckel (som kan delges envar) och en privat nyckel (som måste hållas hemlig). Tekniken kan användas för kryptering och för att ta fram digitala signaturer (se också ISO/IEC 9796 och ISO/IEC 14888)..

Ett hot är att någon förfalskar en digital signatur genom att ersätta en användares öppna nyckel med sin egen. Detta problem löses genom användning av ett öppen nyckelcertifikat.

Krypteringsteknik kan också användas för att skydda krypteringsnycklar. Rutiner kan behöva övervägas för att hantera legala krav på åtkomst till krypteringsnycklar, t.ex. därför att krypterad text kan behöva göras tillgänglig i klartext vid en rättslig prövning.

12.4 Skydd av systemfiler

Mål: Att säkerställa säkerheten för systemfiler.

Åtkomst till systemfiler och källkod bör styras och IT-projekt och stödaktiviteter utföras på ett säkert sätt. Försiktighet bör iakttas för att undvika exponering av känsliga data i testmiljöer.

12.4.1 Styrning av programvara i drift

	Nivå
Det bör finnas rutiner för att styra installation av program i driftsystem. *Kritisk säkerhetsåtgärd: JA* *Risk: Dålig kontroll över installation av programvara kan leda till säkerhetsincidenter. Problem som uppstår på grund av att fel version av programvaran installerats i system eller systemkomponenter kan leda till utebliven support från leverantören.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	För att minska risken för skadlig påverkan på system i drift bör följande riktlinjer övervägas för att styra ändringar: a) Uppdatering av driftsystem, tillämpningar och programvarubibliotek bör endast få utföras av utbildade administratörer efter vederbörligt godkännande från ledningen (se 12.4.3). Kommentar:			
2.	b) Driftsystem bör endast omfatta godkänd exekverbar kod och inte utvecklingskod eller kompilatorer. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
3.	c) Tillämpnings- och operativsystemprogram bör endast införas efter noggrann och framgångsrik test. Testerna bör innefatta test av användbarhet, säkerhet, effekter på andra system och användarvänlighet och bör göras på separata system (se också 10.1.4). Det bör säkerställas att alla motsvarande källprogrambibliotek har uppdaterats. Kommentar:			
4.	d) Ett konfigurationskontrollsystem bör användas för att ha kontroll på all installerad programvara liksom även systemdokumentation. Kommentar:			
5.	e) En strategi för att återgå till tidigare versioner bör finnas innan ändringar införs. Kommentar:			
6.	f) en revisionslogg bör föras över alla uppdateringar av driftens programbibliotek; Kommentar:			
7.	g) Tidigare versioner av tillämpningsprogramvara bör bevaras som ett led i kontinuitetsplaneringen. Kommentar:			
8.	h) Äldre programvaruversioner bör arkiveras tillsammans med all erforderlig information och parametrar, rutiner, konfigurationsdetaljer och stödprogramvara så länge som data bevaras i arkiv.v Kommentar:			
9.	Programvaror, erhållna från leverantör, som används i system i drift bör vidmakthållas på en nivå som stöds av leverantören. Med tiden kommer programvaruleverantörer sluta att stödja äldre programvaruversioner. Organisationen bör tänka på risken av att vara beroende av programvara som saknar support. Kommentar:			
10.	Beslut att uppgradera till en ny programversion bör beakta verksamhetskraven på förändring och versionens säkerhet d.v.s. införande av nya säkerhetsfunktioner eller antal och omfattning av säkerhetsproblem som påverkar denna version. Mindre			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	programvaruändringar bör införas när de kan bidra till att minska eller eliminera svagheter ifråga om säkerhet (se också 12.6.1) Kommentar:			
11.	Fysisk eller logisk åtkomst bör endast tilldelas leverantörer för att lämna nödvändigt stöd och endast med ansvarig chefs tillstånd. Leverantörens aktiviteter bör övervakas. Kommentar:			
12.	Vissa programvaror är beroende av externt tillhandahållna programvaror och moduler. De bör följas upp och kontrolleras för att undvika obehöriga förändringar som kan leda till säkerhetsproblem. Kommentar:			

Övrig information

Operativsystem bör endast uppgraderas när det finns behov av det, t.ex. om den aktuella operativsystemversionen inte längre uppfyller verksamhetens krav. Uppdatering bör inte göras enbart för att en ny operativsystemversion är tillgänglig. Nya operativsystemversioner kan vara av mindre säkra, mindre stabila och svårare att förstå än de aktuella systemen.

12.4.2 Skydd av testdata

	Nivå
Testdata bör väljas med noggrannhet, skyddas och styras. *Kritisk säkerhetsåtgärd: JA* *Risk: Kopiering av känslig information till testmiljö för test och felsökning kan leda till obehörig åtkomst av informationen.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Användning av databaser i drift som innehåller personinformation eller annan känslig information för teständamål bör undvikas. Om personrelaterad eller i andra avseenden känslig information används för teständamål bör alla känsliga detaljer och övrigt känsligt innehåll avlägsnas eller modifieras så att det inte längre kan igenkännas innan de används. Följande riktlinjer bör tillämpas för att skydda driftdata när de används för teständamål: a) rutiner för styrning av åtkomst som tillämpas för produktionssystem bör också gälla vid test av sådana system Kommentar:			
2.	b) behörighet bör ges särskilt varje gång produktionsdata kopieras till ett testsystem Kommentar:			
3.	c) produktionsdata bör raderas från testsystem genast efter avslutad test Kommentar:			
4.	d) kopiering och användning av testdata bör loggas för att erhålla spårbarhet. Kommentar:			

Övrig information

System- och acceptanstest kräver vanligtvis avsevärda volymer testdata som liknar driftdata i så stor utsträckning som möjligt.

12.4.3 Styrning av åtkomst till källprogramkod

	Nivå
Åtkomst till källprogramkod bör begränsas. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Obehörig ändring av källkoden kan resultera i systemfel och/eller illvillig skada.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Åtkomst till källprogramkod och vad därtill hör (såsom utformning, specifikationer, verifieringsplaner och valideringsplaner) bör styras strikt i syfte att förhindra att obehöriga funktioner införs och för att undvika oavsiktliga förändringar. När det gäller källprogramkod kan detta uppnås genom styrd, central lagring av sådan kod, företrädesvis i källkodbibliotek. Följande riktlinjer bör då övervägas (se också 11) för styrning av åtkomst till sådana bibliotek i syfte att minska möjligheten till skadlig påverkan på datorprogram: a) om möjligt bör källprogrambibliotek inte ingå i driftsystem Kommentar:			
2.	b) källkod och källkodsbibliotek för program bör skötas i enlighet med etablerade rutiner Kommentar:			
3.	c) supportpersonal bör inte ha obegränsad åtkomst till källkodsbibliotek Kommentar:			
4.	d) uppdatering av källkodsbiblioteket, och vad därtill hör och utlämning av källprogram till programmerare bör endast ske efter att vederbörligt medgivande har erhållits Kommentar:			
5.	e) programlistor bör förvaras i en säker miljö (se 10.7.4) Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	f) en revisionslogg bör föras över all åtkomst till källkodsbibliotek Kommentar:			
7.	g) för underhåll och kopiering av källkodsbibliotek bör en strikt ändringshantering gälla (se 12.5.1). Kommentar:			

Övrig information

Källkod är kod som skrivs av programmerare, som kompileras (och länkas) för att skapa exekverbara program. Vissa programspråk skiljer inte formellt mellan källkod och exekverbar kod eftersom de senare skapas samtidigt som de förra aktiveras.

Standarderna ISO 10007 och ISO/IEC 12207 ger mer information om konfigurationsstyrning och programvarans livscykelprocess.

12.5 Säkerhet i utvecklings- och underhållsprocesser

Mål: Att bibehålla säkerheten i tillämpningssystemens programvara och information.

Projekt- och underhållsmiljöer bör styras noggrant.

Chefer ansvariga för tillämpningssystem bör också ha ansvar för säkerheten i projekt- eller underhållsmiljön. De bör säkerställa att alla föreslagna systemändringar granskas för att kontrollera att de inte äventyrar säkerheten vare sig i systemet eller i driftmiljön.

