GAP-analys av 27002

Efterlevnad av standarden

Innehållsförteckning

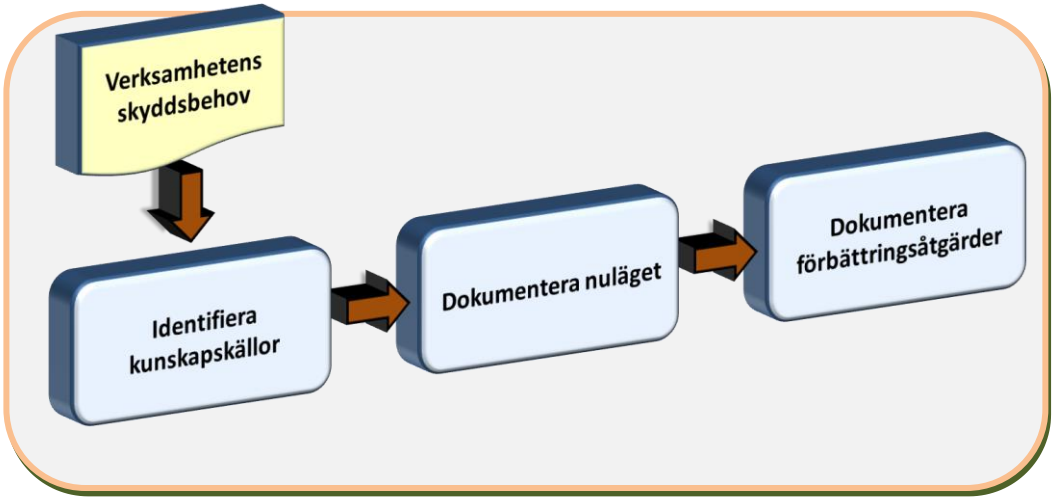
1. Introduktion

1.1 Inledning

De flesta verksamheter i dag är väldigt komplexa, med en blandning av teknologier, processer och medarbetare som alla samverkar för att hantera verksamhetens information på ett så bra sätt som möjligt. Huvudsyftet är att stödja, så att organisationens mål uppfylls. Verksamhetens information måste skyddas så att den alltid är *konfidentiell*, *tillgänglig* och *riktighet*, och därför inför man ett ledningssystem och *administrativa*, *organisatoriska*, *fysiska* och *logiska* skydd.

Det finns därför ett stort behov att tidigt utvärdera på vilken nivå en verksamhets informationssäkerhetsarbete befinner sig i. Genom att värdera sitt skydd kan verksamheten få ett bra kvitto på hur sårbar den är för olika risker som kan uppträda, och det skapar också en trygghet i organisationen att veta hur man mår. Vi har därför tagit fram denna metod för gap-analys, som gör det möjligt att snabbt skapa sig en bild av nuläget för informationssäkerheten. Gap-analysen utförs efter att behov, krav och risker har kartlagts genom verksamhetsanalys och riskanalys. Uttrycket syftar på gapet mellan det som standarden beskriver som bästa praxis och den rådande säkerhetsnivån i verksamheten. Arbetsuppgifterna för gap-analysen illustreras i figuren nedan.

Figur 1. Arbetsuppgifterna under gap-analysen



1.2 Mål och syfte

Målet med denna metod är att vara ett underlag för kontroll av verksamhetens införande av ett ledningssystem (LIS). Metoden ger vägledning för hur denna kontroll går till och skapar ett underlag för att planerat arbeta vidare med de brister som finns.

Syftet med att utföra gap-analysen är att få:

- bevis på hur effektivt ni infört ledningssystem och nivån på ert skydd
- en uppfattning om kvaliteten på informationssäkerhetsarbetet och er säkerhetsprocess
- ett underlag för resten av arbetet med att införa ledningssystemet

1.3 Målgrupp

Den här metoden för gap-analys är användbar för flera grupper av användare:

- projekt som ska införa ett ledningssystem för informationssäkerhet
- personer som är ansvariga för att mäta eller verifiera nivån på säkerhetsskyddet
- verksamhetschefer som vill ställa krav på sin skyddsnivå, till exempel systemägare
- säkerhets- eller informationssäkerhetsansvariga som ska mäta effektiviteten i skyddet.

1.4 När ska metoden användas?

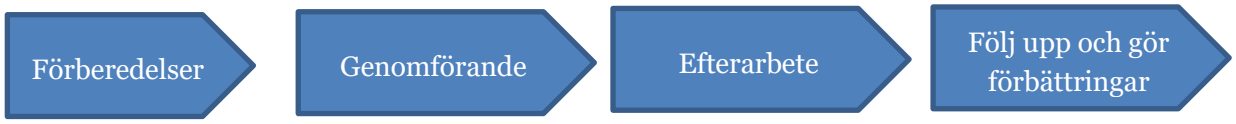
Metoden ska användas för att få fram gapet mellan den existerande och den önskade säkerhetsnivån, innan organisationen inför ett LIS. I metodstödet finner ni två versioner av gap-analysen en för 27001 och en för 27002. Metoden är generisk och fungerar på de flesta verksamheter, även om den troligtvis behöver anpassas något. En viktig del i säkerhetsarbetet är att årligen följa upp säkerhetsnivåns status och verktyget passar bra även för det ändamålet.

2. Metod

2.1 Arbetsflöde vid gap-analys

I detta avsnitt beskrivs stegen för att utföra gap-analysen översiktligt. Det finns ett antal steg som analysledaren bör gå igenom före, under och efter analysen, och en del saker att tänka på. I figuren nedan anges schematiskt stegen för genomförande.

Figur 2. Övergripande process för att göra en gap-analys:



Det första steget i arbetet med gap-analysen utgörs alltså av förberedelser. Det innefattar bland annat att identifiera kunskapskällor, det vill säga kartlägga vilka områdesansvariga man behöver information från, att skicka ut analysunderlag till dem, och att bestämma en agenda för analysarbetet.

I genomförandesteget utförs sedan själva analysen. Förslagsvis utför man en rundvandring och analys av den fysiska miljön, för att sedan gå över i intervjuer med berörda parter. Intervjuerna utgår från underlaget som presenteras i nästa kapitel. Observationer och intervjusvar används sedan för en dokumentation av nuläget genom att sammanställa säkerhetsnivåer för de olika områdena i underlaget, och sammanfatta de brister som framkommit.

