TRANSPORT STYRELSEN

TSG 2022-12011

Vägledning

till Transportstyrelsens föreskrifter och allmänna råd (TSFS 2022:14) om säkerhetsåtgärder för samhällsviktiga leverantörer inom transportsektorn

TRANSPORT STYRELSEN

Vägledning

Datum
2023-03-21

Version
1.0

Dnr/Beteckning
TSG 2022-12011

Upprättad av
Sektionen för säkerhetsskydd
Infrastrukturenheten
Sjö- och luftfart

Versionshistorik

Version	Datum	Beskrivning	Ansvarig
1.0	2023-03-21	Fastställande av vägledning	Andreas Holmgren

TRANSPORT STYRELSEN

Vägledning

Datum
2023-03-21

Version
1.0

Dnr/Beteckning
TSG 2022-12011

Upprättad av
Sektionen för säkerhetsskydd
Infrastrukturenheten
Sjö- och luftfart

Innehåll

Upprättad av
Sektionen för säkerhetsskydd
Infrastrukturenheten
Sjö- och luftfart

1 Inledning

Ökade hot och det skärpta säkerhetsläget i Europa har de senaste åren medfört att nya säkerhetskrav ställts på flera olika samhällssektorer. För verksamheter som levererar samhällsviktiga tjänster gäller NIS-lagen och NIS-förordningen sedan den 1 augusti 2018. Lagen innebär bland annat att verksamheter ska arbeta systematiskt och riskbaserat med informationssäkerhet och rapportera incidenter. Den som inom ramen för NIS-regleringen identifierat sig som en leverantör av en samhällsviktig tjänst, ska anmäla det till berörd tillsynsmyndighet. Transportstyrelsen är tillsynsmyndighet inom sektorn transport.

Myndigheten för samhällsskydd och beredskap, MSB, samordnar det nationella arbetet och utgör också kontaktpunkt gentemot andra EU-medlemsstater. Det innebär bland annat att de tar fram övergripande föreskrifter för alla sektorer som omfattas av NIS-lagen.[1]

Transportstyrelsen har utifrån NIS-lagen och NIS-förordningen tagit fram föreskrifter om säkerhetsåtgärder för transportsektorn.

1.1 Syfte och målgrupp

Syftet med denna vägledning är att stötta de organisationer och företag inom transportsektorn som omfattas av NIS-regleringen i hur de ska uppfylla kraven i Transportstyrelsens föreskrifter om säkerhetsåtgärder. Vägledningen är avsedd att användas av alla verksamheter inom transportsektorn som är leverantörer av samhällsviktiga tjänster enligt MSB:s föreskrifter (MSBFS 2021:9) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

Vägledningen är utformad för att passa alla fyra transportslagen; lufttransport, järnvägstransport, sjöfart och vägtransport. Den kan användas av berörda verksamheter för att påbörja eller vidareutveckla sitt informationssäkerhetsarbete.

[1] MSB:s föreskrifter och allmänna råd (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSB:s föreskrifter och allmänna råd (MSBFS 2018:9) om rapportering av incidenter för leverantörer av samhällsviktiga tjänster och MSB:s föreskrifter (MSBFS 2021:9) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

Vägledningen kan vara till nytta för exempelvis verksamhetens beslutsfattare, säkerhetsansvariga, IT-ansvariga, internrevisorer och andra som arbetar med utveckling, drift och förvaltning av verksamhetens säkerhetsåtgärder.

1.2 Avgränsning

Denna vägledning avgränsas till kraven i Transportstyrelsens föreskrifter om säkerhetsåtgärder med tillhörande allmänna råd för några av säkerhetsåtgärderna. För ytterligare stöd hänvisas till MSB:s föreskrifter om informationssäkerhet samt MSB:s vägledning för säkerhetsåtgärder i informationssystem.[2]

1.3 Läsanvisning

Vägledningen

- förklarar varför åtgärderna som beskrivs är viktiga
- hänvisar till ytterligare vägledning för att underlätta arbetet
- ger förslag på hur föreskrifterna kan omsättas i praktiskt handlande.

Beslutet om hur föreskriftens säkerhetsåtgärder ska genomföras i verksamheten för att uppfylla kraven i föreskriften avgörs utifrån leverantörens egen analys. Leverantörens sätt att införa säkerhetsåtgärderna blir sedan föremål för Transportstyrelsens påföljande tillsyn.