12.5.1 Rutiner för ändringshantering

	Nivå
Införandet av förändringar bör styras genom användning av en formell rutin för ändringshantering. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan rutiner för ändringshantering ökar risken för driftsstörningar under både normala och oförutsedda omständigheter. Riskens omfattning beror på tillgänglighetskraven på systemets. Otillgänglighet till andra kritiska system eller tjänster kan också få allvarliga konsekvenser. Olämplig ändringshantering kan också leda till att viss säkerhetsövervakning ingaktiveras vilket innebär risk för intrång och angrepp.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Formella rutiner för styrning av ändringar bör dokumenteras och införas i syfte att minimera skadlig påverkan på informationssystem. Introduktionen av nya system och större ändringar i existerande system bör ske enligt en formell rutin för dokumentation, specifikation, test, kvalitetskontroll och ett styrt införande. Kommentar:			
2.	Denna process bör omfatta riskbedömning, analys av påverkan av ändringar och specifikation av behovet av säkerhetsåtgärder för att styra säkerheten. Processen bör även säkerställa att säkerhets- och kontrollrutiner inte äventyras, att programmerarna endast har tillgång till de delar av systemet som de behöver nå för sitt arbete			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	och att formellt beslut och godkännande erhållits för alla förändringar. Kommentar:			
3.	Där det är praktiskt bör ändringsrutiner för tillämpningar och drift integreras (se också 10.1.2). Ändringsrutinerna bör innefatta att: a) registrera överenskomna behörighetsnivåer; Kommentar:			
4.	b) säkerställa att ändringar överlämnas av behöriga användare; Kommentar:			
5.	c) granska säkerhetsåtgärder och rutiner för systemintegritet för att säkerställa att de inte äventyras av förändringarna Kommentar:			
6.	d) identifiera all programvara, information, databasenheter och datorutrustning som kräver förändring Kommentar:			
7.	e) inhämta formellt godkännande för detaljerade förslag innan arbetet påbörjas Kommentar:			
8.	f) säkerställa att behöriga användare godtar förändringarna innan de införs Kommentar:			
9.	g) säkerställa att systemdokumentationen uppdateras efter varje genomförd förändring och att inaktuell dokumentation arkiveras eller förstörs Kommentar:			
10.	h) upprätthålla en versionshantering för alla programuppdateringar Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
11.	i) upprätthålla spårbarhet över alla ändringsbegäranden Kommentar:			
12.	j) säkerställa att driftdokumentation (se 10.1.1) och användarrutiner ändras vid behov så att de fortsätter att vara tillämpliga Kommentar:			
13.	k) säkerställa att införandet av förändringar sker vid rätt tidpunkt och inte stör de verksamhetsprocesser som berörs. Kommentar:			

Övrig information
Programändringar kan påverka driftmiljön.

God praxis innefattar att ny programvara testas i en miljö skild från både produktions- och utvecklingsmiljöerna (se också 10.1.4). Det medför bättre kontroll över ny programvara och möjliggör bättre skydd av produktionsdata som används för teständamål. Detta gäller också mindre ändringar, ”servicepack” och annan uppdatering. Automatisk uppdatering bör inte tillåtas av kritiska system eftersom vissa uppdateringar kan medföra att kritiska tillämpningar fallerar (se 12.6).

12.5.2 Teknisk granskning av tillämpningar efter ändringar i operativsystem

	Nivå
När operativsystem ändras bör verksamhetskritiska tillämpningar granskas och testas för att säkerställa att ändringen inte har negativ påverkan på organisationens drift eller säkerhet. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om korrekt funktionalitet av verksamhetskritiska tillämpningar inte säkerställs efter ändringar i relaterade komponenter eller system, kan det få negativ påverkan på organisationens drift eller säkerhet.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Processen bör omfatta att: a) granska rutiner för kontroll och systemintegritet i tillämpningarna för att säkerställa att de inte har komprometterats av förändringarna i driftsystemet Kommentar:			
2.	b) säkerställa att den årliga underhållsplanen och -budgeten täcker granskningar och systemtest som krävs vid förändringar i produktionssystem Kommentar:			
3.	c) säkerställa att meddelanden om produktionssystemändringar lämnas i tid för att möjliggöra att erforderliga tester och granskningar hinner göras innan ändringen införs Kommentar:			
4.	d) säkerställande av att erforderliga förändringar görs i organisationens kontinuitetsplaner (se avsnitt 14). Kommentar:			
5.	En särskild grupp eller person bör tilldelas ansvar för att övervaka sårbarheter och om leverantörer släpper mindre ändringar och fixar (se 12.6). Kommentar:			

12.5.3 Restriktioner mot ändringar i programvarupaket

	Nivå
Modifieringar av programvarupaket bör minimeras, begränsas till nödvändiga ändringar och alla ändringar bör strikt styras. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Ändringar kan leda till att inbyggda kontroller och integritetsprocesser äventyras. Om ändringarna är omfattande kan hanteringen bli kostsam, särskilt om det gäller uppgradering av programvara.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Så långt som möjligt, och praktiskt genomförbart, bör upphandlade programvarupaket användas utan förändring. Då det är nödvändigt att ändra i programvarupaket bör följande punkter beaktas: a) risken för att inbyggda säkerhetsfunktioner och andra rutiner för systemintegritet komprometteras Kommentar:			
2.	b) om leverantörens medgivande bör inhämtas Kommentar:			
3.	c) möjligheten att få den nödvändiga förändringen från leverantören som standarduppdatering av programvarupaketet Kommentar:			
4.	d) följderna om organisationen blir ansvarig för framtida underhåll av programvaran som följd av förändringen. Kommentar:			
5.	Om ändringar är nödvändiga bör originalversionen av programvarupaketet behållas och ändringarna göras i en tydligt identifierad kopia. Ett styrt förfarande för uppdatering av programvara bör införas för att säkerställa att de senaste, godkända småändringarna och uppdateringarna av tillämpningarna är installerade i all godkänd programvara (se 12.6). Alla ändringar bör vara fullständigt testade och dokumenterade så att de om nödvändigt kan införas i framtida versioner av			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	programvarupaketet. Om det krävs bör förändringarna testas och valideras av en oberoende utvärderingsorganisation. Kommentar:			

12.5.4 Informationsläckor

	Nivå
Möjlighet till informationsläckor bör förhindras. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Otillräcklig skydd mot Dolda Kanaler kan leda till informationsläckor.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Följande bör övervägas för att begränsa risken för informationsläckor t.ex. genom användning av dolda kanaler: a) genomsökning av utgående media och kommunikation efter dold information Kommentar:			
2.	b) maskering och anpassning av system- och kommunikationsbeteende för att minska sannolikheten att en utomstående kan härleda information från sådant beteende Kommentar:			
3.	c) användning av system och programvara som anses ha hög integritet, d.v.s. användning av utvärderade produkter (se ISO/IEC 15408) Kommentar:			
4.	d) regelbunden uppföljning av personal- och systemaktiviteter där det är tillåtet enligt gällande författningar Kommentar:			
5.	e) övervakning av resursanvändning i datasystem. Kommentar:			

Övrig information

Dolda kanaler är vägar som inte är avsedda att leda informationsflöden men som icke desto mindre kan existera i ett system eller nätverk. Att t.ex. manipulera bits i paket för kommunikationsprotokoll kan användas som en dold metod för signalering. Genom sin karaktäristik är det svårt, även om inte

är omöjligt att förhindra existensen av alla tänkbara dolda kanaler. Exploateringen av sådana kanaler sker emellertid ofta genom trojansk kod (se också 10.4.1). Att vidta åtgärder för skydd mot trojansk kod minskar därför risken för att dolda kanaler utnyttjas.

Förhindrande av obehörig nätverksåtkomst (11.4) liksom policyer och rutiner för att motverka personalens missbruk av informationstjänster (15.1.5), hjälper till att skydda mot dolda kanaler.

12.5.5 Utlagd programvaruutveckling

	Nivå
Utlagd programvaruutveckling bör kontrolleras och övervakas av organisationen. *Kritisk säkerhetsåtgärd: JA* *Risk: Dålig hantering av utlagd programvaruutveckling kan leda till:* *– Stabilitetsproblem, om inte källkoden finns tillgänglig för att underhålla programmet* *– Att utvecklaren lägger in en så kallad "backdoor" för att komma åt eller manipulera information.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Där programutvecklingen är utlagd till utomstående bör följande punkter beaktas: a) licensieringsarrangemang, äganderätt till koden och upphovsrätt (se 15.1.2) Kommentar:			
2.	b) licensieringsarrangemang, äganderätt till koden och upphovsrätt (se 15.1.2) Kommentar:			
3.	c) depositionsarrangemang i händelse av att den tredje parten inte kan fullgöra sin uppgift Kommentar:			
4.	d) åtkomsträtt för revision med avseende på kvalitet och noggrannhet av utfört arbete Kommentar:			
5.	e) avtalskrav på kvalitet och säkerhetsfunktioner hos kod Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	f) test före installation för att upptäcka skadlig och trojansk kod. Kommentar:			

12.6 Hantering av tekniska sårbarheter

Mål: Att minska riskerna med utnyttjande av publicerade tekniska sårbarheter.

Skyddet för teknisk sårbarhet bör implementeras på ett verkningsfullt, systematiskt och repeterbart sätt med åtgärder vidtagna för att bekräfta dess verkan. Dessa överväganden bör omfatta operativsystem och alla andra tillämpningar i drift.