När analysarbetet är genomfört bör resultaten sammanställas i en nivå- och bristrapport som skickas till alla medverkande för avstämning, varpå en åtgärdsplan utformas och slutrapport skrivs. Slutrapporten kan sedan användas som underlag för förbättringar i organisationens informationssäkerhetsarbete.

2.2 Intervjuteknik

Eftersom detta är en subjektiv och kvalitativ metod är det viktigt att man får en god kontakt med intervjupersonerna. Det är lämpligt att skapa ett bra rum att vara i och låta de som ska intervjuas komma till analysledaren. Ett annat tips är att ge alla som intervjuas en egen kopia av underlaget att titta i. Analysledaren ställer frågor och de intervjuade svarar ja eller nej med kommentarer. Om analysledaren inte kan området i detalj kan man ställa frågan och låta de intervjuade tolka och analysera den. Be alla som intervjuas vara ärliga då detta är hjälp till självhjälp.

2.3 Bedömning av säkerhetsnivåer

Analysledaren ska efter intervjuer och observationer analysera materialet och ange vilka värden som de olika delområdena i underlaget bör få. Värdebedömningar görs enligt skalan nedan.

Nivåskala för bedömningar

0 = Oacceptabelt (ingen efterlevnad)
0,5
1 = Risk (bristfällig efterlevnad)
1,5
2 = Liten risk (acceptabel efterlevnad)
2,5
3 = Mycket liten risk (stor efterlevnad)

För att bestämma en huvudfrågas nivå måste man göra en sammantagen bedömning av frågesvaren och sina egna observationer på plats, samt använda sin erfarenhet. Olika analysledare brukar göra i stort sett samma bedömningar av samma material – sällan skiljer det mer än 0,5 poäng per fråga.

2.4 Att tänka på

När åtgärderna ska granskas är det viktigt att tänka i flera dimensioner för att få reda på om åtgärden är effektiv och ändamålsenlig:

- Är skyddsåtgärden dokumenterad?
- Är skyddsåtgärden verkligen på plats och används den?
- Fungerar skyddsåtgärden som det är tänkt?
- Underhålls skyddsåtgärden?

2.5 Efter gap-analysen

När analysen har genomförts har organisationen en bra dokumentation över alla informationstillgångar, risker och sårbarheter. Med denna kunskap går det att utforma ett lämpligt sätt att styra och leda ledningssystemet för informationssäkerhet.

Hänvisa till MSB metodstöd.

3. Vad ska analyseras?

De områden som ska analyseras är de områden ni ser i bilden enligt nedan:

- Organisationens förutsättningar
- Ledarskap
- Planering
- Stöd
- Verksamhet
- Utvärdering och prestanda
- Förbättringar

Kap.	Rubrik	Antal skydds-åtgärder
5	Informationssäkerhetspolicyer	2
6	Organisation av informationssäkerhet	7
7	Personalsäkerhet	6
8	Hantering av tillgångar	10
9	Styrning av åtkomst	14
10	Kryptografi	2
11	Fysisk och miljörelaterad säkerhet	15
12	Driftsäkerhet	14
13	Kommunikationssäkerhet	7
14	Anskaffning, utveckling och underhåll av system	13
15	Leverantörsrelationer	5
16	Information security incident management	7

Kap.	Rubrik	Antal skydds-åtgärder
17	Hantering av informationssäkerhetsincidenter informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet	4
18	Efterlevnad	8

Själva analysdelen har samma numrering som kapitlen i 27002.

5 Informationssäkerhetspolicy

	Nivå
Här beskrivs nivån totalt för detta kapitel genom ett genomsnitt av de olika avsnitten.	

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

5.1 Ledningens inriktning för informationssäkerhet

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

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

5.1.1 Informationssäkerhetspolicy

Säkerhetsåtgärd

Ett regelverk för informationssäkerhet, som inkluderar informationssäkerhetspolicyn, bör fastställas, godkännas av ledningen, publiceras och kommuniceras till medarbetare och relevanta externa parter. **Svensk ANM.** Den engelska termen ”policys” översätts i den svenska texten med policy och vidhängande regelverk. Termen ”policy” används i översättningen enbart för organisationens övergripande informationssäkerhetspolicy. För övriga förekomster av termen ”policy” används de svenska termerna regler och regelverk. Detta överensstämmer med definitionen av policy i SS-ISO/IEC 27000 och med svenskt språkbruk. *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)

5.1.2 Granskning av regelverk för informationssäkerhet

Säkerhetsåtgärd

	Nivå

Regelverket (inklusive informationssäkerhetspolicyn) för informationssäkerhet bör granskas med planerade intervall, eller om betydande förändringar sker, för att säkerställa deras fortsatta lämplighet, riktighet och verkan. *Kritisk säkerhetsåtgärd: Nej* *Risk: Utan regelbunden översyn kan regelverket (inkl. säkerhetspolicyn) tappa sin effektivitet som verktyg för riskhantering och styrning av informationssäkerhetsarbetet.*	

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

6 Organisation av informationssäkerhetsarbetet

	Nivå
Här beskrivs nivån totalt för detta kapitel.	

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

6.1 Intern organisation

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

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

6.1.1 Informationssäkerhetsroller och ansvar

Säkerhetsåtgärd

	Nivå
Allt ansvar för informationssäkerhet bör definieras och tilldelas. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan en tydlig ansvarsfördelning ökar risken att en uppgift lämnas därhän i tron att någon annan bär ansvaret. (en risk kan fall mellan två stolar)*	

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

6.1.2 Uppdelning av arbetsuppgifter

Säkerhetsåtgärd

Ansvar och ansvarsområden som står i konflikt med varandra bör åtskiljas för att minska möjligheterna för obehörig eller oavsiktlig ändring eller missbruk av organisationens tillgångar. *Kritisk säkerhetsåtgärd: Nej* *Risk:* Om inte det är en strikt uppdelning av arbetsuppgifter finns det risk för oavsiktligt eller avsiktligt missbruk av organisationens tillgångar.	**Nivå**

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

6.1.3 Kontakt med myndigheter

Säkerhetsåtgärd

Lämpliga kontakter med relevanta myndigheter bör upprätthållas. *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)

6.1.4 Kontakt med särskilda intressegrupper

Säkerhetsåtgärd

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

6.1.5 Informationssäkerhet i projektledning

Säkerhetsåtgärd

	Nivå

Informationssäkerhet bör hanteras inom projektledning, oavsett typ av projekt. *Kritisk säkerhetsåtgärd: Ja* *Risk:* Informationssäkerhetsriskerna hanteras inte i projektet.	