För varje säkerhetsåtgärd i de följande kapitlen beskrivs följande:

- Kravet från Transportstyrelsens föreskrifter om säkerhetsåtgärder.
- Allmänna råd (för vissa säkerhetsåtgärder).
- Syftet med kravet.
- Vad säkerhetsåtgärden minst bör omfatta, t.ex. riskanalysens olika steg och slutresultat.
- Hänvisning till liknande krav på säkerhetsåtgärder i andra standarder och regelverk (referenser finns sist i vägledningen).

[2] Vägledning: https://rib.msb.se/filer/pdf/30128.pdf

Där vägledningen anger ”ska-krav” har detta direkt stöd i författningstexten. Vägledningen, som ytterligare preciserar författningstexten, innehåller rekommendationer och dessa uttrycks i huvudsak genom ”bör-krav” eller liknande.

1.4 Förkortade benämningar på regelverk

Följande förkortade benämningar används i vägledningen:

Förkortning	Fullständig titel
NIS-regleringen	NIS-direktivet, NIS-lagen och NIS-förordningen samt föreskrifter som har meddelats med stöd av dessa.
NIS-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
NIS-lagen	Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
NIS-förordningen	Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
MSB:s föreskrifter om informationssäkerhet	Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.
Transportstyrelsens föreskrifter om säkerhetsåtgärder	Transportstyrelsens föreskrifter och allmänna råd (2022:14) om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn.

För andra informationssäkerhetsbegrepp som förekommer i vägledningen hänvisar vi till definitioner i NIS-lagen, NIS-förordningen, MSB:s föreskrifter om informationssäkerhet och Transportstyrelsens föreskrifter om säkerhetsåtgärder samt MSB:s termbank för informationssäkerhet.

2 Förslag på arbetssätt

I detta kapitel beskriver vi några grundläggande principer för ett framgångsrikt införande av NIS-direktivet och ger förslag på hur arbetet kan läggas upp.

2.1 Utnyttja och bygg vidare på befintliga säkerhetsåtgärder

Vägledningen är utformad för att ge stöd till verksamheter i arbetet med att utveckla sitt arbete med att implementera säkerhetsåtgärderna enligt Transportstyrelsens föreskrifter om säkerhetsåtgärder. Det är inte tanken att dessa säkerhetsåtgärder ska ersätta annat säkerhetsarbete eller redan införda åtgärder inom organisationen. Istället ska säkerhetsåtgärderna i föreskriften ses som ett komplement och en vidareutveckling av de säkerhetsåtgärder som redan finns etablerade hos organisationen. En viktig del av denna vägledning blir därför att kartlägga vad som redan finns på plats och utöka dessa befintliga säkerhetsåtgärder i syfte att förbättra säkerhetsnivån så att NIS-regleringens krav uppfylls.

2.2 Integrera med övriga verksamhetsledningssystem

Det är vanligt att organisationer redan har etablerade och kanske även certifierade verksamhetsledningssystem för exempelvis kvalitet, miljö eller informationssäkerhet. I dessa fall är det viktigt att arbetet med säkerhetsåtgärder enligt Transportstyrelsens föreskrifter om säkerhetsåtgärder inte blir en parallell verksamhet. Istället bör arbetet integreras i största möjligaste mån med samma processer och kriterier för exempelvis riskhantering, incidenter, åtkomststyrning, internrevision och uppföljning.

2.3 Ett systematiskt och riskbaserat arbetssätt är inte statiskt

Omvärlden förändras ständigt. Därför kännetecknas ett systematiskt och riskbaserat arbetssätt av ett kontinuerligt förbättringsarbete baserat på hur verksamheten utvecklas och omvärlden förändras. Ett förhållningssätt där man i verksamheten tänker sig att ”bli klar” med att införa säkerhetsåtgärder, för att därefter fokusera på annat, kommer snabbt att innebära att organisationens säkerhetsåtgärder blir föråldrade och att risknivån ökar. Se därför till att säkerhetsarbetet präglas av ständiga förbättringar och prioriteringar utifrån den rådande risknivån. Systematiskt informationssäkerhetsarbete är att arbeta förebyggande och att kontinuerligt anpassa skyddet utifrån organisationens behov och risker.