12.6.1 Skydd för tekniska sårbarheter

	Nivå
Information vid rätt tidpunkt om den tekniska sårbarheten hos informationssystem i drift bör inhämtas, organisationens utsatthet för sådan sårbarhet bedömas, och lämpliga åtgärder vidtagas för att hantera den tillhörande risken. *Kritisk säkerhetsåtgärd: JA* *Risk: Dålig efterlevnad av säkerhetspolicy, dålig patchhantering och bristfälliga sårbarhetsbedömningar ökar sårbarheter och därmed sannolikheten för att risker ska realiseras både i systemet och i verksamheten i stort. Otillräckliga tester av uppdateringar kan också leda till problem.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	En aktuell och fullständig förteckning över tillgångar (se 7.1) är en förutsättning för effektiv hantering av teknisk sårbarhet. Specifik information som behövs för att stödja hanteringen av teknisk sårbarhet omfattar leverantören av programvaran, versionsnummer, aktuell omfattning av användningen (t.ex. vilken programvara är installerad på vilket system) och den person eller de personer inom organisationen som är ansvariga för programvaran. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	Rätt åtgärd vid rätt tidpunkt bör vidtas för att hantera de tekniska sårbarheter som har identifierats. Följande vägledning bör följas för att införa en effektiv hantering av teknisk sårbarhet: a) Organisationen bör definiera och bestämma roller och ansvar för hantering av teknisk sårbarhet inklusive övervakning av sårbarheten, riskbedömning av sårbarheten, programändringar, spårande av tillgångar och det samordningsansvar som kan krävas. Kommentar:			
7.	b) När det gäller programvara och annan teknologi (baserad på inventarielistan, se 7.1.1) bör de informationsresurser identifieras som kommer att användas för att identifiera relevant teknisk sårbarhet och bibehålla kunskap om dem. Dessa informationsresurser bör uppdateras vid ändring i inventariet eller när andra nya och användbara resurser hittas. Kommentar:			
8.	c) En tidsgräns bör definieras för reaktion på tänkbara relevanta tekniska svagheter. Kommentar:			
9.	d) Så snart en potentiell teknisk svaghet har fastställts bör organisationen fastställa tillhörande risker och de åtgärder som behöver vidtas. Åtgärderna kan omfatta programändring av sårbara system och/eller att sätta in andra säkerhetsåtgärder. Kommentar:			
10.	e) Beroende på hur brådskande det är att vidta åtgärder mot en teknisk sårbarhet bör åtgärden utföras i enlighet med säkerhetsåtgärderna som är relaterade till ändringshantering (se 12.5.1) eller genom att följa rutinerna för respons på informationssäkerhetsincidenter (se 13.2). Kommentar:			
11.	f) Om en programändring finns tillgänglig, bör den risk som hänger samman med att installera ändringen bedömas (riskerna som sårbarheten innebär bör jämföras med risken med att installera programändringen). Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
12.	g) Programändringar bör testas och utvärderas innan de installeras för att säkerställa att de är effektiva och inte resulterar i sidoeffekter som inte kan accepteras; om ingen programändring är tillgänglig bör andra säkerhetsåtgärder övervägas som t.ex.: 1) avstängning av tjänster eller andra möjligheter relaterade till sårbarheten 2) anpassning eller tillägg av åtkomstkontroll, t.ex. brandvägg, vid nätverksgränserna (se 11.4.5) 3) ökad övervakning för att upptäcka eller förhindra verkliga angrepp 4) öka medvetenheten om sårbarheten. Kommentar:			
13.	h) En spårbarhetslogg över alla vidtagna rutiner bör föras. Kommentar:			
14.	i) Processen för hantering av teknisk sårbarhet bör regelbundet granskas och värderas i syfte att säkerställa dess verkan och effektivitet. Kommentar:			
15.	j) Högrisksystem bör behandlas först. Kommentar:			

Övrig information

Att organisationens hantering av tekniska sårbarheter fungerar riktigt är kritiskt för många organisationer och det bör därför regelbundet följas upp. En korrekt inventarieförteckning är nödvändig för att säkerställa att potentiellt relevanta sårbarheter är identifierade.

Hanteringen av teknisk sårbarhet kan ses som en delmängd av ändringshanteringen och kan som sådan dra fördel av hanteringen och rutinen för ändringshantering (se 10.1.2 och 12.5.1).

Leverantörer är ofta under stark press att släppa programändringar så snart som möjligt. En programändring behandlar därför kanske inte problemet på ett adekvat sätt och kan ha negativa sidoeffekter. I vissa fall kan det vara svårt att avinstallera en ändring när den en gång har installerats.

Om en adekvat test av ändringen inte är möjlig, t.ex. av kostnadsskäl eller resursbrist kan man överväga att uppskjuta programändringen och bedöma de tillhörande riskerna på grundval av erfarenheter rapporterade av andra användare.

13. Hantering av informationssäkerhets-incidenter

13.1 Rapportering av informationssäkerhetshändelser och svagheter

Mål: Att säkerställa att informationssäkerhetshändelser och svagheter hos informationssystem kommuniceras på ett sådant sätt att korrigerande åtgärder kan vidtas i rätt tid.

Det bör finnas formella rutiner för händelserapportering och eskalering. Alla anställda, uppdragstagare och tredjepartsanvändare bör göras medvetna om rutinerna för rapportering av de olika typerna av händelser och svagheter som kan påverka säkerheten hos organisationens tillgångar. Det bör krävas att de rapporterar eventuella informationssäkerhetshändelser och -svagheter så snart som möjligt till den utsedda kontaktpunkten.13.1.1 Rapportering av informationssäkerhetshändelser

13.1.1 Rapportering av informationssäkerhetshändelser

	Nivå
Informationssäkerhetshändelser bör inrapporteras via lämpliga rapporteringsvägar så snart som möjligt. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan vedertagna kanaler för användarna att rapportera in säkerhetshändelser finns det risk för att informationen inte når rätt person. Det innebär att det blir svårare att begränsa följdverkningarna och att utreda händelsen. Dessutom kan samma händelse upprepas igen.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	En formell rapporteringsrutin för säkerhetshändelser bör upprättas tillsammans med en rutin för incidentrespons och eskalering, där			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	de åtgärder som behöver vidtas vid mottagandet när en rapport om en informationssäkerhetshändelse tas emot. En kontaktpunkt bör utses för inrapportering av informationssäkerhetshändelser. Det bör säkerställas att denna kontaktpunkt är känd i hela organisationen, är ständigt tillgänglig och kan ge adekvat respons inom rimlig tid. Kommentar:			
2.	Alla anställda, uppdragstagare och tredjepartsanvändare bör göras medvetna om sitt ansvar för att rapportera alla informationssäkerhetshändelser så snart som möjligt. De bör också vara medvetna om rutinen för rapportering av informationssäkerhetshändelser och kontaktpunkten. Rapporteringsrutinen bör innefatta: a) lämpliga återkopplingsrutiner för att säkerställa att de som rapporterar informationssäkerhetshändelser informeras om resultatet efter att ärendet har behandlats och avslutats Kommentar:			
3.	b) blankett för rapportering av informationssäkerhetshändelser som hjälpmedel vid rapportering, och som hjälp till den rapporterande personen för att komma ihåg alla nödvändiga åtgärder vid en eventuell säkerhetshändelse Kommentar:			
4.	c) det korrekta sättet att agera vid en eventuell informationssäkerhetshändelse, d.v.s. 1) att omedelbart notera alla viktiga detaljer (t.ex. typ av bristande efterlevnad eller avvikelse, funktionsfel, meddelanden på skärmen, konstigt uppträdande) 2) att inte vidta någon egen åtgärd, utan omedelbart rapportera till kontaktpunkten Kommentar:			
5.	d) hänvisning till ett fastställt formellt disciplinärt förfarande för hantering av anställda, uppdragstagare eller tredjepartsanvändare som bryter mot säkerheten. Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
6.	I högriskmiljöer bör finnas ett överfallslarm[4] så att en person i tvångssituation kan meddela sådana problem. Rutinen för att reagera på överfallslarm bör spegla den högrisksituation som ett sådant alarm visar. Kommentar:			

Övrig information
Exempel på informationssäkerhetshändelser och -incidenter är:

a) bortfall av tjänst, utrustning eller andra resurser

b) systemfel eller överbelastning

c) mänskliga misstag

d) försummelse i efterlevnad av policyer eller riktlinjer

e) överträdelser av fysiska säkerhetsarrangemang

f) okontrollerade systemförändringar

g) felfunktion hos program- eller hårdvara

h) åtkomstförseelser.

Med rimlig hänsyn till konfidentialitetssaspekter kan informationssäkerhetsicidenter användas i utbildning av användare (se 8.2.2) som exempel på vad som kan hända, hur sådana incidenter bör hanteras och hur man kan undvika dem i framtiden. För att kunna hantera informationssäkerhetshändelser och incidenter på rätt sätt kan det bli nödvändigt att insamla bevis så snart som möjligt efter händelsen (se 13.2.3).

Felfunktioner och annat onormalt systembeteende kan indikera en attack mot säkerheten eller verkligt brott mot säkerheten och bör därför alltid rapporteras som informationssäkerhetshändelse.