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

6.2 Mobila enheter och distansarbete

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

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

6.2.1 Regler för mobila enheter

Säkerhetsåtgärd

Regler och stödjande säkerhetsåtgärder bör antas för att hantera de risker som användning av mobila enheter medför. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan regler för hantering av mobila enheter (till exempel USB- minnen), ökar risken för att information lämnar verksamheten, både avsiktligt och oavsiktligt.*	**Nivå**

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

6.2.2 Distansarbete

Säkerhetsåtgärd

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

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

7 Personalsäkerhet

	Nivå
Här beskrivs nivån totalt för detta kapitel.	

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

7.1 Före anställning

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

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

7.1.1 Bakgrundskontroll

Säkerhetsåtgärd

Bakgrundskontroll på alla sökande för anställning bör utföras i enlighet med relevanta författningar och etiska krav och bör stå i proportion till verksamhetskraven, klassificeringen av information som de ges behörighet till och de upplevda riskerna. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan en noggrann verifiering av den sökandes kompetens (vilja och förmåga) att arbeta enligt organisationens krav gällande informationssäkerhet ökar risken för informationsläckage eller att information modifieras eller förstörs.*	Nivå

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

7.1.2 Anställningsvillkor

Säkerhetsåtgärd

	Nivå

Avtal med anställda och leverantörer bör ange deras 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)

7.2 Under anställning

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

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

7.2.1 Ledningens ansvar

Säkerhetsåtgärd

Ledningen bör kräva att alla anställda och leverantörer tillämpar informationssäkerhetskrav i enlighet med för organisationen fastställda regler och rutiner. *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 för att skapa en säkerhetskultur i verksamheten.*	**Nivå**

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

7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet

Säkerhetsåtgärd

	Nivå

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

7.2.3 Disciplinär process

Säkerhetsåtgärd

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

7.3 Avslut eller ändring av anställning

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

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

7.3.1 Avslut eller ändring av anställds ansvar

Säkerhetsåtgärd

	Nivå

Ansvar för informationssäkerhet och skyldigheter som förblir gällande efter avslut eller ändring av anställning, bör definieras och kommuniceras till den anställde eller leverantören samt verkställas. **Svensk ANM**: Svensk arbetsrätt är styrande vid uppsägning eller ändring av anställning. *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)

8 Hantering av tillgångar

	Nivå
Här beskrivs nivån totalt för detta kapitel.	

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

8.1 Ansvar för tillgångar

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

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

8.1.1 Inventering av tillgångar

Säkerhetsåtgärd

	Nivå

Tillgångar som är relaterade till information och informationsbehandlingsresurser bör identifieras och en förteckning över dessa 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: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

8.1.2 Ägarskap av tillgångar

Säkerhetsåtgärd

Tillgångar som återfinns i sammanställningen bör tilldelas ägare. *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)

8.1.3 Tillåten användning av tillgångar

Säkerhetsåtgärd

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

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

8.1.4 Återlämnande av tillgångar

Säkerhetsåtgärd

Alla anställda och externa användare bör återlämna alla organisationens tillgångar som de förfogar över då deras anställning, uppdrag eller avtal upphör. *Kritisk säkerhetsåtgärd: Nej* *Risk: Om tillgångar inte återlämnas uppstår en risk för ekonomisk förlust, avslöjande av hemlig information och brott mot immaterialrätten.*	**Nivå**

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

8.2 Informationsklassning

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

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

8.2.1 Klassning av information

Säkerhetsåtgärd

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

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

8.2.2 Märkning av information

Säkerhetsåtgärd

	Nivå

En lämplig uppsättning rutiner för märkning av information bör utvecklas och införas i enlighet med den modell för informationsklassning 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)

8.2.3 Hantering av tillgångar

Säkerhetsåtgärd

Rutiner för hantering av tillgångar bör utvecklas och införas i enlighet med den modell för informationsklassning som antagits av organisationen. *Kritisk säkerhetsåtgärd: Ja* *Risk: Risken är att tillgången inte identifieras utifrån dess värde och får det skydd den behöver.*	**Nivå**

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

8.3 Hantering av lagringsmedia

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

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

8.3.1 Hantering av flyttbara lagringsmedia

Säkerhetsåtgärd

	Nivå

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

8.3.2 Avveckling av lagringsmedia

Säkerhetsåtgärd

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

8.3.3 Transport av fysiska lagringsmedia

Säkerhetsåtgärd

	Nivå
Lagringsmedia som innehåller information bör skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport. *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: 0=OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1=RISK (BRISTFÄLLIG EFTERLEVNAD), 2=LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3=MYCKET LITEN RISK (STOR EFTERLEVNAD)

9 Styrning av åtkomst

	Nivå
Här beskrivs nivån totalt för detta kapitel.	

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

9.1 Verksamhetskrav för styrning av åtkomst

Mål: Att begränsa åtkomst till information och informationsbehandlingsresurser	**Nivå**

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

9.1.1 Regler för styrning av åtkomst

Säkerhetsåtgärd

Regler för styrning av åtkomst bör upprättas, dokumenteras och vara föremål för uppföljning utifrån verksamhets- och informationssäkerhetskrav. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan åtkomstregler, 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**

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

9.1.2 Tillgång till nätverk och nätverkstjänster

Säkerhetsåtgärd

Användare bör endast ges tillgång till nätverk och nätverkstjänster som de specifikt beviljats tillstånd för. *Kritisk säkerhetsåtgärd: Ja* *Risk:* Användare kan få till gång till information de inte har rätt till och om en angripare tagit över en användares dator kan denne ges stora möjligheter att kartlägga och stjäla information.	**Nivå**

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

9.2 Hantering av användaråtkomst

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

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

9.2.1 Registrering och avregistrering av användare

Säkerhetsåtgärd

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

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

9.2.2 Tilldelning av användaråtkomst

Säkerhetsåtgärd

En formell process för tilldelning av användaråtkomst bör införas för tilldelning och återkallande av åtkomsträttigheter för alla typer av användare till alla system och tjänster. *Kritisk säkerhetsåtgärd: Ja* *Risk: Finns inte en process för tilldelning av användaråtkomst är risken att vi har användare som inte har rätt rättigheter i systemet.*	**Nivå**

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

9.2.3 Hantering av privilegierade åtkomsträttigheter

Säkerhetsåtgärd

Tilldelning och användning av privilegierade åtkomsträttigheter 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**

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

9.2.4 Hantering av användares konfidentiella autentiseringsinformation

Säkerhetsåtgärd

Tilldelningen av konfidentiell autentiseringsinformation bör styras genom en formell hanteringsprocess. *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**

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

9.2.5 Granskning av användares åtkomsträttigheter

Säkerhetsåtgärd

Ägare av tillgångar bör med jämna mellanrum granska användarnas åtkomsträttigheter. *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**

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

9.2.6 Borttagning eller justering av åtkomsträttigheter

Säkerhetsåtgärd

Åtkomsträttigheterna för alla anställda, och externa användare, till information och informationsbehandlingsresurser bör tas bort vid avslutande av deras anställning, avtal eller uppdrag eller justeras vid förändringar. *Kritisk säkerhetsåtgärd: Nej* *Risk: Annan kan använda sig av rättigheter som en användare haft som slutat.*	**Nivå**

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

9.3 Användaransvar

Mål: Att göra användare ansvariga för att skydda sin autentiseringsinformation	**Nivå**

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

9.3.1 Användning av konfidentiell autentiseringsinformation

Säkerhetsåtgärd

Användare bör åläggas att följa organisationens arbetssätt gällande användning av konfidentiell autentiseringsinformation. *Kritisk säkerhetsåtgärd: Nej* *Risk: Utan god säkerhetssed vid val av lösenord ökar risken för otillåtna inloggningar och försämrad tillförlitlighet (användning av ”stulna” inloggningsuppgifter).*	**Nivå**

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

9.4 Styrning av åtkomst till system och tillämpningar

Mål: Att förhindra obehörig åtkomst till system och tillämpningar	**Nivå**

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

9.4.1 Begränsning av åtkomst till information

Säkerhetsåtgärd

Tillgång till information och systemfunktioner bör begränsas i enlighet med regler för styrning av åtkomst. *Kritisk säkerhetsåtgärd: Ja* *Risk: Om inga säkra påloggningsrutiner finns, kan en obehörig användare komma åt företagets information och system.*	**Nivå**

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

9.4.2 Säkra inloggningsrutiner

Säkerhetsåtgärd

Där regler för styrning av åtkomst så kräver, bör tillgång till system och tillämpningar styras genom säkra inloggningsrutiner. *Kritisk säkerhetsåtgärd: Ja* *Risk: en angripare har lätt att ta in sig i systemet som inte motsvarar det skydd informationen borde ha.*	**Nivå**

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

9.4.3 System för lösenordshantering

Säkerhetsåtgärd

System för lösenordshantering bör vara interaktiva och bör säkerställa kvalitativa lösenord. *Kritisk säkerhetsåtgärd: Ja* *Risk: Förstår inte en användare hur hen kan konstruera bra lösenord och finns det inte styrning av detta kan det leda till att en angripare får det lätt att ta sig in i systemet.*	**Nivå**

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

9.4.4 Användning av privilegierade verktygsprogram

Säkerhetsåtgärd

Användning av verktygsprogram som kan ha förmåga att kringgå säkerhetsåtgärder i system och tillämpningar bör begränsas och styras strikt. *Kritisk säkerhetsåtgärd: Nej* *Risk: Om sessioner inte kopplas ner automatiskt blir det möjligt för obehöriga att utföra överbelastningsattacker (Denial of Service).*	**Nivå**

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

9.4.5 Åtkomstkontroll till källkod för program

Säkerhetsåtgärd

	Nivå

Tillgång till källkod för program 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)

10 Kryptering

	Nivå
Här beskrivs nivån totalt för detta kapitel.	

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

10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder

Säkerhetsåtgärd

	Nivå
Regler för användning av kryptografiska säkerhetsåtgärder för skydd av information bör utvecklas och införas. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan regler 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)

10.1.2 Nyckelhantering

Säkerhetsåtgärd

	Nivå

Regler för användning, skydd och giltighetstid för kryptografiska nycklar för deras hela livscykel bör utvecklas och införas. *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)

11 Fysisk och miljörelaterad säkerhet

	Nivå
Här beskrivs nivån totalt för detta kapitel.	

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

11.1 Säkra områden

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

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

11.1.1 Fysiska säkerhetsavgränsningar

Säkerhetsåtgärd

Fysiska avgränsningar bör definieras och användas för att skydda områden som innehåller antingen känslig eller kritisk information och informationsbehandlingsresurser. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan skalskydd exponeras system och (informations-) tillgångar och kan lättare stjälas, skadas eller manipuleras.*	**Nivå**

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

11.1.2 Fysiska tillträdesbegränsningar

Säkerhetsåtgärd

Säkra områden bör skyddas genom lämpliga säkerhetsåtgärder 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**

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

11.1.3 Säkerställande av kontor, rum och anläggningar

Säkerhetsåtgärd

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

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

11.1.4 Skydd mot yttre och miljörelaterade hot

Säkerhetsåtgärd

Fysiskt skydd mot naturkatastrofer, illvilliga angrepp eller olyckor 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**

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

11.1.5 Arbeta i säkra utrymmen

Säkerhetsåtgärd

	Nivå

Rutiner för att arbeta i säkra utrymmen bör utformas 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)