Mer information om rapportering av informationssäkerhetshändelser och hantering av informationssäkerhetsincidenter finns i ISO/IEC TR 18044.

[4] Ett överfallslarm är en metod för att dolt indikera att en handling vidtas under tvång.

13.1.2 Rapportering av säkerhetsbrister

	Nivå
Det bör krävas av alla anställda, uppdragstagare och tredjepartsanvändare av informationssystem och -tjänster att de noterar och rapporterar alla observerade eller misstänkta säkerhetsbrister i system eller tjänster. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan vedertagna kanaler för användare att rapportera in händelser, kan händelserna få mer omfattande konsekvenser (verksamhetsstörningar etc.) än nödvändigt. Dessutom kan utrednings- och uppföljningsarbete försvåras.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Alla anställda, uppdragstagare och tredjepartsanvändare bör rapportera dessa saker antingen till ledningen eller direkt till sin tjänsteleverantör så snart som möjligt för att förhindra informationssäkerhetsincidenter. Rapporteringsmetoden bör vara så lätt, åtkomlig och tillgänglig som möjligt. De bör informeras om att de inte under några omständigheter bör försöka bevisa en misstänkt brist. Kommentar:			

Övrig information

Anställda, uppdragstagare och tredjepartsanvändare bör rådas att inte försöka bevisa misstänkta säkerhetsbrister. Att testa brister kan tolkas som ett tänkbart missbruk av systemet och skulle också kunna orsaka skada på informationssystemet eller -tjänsten och resultera i juridiskt ansvar för den person som utför testen.

13.2 Hantering av informationssäkerhetsincidenter och förbättringar

Mål: Att säkerställa att ett konsekvent och effektivt angreppssätt tillämpas på hanteringen av informationssäkerhetsincidenter.

Ansvarsfördelning och rutiner bör finnas för att effektivt hantera informationssäkerhetshändelser och brister så snart de har rapporterats. En process för ständig förbättring bör tillämpas när det gäller att reagera på, följa upp, värdera och överordnat hantera informationssäkerhetsincidenter.

Där bevis krävs bör de insamlas i överensstämmelse med legala krav.

13.2.1 Ansvar och rutiner

	Nivå
Ledningsansvar och rutiner bör fastställas för att säkerställa en snabb, effektiv och ordnad respons vid informationssäkerhetsincidenter. *Kritisk säkerhetsåtgärd: JA* *Risk: Ineffektiva metoder för incidenthantering och otydlig ansvarsfördelning kan leda till att incidenter orsakar större skada (t.ex. verksamhetsstörningar) och medför högre kostnader än nödvändigt.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Förutom rapportering av informationssäkerhetshändelser och -brister (se också 13.1), bör uppföljning av system, larm och sårbarheter (10.10.2) användas för att upptäcka informationssäkerhetsincidenter. Följande riktlinjer för rutiner för hantering av informationssäkerhetsincidenter bör övervägas: a) rutiner bör upprättas för att hantera olika typer av informationssäkerhetsincidenter innefattande: 1) fel i informationssystem och bortfall av tjänst 2) skadlig kod (se 10.4.1) 3) tillgänglighetsattacker 4) fel som resultat av ofullständiga eller felaktiga verksamhetsdata 5) överträdelser mot konfidentialitet och riktighet 6) felaktig användning av informationssystem Kommentar:			
2.	b) i tillägg till normala katastrofplaner (se 14.1.3) bör rutinerna också täcka (se också 13.2.2): 1) analys och identifiering av orsaken till incidenten 2) begränsning/avgränsning 3) planering och genomförande av korrigerande åtgärd för att förhindra upprepande, om det är nödvändigt 4) kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten 5) rapportering av åtgärd till vederbörande myndighet Kommentar:			
3.	c) spårbarhetsloggar och liknande bevis bör samlas in (se 13.2.3) och säkras i lämplig omfattning för: 1) intern problemanalys 2) användning som rättsligt bevis vid ett tänkbart avtalsbrott eller författningskrav eller när det gäller civil- eller brottmål t.ex. enligt lagstiftning om datormissbruk eller persondataskydd 3) förhandling om ersättning från programvaru- eller tjänsteleverantör			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
4.	d) åtgärder för återhämtning efter säkerhetsbrott och för att korrigera systemfel bör styras noggrant och formellt; rutinerna bör säkerställa att: 1) endast tydligt identifierad och behörig personal tillåts åtkomst till aktiva system och data (se också 6.2 beträffande extern åtkomst) 2) alla vidtagna nödåtgärder dokumenteras i detalj 3) nödåtgärder rapporteras till ledningen och granskas på ett systematiskt sätt 4) systemintegriteten hos verksamhetssystem och säkerhetsåtgärder bekräftas med minimal tidsfördröjning. Kommentar:			
5.	Målen för hantering av informationssäkerhetsincidenter bör bestämmas tillsammans med ledningen och det bör säkerställas att de som är ansvariga för hantering av informationssäkerhetsincidenter förstår organisationens prioriteter för hantering av sådana incidenter. Kommentarer:			

Övrig information

Informationssäkerhetsincidenter kan överskrida organisationens och nationella gränser. För att reagera på sådana incidenter finns det ett ökande behov av att koordinera reaktioner och i tillämplig omfattning ge information om dessa incidenter till externa organisationer.

13.2.2 Att lära av informationssäkerhetsincidenter

	Nivå
Det bör finnas metoder för att möjliggöra kvantifiering och övervakning av typer, volymer och kostnader för informationssäkerhetsincidenter. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Ineffektiva rutiner för incidenthantering, även innefattande orsak/verkan- analyser, kan leda till att incidenter upprepas, vilket kan medföra höga kostnader.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Den information som erhålls genom utvärdering av informationssäkerhetsincidenter bör användas för att identifiera återkommande incidenter eller incidenter av stor betydelse. Kommentar:			

Övrig information
Utvärderingen av informationssäkerhetsincidenter kan peka på ett behov av förstärkta eller utökade säkerhetsåtgärder för att begränsa frekvens, skada och kostnad för framtida incidenter eller på att hänsyn tas till detta vid granskning av säkerhetspolicyn (se 5.1.2)

13.2.3 Insamling av bevis

	Nivå
Då en uppföljande åtgärd mot en person eller organisation efter en informationssäkerhetsincident innefattar en juridisk åtgärd (civil- eller brottmål) bör bevis insamlas, bevaras och presenteras i överensstämmelse med bevisregler i den eller de relevanta jurisdiktionerna. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan noggranna juridiska rutiner och verktyg för att samla in bevis, kan en uppföljande åtgärd ifrågasättas (internt eller i speciella fall av en domstol).*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Interna rutiner bör utarbetas och följas när bevis insamlas och läggs fram i syfte att vidta disciplinär åtgärd som handläggs inom organisationen. Kommentar:			
2.	Generellt täcker bevisreglerna: a) om bevisen är godtagbara: om bevisen kan användas i domstol eller ej Kommentar:			
3.	b) hur tungt bevisen väger: bevisens kvalitet och fullständighet. Kommentar:			
4.	För att uppnå godtagbarhet för bevis bör organisationen säkerställa att deras informationssystem överensstämmer med eventuell publicerad standard eller praxis för framtagning av godtagbara bevis. Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	Vikten av lämnade bevis bör överensstämma med eventuellt tillämpliga krav. För att uppnå vägande bevis bör säkerhetsåtgärdernas kvalitet och fullständighet användas för att korrekt och konsekvent skydda bevisen (d.v.s. processkontrollbevis), och under hela den period som de avsedda bevisen lagras och behandlas vilket bör visas genom en tydlig spårbarhet. Generellt kan en tydlig spårbarhet åstadkommas på följande sätt: a) För pappersdokument; originalet förvaras säkert med en redogörelse för vilken person som fann dokumentet, var dokumentet hittades, när det hittades och vem som bevittnade upptäckten. En eventuell utredning bör säkerställa att originalen inte är manipulerade.			
6.	b) För information på datamedia; spegelbilder eller kopior (beroende på tillämpliga krav) av alla flyttbara media, all information på hårddisk eller i minne bör tas om hand för att säkerställa tillgänglighet. Den logg som omfattar alla åtgärder under kopieringsprocessen bör bevaras och förfarandet bevittnas. Mediaoriginalet och loggen (och om det inte är möjligt, åtminstone en spegling eller kopia) bör förvaras säkert och orört. Kommentar:			
7.	Forensiskt arbete bör endast utföras på kopior av bevismaterialet. Integriteten hos allt bevismaterial bör skyddas. Kopiering av bevismaterial bör övervakas av tillförlitlig personal och information om när och var kopieringen utfördes, vem som utförde kopieringen och vilka redskap och program som utnyttjades bör loggas. Kommentar:			

Övrig information

När en informationssäkerhetshändelse först upptäcks är det kanske inte tydligt om huruvida händelsen kommer att hamna i domstol. Därför finns det en fara att nödvändigt bevismaterial förstörs avsiktligt eller oavsiktligt innan det är uppenbart hur allvarlig incidenten är. Det är tillrådligt att engagera en advokat eller polisen tidigt i en eventuell legal åtgärd och få råd om vilka bevis som krävs.