11.1.6 Leverans- och lastningsområden

Säkerhetsåtgärd

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

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

11.2 Utrustning

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

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

11.2.1 Placering av utrustning och skydd

Säkerhetsåtgärd

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

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

11.2.2 Tekniska försörjningssystem

Säkerhetsåtgärd

Utrustning bör skyddas från elavbrott och andra störningar som orsakas av fel 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**

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

11.2.3 Kablagesäkerhet

Säkerhetsåtgärd

Kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada. *Kritisk säkerhetsåtgärd: Nej* *Risk: Bristfälligt kablageskydd medför en ökad risk för störningar, överföringsfel och obehörig avlyssning.*	**Nivå**

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

11.2.4 Underhåll av utrustning

Säkerhetsåtgärd

Utrustning bör underhållas korrekt för att säkerställa fortsatt tillgänglighet och riktighet. *Kritisk säkerhetsåtgärd: Nej* *Risk: Bristfällig service och underhåll av utrustning kan leda till avbrott och haveri.*	**Nivå**

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

11.2.5 Utförsel av tillgångar

Säkerhetsåtgärd

Utrustning, information eller program bör inte avlägsnas utanför organisationens lokaler utan tillstånd. *Kritisk säkerhetsåtgärd: Nej* *Risk: Information och tillgångar kan exponeras på ett sätt som verksamheten inte önskar.*	**Nivå**

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

11.2.6 Säkerhet för utrustning och tillgångar utanför organisationens lokaler

Säkerhetsåtgärd

Säkerhet bör tillämpas på tillgångar utanför organisationens lokaler med hänsyn till de särskilda risker som finns förknippade med att arbeta utanför organisationens lokaler. *Kritisk säkerhetsåtgärd: Nej* *Risk: Utan regler för hantering av utrustningen utanför de egna lokalerna ökar risken för informationsförlust, informationsspridning eller skada på utrustningen.*	**Nivå**

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

11.2.7 Säker kassering eller återanvändning av utrustning

Säkerhetsåtgärd

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

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

11.2.8 Obevakad utrustning som hanteras av användare

Säkerhetsåtgärd

Användare bör säkerställa att obevakad utrustning har lämpligt skydd. *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**

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

11.2.9 Regel om rent skrivbord och tom skärm

Säkerhetsåtgärd

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

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

12 Driftsäkerhet

Här beskrivs nivån totalt för detta kapitel.	**Nivå**

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

12.1 Driftsrutiner och ansvar

	Nivå

Mål: Att säkerställa korrekt och säker drift av informationsbehandlingsresurser	

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

12.1.1 Dokumenterade driftsrutiner

Säkerhetsåtgärd

Driftrutiner bör dokumenteras 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**

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

12.1.2 Ändringshantering

Säkerhetsåtgärd

Förändringar i organisation, verksamhetsprocesser eller informationsbehandlingsresurser och system som påverkar informationssäkerheten 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**

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

12.1.3 Kapacitetshantering

Säkerhetsåtgärd

	Nivå

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

12.1.4 Separation av utvecklings-, test- och driftmiljöer

Säkerhetsåtgärd

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

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

12.2 Skydd mot skadlig kod

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

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

12.2.1 Säkerhetsåtgärder mot skadlig kod

Säkerhetsåtgärd

	Nivå

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

12.3 Säkerhetskopiering

Mål: Att skydda mot förlust av data	**Nivå**

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

12.3.1 Säkerhetskopiering av information

Säkerhetsåtgärd

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

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

12.4 Loggning och övervakning

Mål: Att logga händelser och skapa bevis	**Nivå**

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

12.4.1 Loggning av händelser

Säkerhetsåtgärd

Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser bör skapas, bevaras och granskas regelbundet. *Kritisk säkerhetsåtgärd: Ja* *Risk: Bristfällig hantering av revisionsloggar gör det svårare att identifiera och utreda säkerhetsincidenter.*	**Nivå**

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

12.4.2 Skydd av logginformation

Säkerhetsåtgärd

Loggningsverktyg och logginformation bör skyddas mot manipulation och obehörig åtkomst. *Kritisk säkerhetsåtgärd: Ja* *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**

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

12.4.3 Administratörs- och operatörsloggar

Säkerhetsåtgärd

Systemadministratörers och systemoperatörers aktiviteter bör loggas och loggarna bör skyddas och granskas regelbundet. *Kritisk säkerhetsåtgärd: Ja* *Risk: Bristfällig loggning av aktiviteter gör det svårare att identifiera och utreda säkerhetshändelser.*	**Nivå**

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

12.4.4 Synkronisering av tid

Säkerhetsåtgärd

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller säkerhetsdomän bör synkroniseras mot en och samma referenskälla för tid. *Kritisk säkerhetsåtgärd: Ja* *Risk: Felaktiga tidstämplar gör det svårare att utreda säkerhetshändelser och att säkerställa spårbarheten.*	**Nivå**

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

12.5 Styrning av driftsystem

Mål: Att säkerställa riktigheten hos driftsystem.	**Nivå**

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

12.5.1 Installation av program på driftsystem

Säkerhetsåtgärd

Rutiner bör införas för att styra installation av program på driftsystem. *Kritisk säkerhetsåtgärd: Nej* *Risk: En angripare kan få möjlighet att installera program som verksamheten inte känner till.*	**Nivå**

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

12.6 Hantering av tekniska sårbarheter

Mål: Att förhindra utnyttjande av tekniska sårbarheter	**Nivå målområdet**

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

12.6.1 Hantering av tekniska sårbarheter

Säkerhetsåtgärd

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

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

12.6.2 Restriktioner för installation av program

Säkerhetsåtgärd

Regler för programinstallationer som utförs av användare bör upprättas och införas. *Kritisk säkerhetsåtgärd: Ja* *Risk: Om det inte finns regler för programinstallationer finns det en risk för att man får in programvara som kan komprommettera systemmiljön.*	**Nivå**

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

12.7 Överväganden gällande revision av informationssystem

Mål: Att minimera revisionsverksamhetens påverkan på driftsystem	**Nivå målområdet**

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

12.7.1 Revisionskontroller för informationssystem

Säkerhetsåtgärd

	Nivå

Revisionskrav och revisionsaktiviteter som omfattar verifiering av status på driftsystem bör planeras noggrant och godkännas för att minimera 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)