Bevis kan överskrida organisationens och/eller jurisdiktionens gränser. I sådana fall bör det säkerställas att organisationen har rätt att insamla den efterfrågade informationen som bevis. De olika jurisdiktionernas krav bör också beaktas för att maximera chanserna till acceptans i de relevanta jurisdiktionerna.

14. Kontinuitetsplanering för verksamheten

14.1 Informationssäkerhetsaspekter på kontinuitetsplanering för verksamheten

Mål: Att motverka avbrott i organisationens verksamhet och att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystem eller katastrofer och att säkra återstart inom rimlig tid.

En ledningsprocess för kontinuitetsplanering bör införas för att minimera följderna för organisationen och återhämtning efter förlust av informationstillgångar (som kan vara ett resultat av t.ex. naturkatastrofer, olyckshändelser, utrustningsfel eller avsiktliga åtgärder) till en godtagbar nivå genom en kombination av förebyggande och återställande skydd. Denna process bör identifiera kritiska verksamhetsprocesser, samt integrera krav på kontinuitet i verksamheten från informationssäkerhetsperspektiv med andra kontinuitetskrav utifrån aspekter som drift, personalbemanning, material, transport och resurser.

Konsekvenserna av katastrofer, säkerhetsbrister, förlust av tjänster och tjänstetillgänglighet bör analyseras med hänsyn till inverkan på verksamheten. Kontinuitetsplaner bör upprättas och införas för att säkerställa att viktiga funktioner kan återställas inom rimlig tid. Informationssäkerhet bör vara en integrerad del av den överordnade processen för kontinuitetsplanering och även av andra ledningsprocesser inom organisationen.

Kontinuitetsplanering för verksamheten bör innefatta åtgärder för att identifiera och minska risker, förutom den allmänna riskbedömningsprocessen, begränsa konsekvenserna av skadliga incidenter och säkerställa att den information som krävs för verksamheten är tillgänglig.

14.1.1 Att inkludera informationssäkerhet i verksamhetens kontinuitetsplaneringsprocess

	Nivå
En ledningsprocess för kontinuitetsplanering i hela verksamheten bör utvecklas och underhållas. Denna process bör behandla de informationssäkerhetskrav som behövs för att hålla organisationens verksamhet i kontinuitet. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan ledningsprocess för kontinuitetsplanering finns det risk för att företaget inte klarar av att hantera kriser eller katastrofer.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Processen bör föra samman följande viktiga delar av verksamhetens kontinuitetsplanering: a) förståelse för de risker verksamheten är utsatt för i termer av sannolikhet och tidseffekter inklusive identifiering och prioritering av kritiska verksamhetsprocesser (se 14.1.2) Kommentar:			
2.	b) identifiering av samtliga berörda tillgångar i kritiska verksamhetsprocesser (se 7.1.1) Kommentar:			
3.	c) förståelse för den inverkan som avbrott orsakat av informationssäkerhetsincidenter troligen har på verksamheten (det är viktigt att hitta lösningar som hanterar såväl mindre incidenter som allvarligare incidenter som kan hota organisationens fortlevnad) och fastställa verksamhetsmålen för informationsbehandlingsresurserna Kommentar:			
4.	d) överväganden om upphandling av lämpliga försäkringar som kan ingå som led i hela kontinuitetsprocessen liksom vara en del av verksamhetens riskhantering Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
5.	e) identifiering och överväganden om införande av ytterligare förebyggande och dämpande åtgärder Kommentar:			
6.	f) identifiering av tillräckliga finansiella, organisatoriska , tekniska och miljömässiga resurser för att behandla de fastställda informationssäkerhetskraven Kommentar:			
7.	g) säkerställande av personalsäkerhet samt skydd av informationsbehandlingsresurser och av organisationens egendom Kommentar:			
8.	h) formulera och dokumentera verksamhetens kontinuitetsplaner och därvid behandla informationssäkerhetskraven i enlighet med beslutad kontinuitetsstrategi för verksamheten (se 14.1.3) Kommentar:			
9.	i) regelbunden test och uppdatering av införda planer och rutiner (se 14.1.5) Kommentar:			
10.	j) säkerställa att planeringen av verksamhetens kontinuitet är inordnad i organisationens processer och struktur, ansvaret för verksamhetens kontinuitetsplaneringsprocess bör tilldelas på en lämplig nivå inom organisationen (se 6.1.1). Kommentar:			

14.1.2 Kontinuerlig verksamhet och riskbedömning

	Nivå
Händelser som kan orsaka avbrott i verksamhetsprocesser bör identifieras tillsammans med sannolikheten och effekten av sådana avbrott och deras konsekvenser för informationssäkerheten. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Det finns en risk att en felaktig lösning som inte passar företagets behov planeras. Lösningen kan vara överdimentionerade eller underdimentionerade.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Informationssäkerhetsaspekter på kontinuerlig verksamhet bör baseras på identifiering av händelser (eller en följd av händelser) som kan orsaka avbrott i organisationens verksamhetsprocesser, som t.ex. utrustningsfel, mänskliga misstag, stöld, brand, naturkatastrofer och terroristhandlingar. Identifieringen bör följas av en riskbedömning för att bedöma sannolikhet och effekt av sådana avbrott i termer av tid, skadans omfattning och tid för återhämtning. Kommentar:			
2.	Riskbedömning i fråga om kontinuerlig verksamhet bör utföras med full medverkan av ägare av verksamhetsresurser och processägare. Denna bedömning bör omfatta alla verksamhetsprocesser och inte begränsas till informationsbehandlingsresurserna, men bör inkludera resultat som specifikt rör informationssäkerhet. Det är viktigt att länka samman de olika riskaspekterna för att få fram en fullständig bild av organisationens krav på en kontinuerlig verksamhet. I riskbedömningen bör risker identifieras, kvantifieras och prioriteras mot kriterier och mål som är relevanta för organisationen inklusive kritiska resurser, påverkan vid avbrott, godtagbar stilleståndstid och återställningsprioriteter. Kommentar:			
3.	Beroende på resultatet av riskbedömningen bör en strategi för verksamhetens kontinuitet utarbetas för att bestämma det överordnade sättet att verka för kontinuerlig verksamhet. Så snart denna strategi har utarbetats bör den bekräftas av ledningen och en plan för att införa strategin utformas och bekräftas. Kommentar:			

14.1.3 Utveckling och införande av kontinuitetsplaner innefattande informationssäkerhet

	Nivå
Planer bör utarbetas och införas för att upprätthålla eller återställa drift och säkerställa tillgänglighet till information på den nivå som krävs och inom erforderlig tid efter avbrott eller fel i kritiska verksamhetsprocesser. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan beredskapsplanering, ökar risken för långdragna störningar i verksamheten.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Planeringsprocessen för kontinuitetsplanering bör beakta följande: a) identifiering av och överenskommelser om allt ansvar och alla kontinuitetsrutiner Kommentar:			
2.	b) fastställande av godtagbar förlust av information och tjänster Kommentar:			
3.	c) införande av rutiner för att möjliggöra återhämtning och återställning av verksamhetens drift och informationstillgänglighet inom erforderlig tid; särskild uppmärksamhet behöver ägnas åt att fastställa interna och externa verksamhetsberoenden och befintliga avtal Kommentar:			
4.	d) driftsrutiner som bör följas efter genomförd återhämtning och återställning Kommentar:			
5.	e) dokumentation av överenskomna rutiner och processer Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
6.	f) erforderlig utbildning av personalen i de fastställda rutinerna och processerna inklusive krishantering Kommentar:			
7.	g) test och uppdatering av planerna. Kommentar:			
8.	Planeringen bör fokuseras på verksamhetens mål t.ex. att återställa kommunikationstjänster gentemot kunder inom godtagbar tid. De tjänster och resurser som erfordras för att underlätta detta bör fastställas inklusive bemanning, resurser som inte har med informationsbehandling att göra, liksom även reservarrangemang för informationsbehandlingsresurser. Sådana reservrutiner kan omfatta avtal med tredje part i form av ömsesidiga överenskommelser eller kommersiella tjänster. Kommentar:			
9.	Kontinuitetsplaner bör ta upp organisationens sårbarhet och kan därför omfatta känslig information som kräver lämpligt skydd. Kopior av kontinuitetsplanerna bör förvaras på annan plats på tillräckligt avstånd för att undgå skada vid en katastrof på ordinarie driftställe. Ledningen bör säkerställa att kopior av kontinuitetsplanerna är uppdaterade och har ett skydd på samma säkerhetsnivå som på ordinarie driftställe. Övrigt material som är nödvändigt för att utföra kontinuitetsplanerna bör också förvaras på annan plats. Kommentar:			
10.	Om alternativa tillfälliga lokaliteter används bör en styrning av säkerheten ha införts där som motsvarar den som tillämpas på ordinarie driftställe. Kommentar:			

Övrig information

Det bör noteras att krishanteringsplaner och -aktiviteter (se 14.1.3 f)) kan vara annorlunda än kontinuitetshanteringen; d.v.s. en kris kan inträffa som kan tas om hand genom normala ledningsrutiner.