13 Kommunikationssäkerhet

Här beskrivs nivån totalt för detta kapitel.	**Nivå för området**

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

13.1 Hantering av nätverkssäkerhet

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

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

13.1.1 Säkerhetsåtgärder för nätverk

Säkerhetsåtgärd

Nätverk bör hanteras och styras för att skydda information i system och tillämpningar. *Kritisk säkerhetsåtgärd: Nej* *Risk: Att det ansluts utrustning som kan påverka säkerheten i systemmiljön.*	**Nivå**

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

13.1.2 Säkerhet hos nätverkstjänster

Säkerhetsåtgärd

Säkerhetsmekanismer, tjänstenivåer och ledningskrav vad gäller alla nätverkstjänster bör identifieras och inkluderas i avtal för nätverkstjänster, oavsett om dessa tjänster tillhandahålls internt eller som outsourcade tjänster. *Kritisk säkerhetsåtgärd: Nej* *Risk: Bristfällig hantering av nätverkssäkerhet kan leda till försämrad tillgänglighet, obehörig åtkomst eller avlysning av information.*	**Nivå**

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

13.1.3 Separation av nätverk

Säkerhetsåtgärd

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

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

13.2 Informationsöverföring

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

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

13.2.1 Regler och rutiner för informationsöverföring

Säkerhetsåtgärd

	Nivå

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

13.2.2 Överenskommelser om informationsöverföring

Säkerhetsåtgärd

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

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

13.2.3 Elektronisk meddelandehantering

Säkerhetsåtgärd

Information som hanteras genom elektronisk meddelandehantering bör ha tillräckligt skydd. *Kritisk säkerhetsåtgärd: Nej* *Risk: Utan tillräckligt skydd av elektroniskt meddelande finns det en risk att meddelandet förlorar konfidentialitet, tillgänglighet eller riktighet.*	**Nivå**

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

13.2.4 Konfidentialitet och förbindelser om konfidentialitet

Säkerhetsåtgärd

	Nivå

Krav på konfidentialitet eller förbindelser rörande konfidentialitet som återspeglar organisationens behov av skydd av information bör identifieras, regelbundet granskas och dokumenteras. *Kritisk säkerhetsåtgärd: Ja* *Risk: Medarbetare och partners kan avslöja information som de inte vara medvetna om hade ett skyddsvärde.*	

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

14 Anskaffning, utveckling och underhåll av system

	Nivå
Här beskrivs nivån totalt för detta kapitel.	

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

14.1 Säkerhetskrav på informationssystem

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

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

14.1.1 Analys och specifikation av informationssäkerhetskrav

Säkerhetsåtgärd

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

14.1.2 Säkerställande av programtjänster på publika nätverk

Säkerhetsåtgärd

Information i programtjänster på publika nätverk bör skyddas från bedräglig aktivitet, avtalstvist och obehörigt röjande och modifiering. *Kritisk säkerhetsåtgärd: Ja* *Risk: Det görs anslutningar som skapar en risknivå på verksamheten som kan leda till intrång och överbelastningsattacker.*	**Nivå**

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

14.1.3 Skydd av transaktioner i tillämpningstjänster

Säkerhetsåtgärd

Information hanterad som del i programtjänsters transaktioner bör skyddas för att förhindra ofullständig överföring, felaktig styrning av nätverkstrafik, obehörig ändring av meddelanden, obehörigt röjande, obehörig duplicering av meddelanden eller återuppspelning. *Kritisk säkerhetsåtgärd: Ja* *Risk: Information under kommunikation kan drabbas av ofullständig överföring, felaktig styrning av nätverkstrafik, obehörig ändring av meddelanden, obehörigt röjande, obehörig duplicering av meddelanden eller återuppspelning m.m..*	**Nivå**

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

14.2 Säkerhet i utvecklings- och supportprocesser

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

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

14.2.1 Regler för säker utveckling

Säkerhetsåtgärd

Regler för utveckling av program och system bör upprättas och tillämpas vid systemutveckling inom organisationen. *Kritisk säkerhetsåtgärd: Ja* *Risk: Vi skapar system och lösningar som är osäkra och som kostar mycket att rätta till när det görs granskningar av säkerheten innan driftsättning.*	**Nivå**

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

14.2.2 Rutiner för hantering av systemändringar

Säkerhetsåtgärd

Systemförändringar inom utvecklingscykeln bör styras genom användning av formella riktlinjer för ändringshantering. *Kritisk säkerhetsåtgärd: Ja* *Risk: Utan riktlinjer för systemändringar kan säkerheten kompromitteras om det inte görs på rätt sätt.*	**Nivå**

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

14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö

Säkerhetsåtgärd

När driftsmiljön ändras bör verksamhetskritiska tillämpningar granskas och testas för att säkerställa att det inte innebär negativ påverkan på verksamheten eller säkerheten. *Kritisk säkerhetsåtgärd: Ja* *Risk: Om vi inte gör en granskning kan det leda till att vi driftsätter system med stora säkerhetsbrister och som kan påverka hela vår systemmiljö.*	**Nivå**

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

14.2.4 Restriktioner för ändringar av programpaket

Säkerhetsåtgärd

	Nivå

Ändringar av programpaket bör förhindras eller begränsas till nödvändiga ändringar och alla ändringar bör styras noggrant. *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)

14.2.5 Principer för utveckling av säkra system

Säkerhetsåtgärd

	Nivå
Riktlinjer för utveckling av säkra system bör upprättas, dokumenteras, underhållas och tillämpas vid alla införanden av informationssystem. *Kritisk säkerhetsåtgärd: Ja* *Risk: Vi bygger inte in säkerheten från början.*	

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

14.2.6 Säker utvecklingsmiljö

Säkerhetsåtgärd

	Nivå
För systemutvecklings- och integrationsåtgärder bör organisationen upprätta och på lämpligt sätt skydda säkra utvecklingsmiljöer som sträcker sig över systemets hela livscykel. *Kritisk säkerhetsåtgärd: Ja* *Risk: När systemen är i utvecklingsmiljön kan system och data påverkas negativt.*	