14.1.4 Ramverk för kontinuitetsplanering i verksamheten

	Nivå
Ett samlat ramverk för kontinuitetsplanering bör finnas för att säkerställa att alla planer är konsekventa, att informationssäkerhetskraven behandlas konsekvent och för att fastställa prioriteringar gällande test och underhåll. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Inkonsekventa kontinuitetsplaner kan leda till oklara prioriteringar och att olika åtgärder tar ut varandra.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Varje kontinuitetsplan bör beskriva hur kontinuiteten behandlas, t.ex. sättet för att säkerställa informationens eller informationssystemens tillgänglighet och säkerhet. Varje plan bör också redovisa eskaleringsplanen och villkoren för aktivering av denna, liksom också de personer som är ansvariga för att exekvera varje del av planen. När nya krav identifieras bör nödrutiner, t.ex. evakueringsplaner eller reservarrangemang uppdateras efter behov. Rutiner för att säkerställa att kontinuitetsfrågor alltid får lämplig behandling bör finnas inom ramen för organisationens ändringshantering. Kommentar:			
2.	Varje plan bör ha en särskild ägare. Nödrutiner, manuella reservrutiner och återstartplaner bör ligga inom ansvarsområdet för ägaren till berörda organisationsresurser eller processer. Reservarrangemang för alternativa tekniska tjänster såsom informationsbehandlings- och kommunikationsresurser bör normalt vara ett ansvar för tjänsteleverantörerna. Kommentar:			
3.	Ett ramverk för kontinuitetsplaneringen bör behandla de identifierade säkerhetskraven och överväga följande: a) villkor för att aktivera de planer som beskriver rutinerna som ska följas (t.ex. hur situationen ska bedömas, vilka som ska beröras) innan varje enskild plan aktiveras Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
4.	b) nödrutiner som beskriver de åtgärder som ska vidtas efter en incident som äventyrar den löpande verksamheten Kommentar:			
5.	c) reservrutiner som beskriver åtgärder för att flytta viktiga verksamheter eller stödfunktioner till alternativa, tillfälliga lokaler och återföra verksamhetsprocesser i drift inom erforderlig tid Kommentar:			
6.	d) temporära driftsrutiner att följa i väntan på återhämtning och återställning Kommentar:			
7.	e) rutiner för återställning som beskriver de åtgärder som behöver vidtas för att återgå till normal verksamhet Kommentar:			
8.	f) underhållsschema som beskriver hur och när planen kommer att testas och processen för underhåll av planen Kommentar:			
9.	g) åtgärder som rör medvetenhet, information och utbildning som syftar till att skapa förståelse för kontinuitetsplaneringsprocessen och säkerställa att rutinerna är och förblir effektiva Kommentar:			
10.	h) ansvarsbeskrivningar som anger vem som ansvarar för var och en av planens olika delar. Reservpersoner bör utses om det är nödvändigt Kommentar:			
11.	i) de kritiska tillgångar och resurser som behövs för att kunna genomföra nödrutiner samt reserv- och återstartrutiner. Kommentar:			

14.1.5 Test, underhåll och omprövning av kontinuitetsplaner

	Nivå
Kontinuitetsplaner för verksamheten bör testas och uppdateras regelbundet för att säkerställa att de är aktuella och verkningsfulla. *Kritisk säkerhetsåtgärd: JA* *Risk: Backup-system måste vara synkroniserade med de normala produktionsmiljöerna. Detta kräver täta tester av konfigurationer av backup-system. Uteblivna tester medför en ökad risk för driftstörningar vid oväntade händelser.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Test av kontinuitetsplanen bör säkerställa att alla i återhämtningspersonalen liksom annan relevant personal har kännedom om planerna och sitt ansvar för verksamhetens kontinuitet och informationssäkerhet och har vetskap om sin roll när en plan startas. Kommentar:			
2.	Testschemat för kontinuitetsplanen eller -planer bör visa hur och när varje enskilt element i planen bör testas. Varje del av planen eller planerna bör testas ofta. Kommentar:			
3.	Ett flertal tekniker bör utnyttjas för att säkerställa att avbrottsplanen eller -planerna kommer att fungera i verkligheten. Teknikerna bör innefatta: a) skrivbordstest av olika avbrottsscenarier (för att diskutera arrangemang för återhämtning baserat på avbrottsexempel) Kommentar:			
4.	b) simuleringar (särskilt för att öva personal i deras roller efter incidenter och i krishantering) Kommentar:			
5.	c) tekniskt test av återhämtning (för att säkerställa att informationssystem kan återställas på ett effektivt sätt)			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	Kommentar:			
6.	d) test av återhämtning på alternativ plats (genom att köra normal drift parallellt med återhämtning på annan plats än den normala) Kommentar:			
7.	e) test av leverantörsresurser och -tjänster (för att säkerställa att externt levererade tjänster och produkter klarar avtalade åtaganden) Kommentar:			
8.	f) fullskaleövning (test av att organisationen, personal, utrustning, resurser och rutiner klarar avbrott). Kommentar:			
9.	Dessa tekniker kan användas av alla organisationer. De bör tillämpas på ett sätt som är relevant för den aktuella återställningsplanen. Resultaten av testerna bör antecknas och åtgärder vidtas för att förbättra planerna där det bedöms nödvändigt. Kommentar:			
10.	Ansvar bör tilldelas för att regelbundet granska alla kontinuitetsplaner. Genomförda förändringar i verksamheten som ännu inte återspeglas i kontinuitetsplanerna bör leda till lämplig uppdatering av planerna. Den formella processen för ändringshantering bör säkerställa att de uppdaterade planerna blir distribuerade och förstärkas av regelbundna granskningar av den fullständiga planen. Kommentar:			
11.	Exempel på förändringar där uppdatering av kontinuitetsplaner bör övervägas är anskaffning av ny utrustning, uppgradering av system och förändringar i: a) personal; b) adresser eller telefonnummer c) verksamhetsstrategi;			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	d) läge, utrustning och resurser; e) lagstiftning; f) uppdragstagare, leverantörer och viktiga kunder g) processer – även nya och indragna; h) risker (operationella och finansiella). Kommentar:			

15. Efterlevnad

15.1 Efterlevnad av rättsliga krav

Mål: Att undvika överträdelser av lagar, författningar eller avtalsförpliktelser, samt andra säkerhetskrav.

Utformning, drift, användning och administration av informationssystem kan vara föremål för bestämmelser i lagar, författningar och säkerhetskrav i avtal.

Rådgivning i frågor om särskilda rättsliga krav bör inhämtas från organisationens juridiska rådgivare eller från lämplig juridisk expertis. Rättsliga krav varierar från land till land och kan vara olika för information skapad i ett land och som överförs till annat land (s.k. trans-border data flow).

15.1.1 Identifiering av tillämplig lagstiftning

	Nivå
Tillämpliga krav i författningar och i avtal liksom organisationens sätt att uppfylla dessa krav bör explicit definieras, dokumenteras och hållas uppdaterade för varje informationssystem och för organisationen som helhet. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan regelbunden avstämning mot krav i tillämpliga författningar och avtal finns det risk för obemärkta och omedvetna lagöverträdelser.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	De specifika säkerhetsåtgärderna och det individuella ansvaret för att uppfylla kraven bör likaså definieras och dokumenteras. Kommentar:			

15.1.2 Immaterialrätt

	Nivå
Lämpliga åtgärder bör vidtas för att säkerställa efterlevnad av krav i författningar och avtal när det gäller användning av material för vilka immaterialrätt kan gälla och även i fråga om användning av upphovsrättsskyddade programvaror. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Brott mot immaterialrätten kan leda till rättsliga och ekonomiska påföljder. Dessutom kan förtroendet för organisationen ta skada.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande riktlinjer bör beaktas för att skydda material för vilket immaterialrätt kan gälla: a) publicera en policy för efterlevnad av immaterialrätt som definierar den legala användningen av programvaru- och informationsprodukter Kommentar:			
2.	b) anskaffa programvara endast genom kända och ansedda källor för att säkerställa att upphovsrätt inte kränks Kommentar:			
3.	c) vidmakthålla medvetenhet om policyer för att skydda immaterialrätten och informera om organisationens avsikt att vidta disciplinära åtgärder mot personal som bryter mot den Kommentar:			
4.	d) inrätta och vidmakthålla adekvata register över tillgångar och identifiera alla tillgångar med krav på immaterialrättsligt skydd Kommentar:			
5.	e) vidmakthålla bevis på äganderätt till licenser, masterskivor, manualer, etc Kommentar:			

Nivåstyrande frågor		JA	NEJ	VET EJ
6.	f) införa säkerhetsåtgärder för att säkerställa att eventuellt maximerat antal användare inte överskrids Kommentar:			
7.	g) kontrollera att endast godkänd programvara och licensierade produkter är installerade Kommentar:			
8.	h) ange en policy för att upprätthålla licensvillkoren Kommentar:			
9.	i) ange en policy för att avveckla eller överlåta programvara till annan Kommentar:			
10.	j) använda adekvata hjälpmedel för spårbarhet Kommentar:			
11.	k) följa villkor för att hämta och använda programvara och information från publika nät Kommentar:			
12.	l) tillse att kopiering, konvertering till annat format eller utdrag från kommersiella inspelningar (film, audio) inte sker, förutom där det tillåts enligt upphovsrättslagstiftning Kommentar:			
13.	m) tillse att kopiering, helt eller delvis, inte sker av böcker, artiklar, rapporter eller andra dokument förutom där det tillåts enligt upphovsrättslagstiftning. Kommentar:			

Övrig information

Immaterialrätten innefattar upphovsrätt på programvara eller dokument, designrättigheter, varumärken, patent och källkodslicenser.