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

14.2.7 Outsourcad utveckling

Säkerhetsåtgärd

	Nivå

Organisationen bör övervaka och styra outsourcad systemutveckling. *Kritisk säkerhetsåtgärd: Ja* *Risk: Om man inte övervakar och styr outsourcad systemutveckling kan det byggas in brister i system och verksamhetens information inte hanteras lagenligt.*	

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

14.2.8 Säkerhetstestning

Säkerhetsåtgärd

Säkerhetsfunktionalitet bör testas vid utveckling. *Kritisk säkerhetsåtgärd: Ja* *Risk: Testas inte säkerhetsfunktioner vid utvecklingen så kan det medföra att säkerhetsbrister byggs in eller att kravställda funktioner inte utvecklats.*	**Nivå**

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

14.2.9 Acceptanstestning av system

Säkerhetsåtgärd

Program för acceptanstester och relaterade kriterier bör fastställas för nya informationssystem, uppgraderingar och nya versioner. *Kritisk säkerhetsåtgärd: Ja* *Risk: Är inte program för acceptanstester kan det med föra att systemet får sårbarheter, och säkerhetsrelaterade fel.*	**Nivå**

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

14.3 Testdata

Mål: Att säkerställa skyddet av data som används för tester	**Nivå**

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

14.3.1 Skydd av testdata

Säkerhetsåtgärd

Testdata bör noggrant väljas ut, 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**

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

15 Leverantörsrelationer

Här beskrivs nivån totalt för detta kapitel.	**Nivå**

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

15.1 Informationssäkerhet i leverantörsrelationer

Mål: Att säkerställa skydd av de av organisationens tillgångar som leverantörer har åtkomst till.	**Nivå**

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

15.1.1 Informationssäkerhetsregler för leverantörsrelationer

Säkerhetsåtgärd

Informationssäkerhetskrav för att reducera riskerna förknippade med leverantörers åtkomst till organisationens tillgångar bör avtalas med leverantören och dokumenteras. *Kritisk säkerhetsåtgärd: Ja* *Risk: Verksamheten har inte kontroll över leverantörens åtkomst till tillgångar vilket kan medföra att de får större åtkomst än vad som behövs.*	**Nivå**

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

15.1.2 Hantering av säkerhet inom leverantörsavtal

Säkerhetsåtgärd

Alla relevanta informationssäkerhetskrav bör upprättas och avtalas med varje leverantör som kan tillgå, behandla, lagra, kommunicera eller som tillhandahåller infrastrukturkomponenter för organisationens information. *Kritisk säkerhetsåtgärd: Ja* *Risk: Verksamhetens information och tillgångar har inte den säkerhetsnivå som behövs.*	**Nivå**

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

15.1.3 Försörjningskedja för informations- och kommunikationsteknologi

Säkerhetsåtgärd

Avtal med leverantörer bör innehålla krav på att hantera informationssäkerhetsriskerna förknippade med försörjningskedjan för tjänster och produkter baserade på informations- och kommunikationsteknologi. *Kritisk säkerhetsåtgärd: Nej* *Risk: Verksamheten har inte kontroll på hela försörjningskedjan vilket är särskilt viktigt när man får en säkerhetsincident.*	**Nivå**

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

Försörjningskedjan för informations- och kommunikationsteknik som behandlas här omfattar molntjänster.

15.2 Hantering av leverantörers tjänsteleverans

Mål: Att upprätthålla en överenskommen nivå av informationssäkerhet och tjänsteleverans i linje med leverantörsavtal	**Nivå**

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

15.2.1 Övervakning och granskning av leverantörstjänster

Säkerhetsåtgärd

Organisationer bör regelbundet övervaka, granska och revidera leverantörers tjänsteleverans. *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**

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

15.2.2 Ändringshantering av leverantörers tjänster

Säkerhetsåtgärd

Ändringar av tillhandahållande av tjänster från leverantörer, inklusive underhåll och förbättring av befintlig informationssäkerhetspolicy med tillhörande regelverk och befintliga rutiner bör hanteras, med beaktande av informationens, systemens och processernas kritiska betydelse för verksamheten och riskerna ska omvärderas. *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**

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

16 Hantering av informationssäkerhetsincidenter

Här beskrivs nivån totalt för detta kapitel.	**Nivå**

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

16.1 Hantering av informationssäkerhetsincidenter och förbättringar

Mål: Att säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation kring säkerhetshändelser och svagheter	**Nivå**

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

16.1.1 Ansvar och rutiner

Säkerhetsåtgärd

Ledningsansvar och rutiner bör fastställas för att säkerställa snabb, verkningsfull och korrekt hantering av 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**

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

16.1.2 Rapportering av informationssäkerhetshändelser

Säkerhetsåtgärd

Informationssäkerhetshändelser bör rapporteras genom lämpliga rapporteringsvägar så snabbt 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**

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

16.1.3 Rapportering av svagheter gällande informationssäkerhet

Säkerhetsåtgärd

	Nivå

Anställda och leverantörer som använder organisationens informationssystem och -tjänster bör vara skyldiga att notera och rapportera alla observerade eller misstänkta svagheter gällande informationssäkerhet i system eller tjänster. *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)

16.1.4 Bedömning av och beslut om informationssäkerhetshändelser

Säkerhetsåtgärd

Informationssäkerhetshändelser bör bedömas och beslut bör fattas om de klassificeras som informationssäkerhetsincidenter. *Kritisk säkerhetsåtgärd: Ja* *Risk: Informationssäkerhetshändelsen hanteras inte på rätt sätt och man vidtar inte rätt åtgärder för att samma händelse inte inträffar igen.*	**Nivå**

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

16.1.5 Hantering av informationssäkerhetsincidenter

Säkerhetsåtgärd

Informationssäkerhetsincidenter bör hanteras i enlighet med dokumenterade rutiner. *Kritisk säkerhetsåtgärd: Ja* *Risk: Har man inte rutiner så kan det leda till risker som felaktig hantering, tiden för hantering blir lång och man gör inte rätt åtgärder.*	**Nivå**