Programvaruprodukter med äganderätt levereras vanligtvis under licensavtal som specificerar licensvillkor, t.ex. begränsning av förfoganderätten till produkterna till speciella maskiner eller begränsning av kopieringsrätten enbart till säkerhetskopiering. Den immaterialrättsliga situationen för programvara utvecklad av organisationen kräver klargörande med personalen.

Krav i författningar och avtal kan medföra begränsningar i fråga om kopiering av material med äganderätt. Särskilt kan krav ställas på att endast material som utvecklats av organisationen, eller som är licensierat, eller som tillhandahålls av den som utvecklat materialet för organisationen, får användas. Intrång i upphovsrätt kan leda till rättslig åtgärd som kan innebära domstolsförfarande.

15.1.3 Skydd av organisationens register och andra redovisande dokument

	Nivå
Organisationens viktiga register och andra redovisande dokument bör skyddas mot förlust, förstörelse och förfalskning i enlighet med författnings-, avtals- och verksamhetskrav. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om register och andra redovisande dokument inte skyddas kan det bli omöjligt att använda de som bevis i tänkbara rättstvister och brottsmål, eller i finansiell redovisning.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Register och andra redovisande dokument bör kategoriseras efter typ, t.ex. bokföringsregister, databasregister, transaktionsloggar, spårbarhetsloggar och driftsrutiner, alla med detaljer om arkiverinsgstid och lagringsmedium, t.ex. papper, microfiche, magnetmedia, optiska media. Kryptonycklar, nyckelmaterial och -program som hör till krypterade arkiv eller digitala signaturer (se 12.3) bör också sparas för att möjliggöra dekryptering av register och andra redovisande dokument under hela den tid de bevaras. Kommentar:			
2.	Risken för försämrad läsbarhet hos media som används för lagring bör beaktas. Lagrings- och hanteringsrutiner bör tillämpas i enlighet med leverantörens rekommendationer. För långtidslagring bör användning av papper och microfiche övervägas. Kommentar:			
3.	Där lagring i elektronisk form väljs bör rutiner som säkerställer läsbarheten (både medias och formatets) under hela arkiveringstiden finnas, för skydd mot förlust på grund av framtida teknikändringar. Kommentar:			
4.	System för lagring av data bör väljas så att nödvändiga data kan återhämtas inom godtagbar tid och i ett godtagbart format, beroende på de krav som ska tillgodoses. Kommentar:			
5.	Systemet för lagring och hantering bör säkerställa tydlig			

Nivåstyrande frågor		JA	NEJ	VET EJ
	identifikation av register och andra redovisande dokument och av deras arkiveringstid som de definierats i författningar, i de fall de är tillämpliga. Systemet bör tillåta erforderlig förstöring av register och andra redovisande dokument efter denna tid, om inte organisationen behöver dem. Kommentar:			
6.	För att uppfylla dessa mål för skyddet av register och andra redovisande dokument bör följande steg tas inom en organisation: a) utforma riktlinjer för bevarande, lagring, hantering och kassering av register, andra redovisande dokument, samt information b) ett arkiveringsschema som anger register och andra redovisande dokument och deras bevarandeperiod upprättas c) en förteckning över var viktig information finns bör upprättas d) erforderliga åtgärder för att skydda register, andra redovisande dokument och information från förlust, förstörelse och förfalskning bör införas. Kommentar:			

Övrig information

Vissa register och andra redovisande dokument kan behöva säkert bevarande med hänsyn till krav i författningar eller avtal och även för att stödja viktiga verksamhetsaktiviteter. Exempel på detta är register och andra redovisande dokument som kan behövas som bevis på att en organisations verksamhet bedrivs i enlighet med författningar, för att säkerställa erforderligt försvar i eventuella civil- eller brottmål eller för att bekräfta en organisations finansiella status inför aktieägare, externa parter och revisorer. Tidsperiod och datainnehåll för arkivering av information kan vara bestämd genom nationell lagstiftning.

Ytterligare information om hantering av organisationens register och andra redovisande dokument finns i ISO 15489-1.

15.1.4 Skydd av personuppgifter

	Nivå
Data- och integritetsskydd bör säkerställas i enlighet med relevant lagstiftning och, där det är tillämpligt, avtalsklausuler. *Kritisk säkerhetsåtgärd: JA* *Risk: Utan rätt skydd av personuppgifter finns det en risk att information hamnar i fel händer. Detta kan leda till att personlig information säljs och används för identitetsstöld.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Organisationen bör utforma och införa en policy för data- och integritetsskydd. Denna policy bör meddelas till alla personer som är involverade i bearbetningen av personuppgifter. Kommentar:			
2.	Efterlevnad av denna policy och alla relevanta författningar ställer krav på lämplig ledningsstruktur och styrning. Ofta kan detta uppnås genom att utse ett personuppgiftsombud som har till uppgift att vägleda chefer, användare och servicepersonal i frågor om deras individuella ansvar och de särskilda rutiner som bör följas. Ansvar för hantering av personuppgifter och för att säkerställa medvetenhet om dataskyddsprinciper bör handläggas i enlighet med relevant lagstiftning. Lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter bör införas. Kommentar:			

Övrig information
Ett antal länder har infört lagstiftning med säkerhetsåtgärder avseende insamling, bearbetning och överföring av personuppgifter (generellt information om levande personer som kan identifieras genom informationen). Beroende på respektive nationell lagstiftning kan sådana åtgärder ålägga skyldigheter på den som insamlar, bearbetar, och sprider personuppgifter och kan innebära begränsningar i möjligheterna att överföra dessa data till andra länder.

15.1.5 Förhindrande av missbruk av informationsbehandlingsresurser

	Nivå
Användare bör avrådas från att använda informationsbehandlingsresurser för obehöriga ändamål. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Missbruk av informationsbehandlingsresurser kan leda till störningar och ha för avsikt att få obehörig åtkomst.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Ledningen bör lämna sitt godkännande för användning av informationsbehandlingsresurser. All användning av dessa resurser för annat än organisationens ändamål utan ledningens godkännande (se 6.1.4), eller för annat eventuellt obehörigt ändamål bör betraktas som otillbörlig användning av resurserna. Om någon obehörig åtgärd identifieras genom övervakning eller andra metoder bör den berörde chefen uppmärksammas på detta för att överväga lämplig disciplinär eller rättslig åtgärd. Kommentar:			
2.	Juridisk rådgivning bör inhämtas innan övervakningsrutiner införs. Kommentar:			
3.	Alla användare bör vara medvetna om den exakta omfattningen av den åtkomst som tillåts dem och den övervakning som görs för att upptäcka obehörig användning. Detta kan uppnås genom att ge användarna skriftlig behörighet. En kopia bör signeras av användaren och bevaras på ett säkert sätt av organisationen. Anställda i en organisation, uppdragstagare och tredjepartsanvändare bör meddelas att ingen åtkomst beviljas utom den för vilken behörighet givits. Kommentar:			
4.	Vid påloggning bör ett varningsmeddelande visas som säger att den informationsbehandlingsresurs som påloggas ägs av organisationen och att obehörig åtkomst inte tillåts. Användaren måste bekräfta och reagera på avsett sätt på meddelandet på skärmen för att kunna fortsätta påloggningen (se 11.5.1). Kommentar:			

Övrig information

En organisations informationsbehandlingsresurser är avsedda primärt eller uteslutande för verksamheten.

Upptäckt av intrång, kontroll av innehåll och andra redskap för övervakning kan hjälpa till att förhindra och upptäcka missbruk av informationsbehandlingsresurser.

Många länder har lagstiftning till skydd mot missbruk av datorer. Det kan vara en brottslig handling att använda en dator för obehöriga ändamål.