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

16.1.6 Att lära av informationssäkerhetsincidenter

Säkerhetsåtgärd

	Nivå

Kunskaper baserade på analyser av hanterade informationssäkerhetsincidenter bör användas för att minska sannolikheten eller påverkan av framtida incidenter. *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)

16.1.7 Insamling av bevis

Säkerhetsåtgärd

Organisationen bör fastställa och tillämpa rutiner för identifiering, insamling, kopiering och bevarande av information som kan tjäna som bevis. *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**

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

17 Informationssäkerhets-aspekter avseende hantering av verksamhetens kontinuitet

Här beskrivs nivån totalt för detta kapitel.	**Nivå**

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

17.1 Kontinuitet för informationssäkerhet

Mål: Kontinuiteten för informationssäkerhet bör vara integrerad i organisationens ledningssystem för kontinuitetshantering	**Nivå**

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

17.1.1 Planering av kontinuitet för informationssäkerhet

Säkerhetsåtgärd

Organisationen bör fastställa sina krav på informationssäkerhet och kontinuitet för styrning av informationssäkerhet vid svåra situationer, exempelvis under en kris eller katastrof. *Kritisk säkerhetsåtgärd: Ja* *Risk: Verksamheten har inte den kontinuitetsförmåga den bör av sina säkerhetsåtgärder vilket kan leda till att information kan förloras, avslöjas eller att det tar lång tid att komma tillbaks till normalläge.*	**Nivå**

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

17.1.2 Införa kontinuitet för informationssäkerhet

Säkerhetsåtgärd

Organisationen bör fastställa, dokumentera, införa och upprätthålla processer, rutiner och säkerhetsåtgärder för att säkerställa den nivå av kontinuitet för informationssäkerhet som krävs vid en svår situation. *Kritisk säkerhetsåtgärd: Ja* *Risk: Säkerhetsnivån kan vara för låg eller hög vid kontinuitetsläget.*	**Nivå**

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

17.1.3 Styra, granska och utvärdera kontinuitet för informationssäkerhet

Säkerhetsåtgärd

Organisationen bör verifiera de fastställda och införda säkerhetsåtgärderna för kontinuitet för informationssäkerhet med jämna mellanrum för att säkerställa att de är giltiga och verkningsfulla under störningar. *Kritisk säkerhetsåtgärd: Ja* *Risk: Görs inte detta kan det leda till att informationssäkerheten inte har den förmåga som är planerad vid en större händelse.*	**Nivå**

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

17.2 Redundans

	Nivå

Mål: Att säkerställa tillgänglighet till informationsbehandlingsresurser	

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

17.2.1 Tillgänglighet för informationsbehandlingsresurser

Säkerhetsåtgärd

Informationsbehandlingsresurser bör vid införande ha tillräcklig redundans för att uppfylla krav på tillgänglighet. *Kritisk säkerhetsåtgärd: Ja* *Risk: Finns inte tillräcklig redundans kan det leda till avbrott som blir långa.*	**Nivå**

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

18 Efterlevnad

Här beskrivs nivån totalt för detta kapitel.	**Nivå**

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

18.1 Efterlevnad av juridiska och avtalsmässiga krav

Mål: Att undvika överträdelser av författningsenliga eller avtalsmässiga skyldigheter relaterade till informationssäkerhet och av eventuella säkerhetskrav.	**Nivå**

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

18.1.1 Identifiering av gällande lagstiftning och avtalsmässiga krav

Säkerhetsåtgärd

	Nivå

Alla relevanta författningsenliga och avtalsmässiga krav samt organisationens tillvägagångssätt för att uppfylla dessa krav bör uttryckligen identifieras, dokumenteras och hållas uppdaterade för varje informationssystem och organisationen. *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)

18.1.2 Immateriella rättigheter

Säkerhetsåtgärd

Lämpliga rutiner bör införas för att säkerställa efterlevnad av författningsenliga och avtalsmässiga krav relaterade till immateriella rättigheter och användning av proprietär programprodukter. *Kritisk säkerhetsåtgärd: Nej* *Risk: Brott mot immaterialrätten kan leda till rättsliga och ekonomiska påföljder. Dessutom kan förtroendet för organisationen ta skada.*	**Nivå**

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

18.1.3 Skydd av dokumenterad information

Säkerhetsåtgärd

Dokumenterad information bör skyddas från förlust, förstörelse, förfalskning, obehörig åtkomst och otillåten utgivning i enlighet med författningsenliga, avtalsmässiga och verksamhetsmässiga krav. *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**

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

18.1.4 Skydd av personlig integritet och personuppgifter

Säkerhetsåtgärd

	Nivå

I förekommande fall bör skydd av personlig integritet och personuppgifter säkerställas i enlighet med gällande författningar. *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)

18.1.5 Reglering av kryptografiska säkerhetsåtgärder

Säkerhetsåtgärd

Kryptografiska säkerhetsåtgärder bör användas i enlighet med alla gällande 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**

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

18.2 Granskningar av informationssäkerhet

Mål: Att säkerställa att informationssäkerhet införs och drivs i enlighet med organisationens regler och rutiner	**Nivå**

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

18.2.1 Oberoende granskning av informationssäkerhet

Säkerhetsåtgärd

Organisationens tillvägagångssätt för att hantera informationssäkerhet och dess införande (d.v.s. mål, säkerhetsåtgärder, regler, processer och rutiner för informationssäkerhet) bör med jämna mellanrum eller när betydande förändringar sker genomgå oberoende granskning. *Kritisk säkerhetsåtgärd: Ja* *Risk: Genomförs inte oberoende granskningar vet verksamheten inte om den har rätt säkerhet.*	**Nivå**

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

18.2.2 Efterlevnad av säkerhetspolicy, regler och standarder

Säkerhetsåtgärd

Högsta ledningen bör inom gällande ansvarsområden regelbundet granska efterlevnaden av informationssäkerhetspolicyn, gällande regler och riktlinjer, standarder och eventuella andra säkerhetskrav i förhållande till informationsbearbetning och rutiner. *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**

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

18.2.3 Granskning av teknisk efterlevnad

Säkerhetsåtgärd

Informationssystem bör granskas regelbundet avseende efterlevnad av organisationens informationssäkerhetspolicy, regler, riktlinjer och standarder. *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**

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