Lagenligheten av att övervaka användningen varierar från land till land och kan ställa krav på att ledningen meddelar alla användare om sådan övervakning och/eller erhåller deras godkännande. I de fall systemet som påloggningen avser utnyttjas för allmän åtkomst (t.ex. en webbserver) och är föremål för säkerhetsövervakning bör ett meddelande om detta visas.

15.1.6 Reglering av kryptering

	Nivå
Kryptering bör användas i enlighet med alla relevanta avtal och författningar. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Risk för bristande efterlevnad av gällande avtal, lagar och fordringar kan leda till rättsliga åtgärder och ekonomiska förluster, och skadat anseende.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	Följande punkter bör beaktas för att nå överensstämmelse med relevanta avtal, lagar och författningar: a) begränsningar för import och/eller export av hårdvara och mjukvara för att utföra krypteringsfunktioner Kommentar:			
2.	b) begränsningar för import och/eller export av hårdvara och mjukvara avsedda att kompletteras med krypteringsfunktioner Kommentar:			
3.	c) begränsningar i användningen av kryptering Kommentar:			
4.	d) obligatoriska eller frivilliga metoder för landets myndigheters åtkomst till information som krypterats med hårdvara eller mjukvara för att erhålla konfidentialitet för innehållet. Kommentar:			
5.	Juridisk rådgivning bör sökas för att säkerställa efterlevnad av nationell lagstiftning. Innan krypterad information eller medel för kryptering flyttas till annat land bör också juridiska råd inhämtas. Kommentar:			

15.2 Efterlevnad av säkerhetspolicyer, -standarder och teknisk efterlevnad

Mål: Att säkerställa att system följer organisationens säkerhetspolicyer och -standarder.

Informationssystemens säkerhet bör granskas regelbundet.

Sådana granskningar bör ske mot tillämpliga säkerhetspolicyer. De tekniska plattformarna och informationssystemen bör granskas vad avser efterlevnad av tillämpliga standarder för införande av säkerhet och dokumenterade säkerhetsåtgärder.

15.2.1 Efterlevnad av säkerhetspolicyer och -standarder

	Nivå
Chefer bör säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområden utförs korrekt för att uppnå efterlevnad av säkerhetspolicyer och -standarder. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Utan att kontrollera att säkerhetsåtgärder fungerar som avsett och utan regelbundna granskningar, finns det en ökad risk att säkerhetsåtgärder blir ineffektiva med avseende på risksituationen.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Chefer bör regelbundet granska efterlevnaden av tillämpliga säkerhetspolicyer, standarder och andra säkerhetskrav ifråga om informationsbehandling inom sina respektive ansvarsområden. Kommentar:			
2.	Om eventuell avvikelse påträffas som resultat av granskningen bör chefer: a) ta reda på anledningen till avvikelsen b) bedöma behovet av åtgärder för att säkerställa att bristande efterlevnad inte inträffar igen c) besluta om och införa lämpliga korrigerande åtgärder			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
	d) granska de korrigerande åtgärder som vidtagits. Kommentar:			
3.	Resultat av granskningar och korrigerande åtgärder vidtagna av chefer bör dokumenteras och dessa dokument bevaras. Chefer bör rapportera resultatet till de personer som genomför de oberoende granskningarna (se 6.1.8) när den oberoende granskningen äger rum inom eget ansvarsområde. Kommentar:			

Övrig information
Övervakning av system i drift behandlas i 10.10.

15.2.2 Kontroll av teknisk efterlevnad

	Nivå
Informationssystem bör regelbundet kontrolleras vad avser efterlevnad av standarder för införande av säkerhet. *Kritisk säkerhetsåtgärd: JA* *Risk: Att inte kontrollera systemsäkerheten (inklusive sårbarheter i systemet) och dess stödjande systemkomponenter ökar risken att systemet inte fungerar som förväntat och att sannolikheten för säkerhetshål (både misstag och attacker) ökar. Risken är hög med tanke på befintliga svagheter i övervakning och sårbarhet och patchhantering.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Kontroll av teknisk efterlevnad bör utföras antingen manuellt (med stöd av lämpliga programvaruhjälpmedel, om nödvändigt) av en erfaren systemexpert och/eller med hjälp av automatiserade verktygsprogram som genererar en teknisk rapport för efterföljande tolkning av en teknisk specialist. Kommentar:			
2.	Om penetrationstester eller sårbarhetsanalyser utförs bör försiktighet iakttas eftersom sådana åtgärder kan leda till att systemets säkerhet äventyras. Sådana tester bör vara planerade, dokumenterade och möjliga att upprepa. Kommentar:			§
3.	Kontroll av teknisk efterlevnad bör endast utföras av kompetenta, behöriga personer eller under övervakning av sådana personer. Kommentar:			

Övrig information
Kontroll av teknisk efterlevnad innefattar granskning av driftsystem för att säkerställa att skydd för hårdvara och programvara har implementerats korrekt. Denna typ av efterlevnadskontroll ställer krav på teknisk expertis.

Efterlevnadskontroll täcker också t.ex., penetrationstester och sårbarhetsanalyser som kan utföras av oberoende experter särskilt kontrakterade för detta ändamål. Detta kan vara nyttigt när det gäller att upptäcka sårbarheter i systemet och för att kontrollera hur effektiva säkerhetsåtgärderna är när det gäller att förhindra obehörig åtkomst som en följd av dessa sårbarheter.

Penetrationstester och sårbarhetsanalyser ger en ögonblicksbild av ett system i ett specifikt tillstånd vid en specifik tidpunkt. Ögonblicksbilden är begränsad till de delar av systemet som faktiskt testas under penetrationstesten/-erna. Penetrationstester och sårbarhetsanalyser är inte en ersättning för riskbedömning.

15.3 Överväganden vid revision av informationssystem

Mål: Att maximera revisionens verkan och minimera störningar på/från IT-revisionsprocessen.

Säkerhetsåtgärder bör finnas för att skydda system i drift och granskningsverktyg under pågående revision av informationssystem.

Skydd krävs också av granskningsverktygen för att bevara deras riktighet och systemintegritet samt för att förhindra missbruk.

15.3.1 Säkerhetsåtgärder för revision av informationssystem

	Nivå
Revisionens krav och åtgärder som innefattar kontroller av system i drift bör planeras noggrant och godkännas för att minimera risken för störningar i verksamhetsprocesser. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Om systemsäkerheten är kontrollerad på ett olämpligt sätt, kan detta leda till driftsstörningar. Även obehörig åtkomst kan erhållas.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Följande vägledning bör observeras: a) revisionens krav bör behandlas i samråd med berörda chefer Kommentar:			
2.	b) omfattningen av kontrollerna bör överenskommas och styras Kommentar:			
3.	c) kontrollerna bör begränsas till läsåtkomst (read-only access) av programvara och data Kommentar:			

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
4.	d) annan åtkomst än läsåtkomst bör endast tillåtas för isolerade kopior av systemfiler som bör raderas när revisionen genomförts alternativt ges tillfredsställande skydd om det är nödvändigt att behålla sådana filer med hänsyn till krav på dokumentation av revisionen Kommentar:			
5.	e) resurser som krävs för att genomföra kontrollerna bör uttryckligt definieras och ställas till revisionens förfogande Kommentar:			
6.	f) krav på särskilda eller ytterligare bearbetningar för revisionsändamål bör identifieras och godkännas Kommentar:			
7.	g) all åtkomst bör följas upp och loggas för att åstadkomma spårbarhet; användning av tidsstämplade revisionsspår bör övervägas för kritiska data eller system Kommentar:			
8.	h) alla rutiner, krav och ansvarsförhållanden bör dokumenteras Kommentar:			
9.	i) den eller de personer som genomför revisionen bör vara oberoende i förhållande till de aktiviteter som revideras. Kommentar:			

15.3.2 Skydd av verktyg för granskning av informationssystem

	Nivå
Åtkomst till granskningsverktyg för informationssystem bör begränsas för att hindra eventuellt missbruk eller otillåten påverkan. *Kritisk säkerhetsåtgärd: NEJ* *Risk: Ifall tredje part deltar i en revision, kan det finnas risk för missbruk av granskningsverktyg av denna tredje part, och att denna tredje parts organisation får åtkomst till information.*	

NIVÅ: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		JA	NEJ	VET EJ
1.	Granskningsverktyg för informationssystem, t.ex. programvara eller datafiler, bör förvaras åtskilda från utvecklings- och produktionssystem och inte förvaras i bandbibliotek eller hos användare om de inte får särskilt anpassat ytterligare skydd. Kommentar:			

Övrig information

Ifall tredje part är involverad i en revision, kan det finnas risk för missbruk av granskningsverktygen av dessa tredje parter, och att denna tredje parts organisation får åtkomst till information. Säkerhetsåtgärder som i 6.2.1 (att bedöma risken) och 9.1.2 (att begränsa fysisk åtkomst) kan övervägas för hantering av denna risk. Eventuella följdåtgärder bör vidtas, såsom att omedelbart ändra lösenord som avslöjats för revisorerna.