2.4 Överlappningar mellan NIS-regleringen och säkerhetsskyddslagen

För att bedöma huruvida verksamheten omfattas av NIS-regleringen eller säkerhetsskyddslagen (2018:585), eller både och, är det viktigt att börja med

att göra en verksamhetsanalys, identifiera information som används och att de informationstillgångar som identifierats i den förteckning som beskrivs närmare i avsnitt 3.2 är informationsklassade. NIS-regleringen och säkerhetsskyddslagen överlappar många gånger varandra, och för att kunna avgöra vilka regler som ska tillämpas behöver man göra en noggrann inledande analys för att identifiera vilka delar som tillhör säkerhetsskyddet och vilka som tillhör NIS.

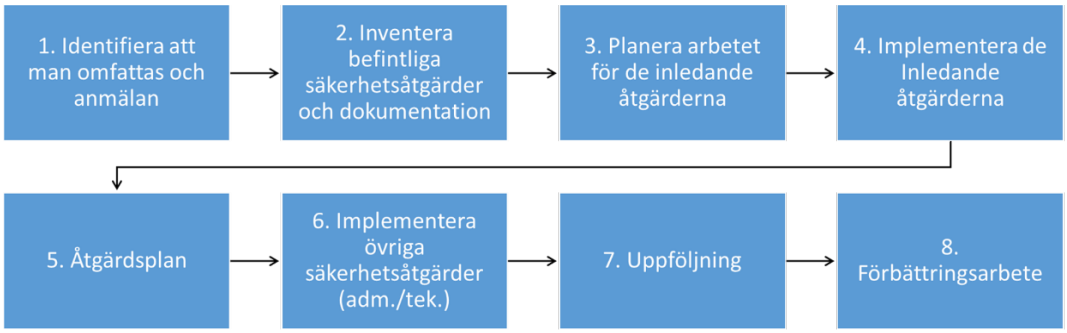
NIS-regleringen omfattar specifikt nätverk och informationssystem medan säkerhetsskyddslagen kan beröra dessa och andra delar av verksamheten. Säkerhetsskyddslagen har företräde framför NIS-regleringen, men det kan vara så att verksamheten omfattas av båda lagstiftningarna beroende på den information som hanteras.

2.5 Förslag på arbetssätt

Det arbetssätt vi beskriver i detta avsnitt är ett förslag på hur arbetet kan läggas upp inledningsvis och i vilken ordning de olika säkerhetskraven kan genomföras. Arbetssättet som föreslås för det inledande arbetet påverkar i hög grad hur de resterande säkerhetsåtgärderna införs. Beroende på förutsättningarna i organisationen kan naturligtvis andra upplägg också fungera bra.

Arbetssättet är indelat i två block. Det första blocket (1-5) innehåller aktiviteter för att genomföra inventering, förteckning och riskanalys som leder fram till en första version av åtgärdsplan. Det andra blocket (6-8) innehåller aktiviteter för att införa resterande administrativa och tekniska säkerhetsåtgärder i föreskriften samt etablering av ett kontinuerligt arbetssätt med ständiga förbättringar.

Grafiskt kan arbetssättet beskrivas så här:



Kort förtydligande av upplägget:

1. Verksamheten börjar med att analysera huruvida man omfattas av NIS-lagen. Om verksamheten omfattas, anmäler man detta till Transportstyrelsen.
2. Verksamheten inventerar de säkerhetsåtgärder och den dokumentation som redan finns i organisationen. Vi rekommenderar att man gör en gap-analys för att jämföra införda säkerhetsåtgärder med de säkerhetsåtgärder som NIS-regleringen ställer krav på.
3. En plan tas fram för att styra det inledande arbetet. Vad ska göras först? Vem ansvarar? Är man beroende av annan verksamhet?
4. Påbörja arbetet med de inledande åtgärderna enligt kapitel 3 i denna vägledning. Det gäller inventering, förteckning, omvärldsbevakning, riskanalys, åtgärdsplanering och uppföljning.
5. Baserat på det inledande arbetet vidareutevecklar man sedan, utifrån risknivå och prioritet, befintlig åtgärdsplan med de säkerhetsåtgärder som inte identifierats i den inledande riskanalysen.
6. Inför övriga administrativa och tekniska säkerhetsåtgärder utifrån åtgärdsplanen i punkt 5.
7. Verksamheten följer upp och kontrollerar hur arbetet med de olika säkerhetsåtgärderna fortskrider.
8. Verksamheten fortsätter att utveckla säkerhetsåtgärderna inom sitt ordinarie förbättringsarbete.

3 Inledande säkerhetsåtgärder

I det här kapitlet beskriver vi de säkerhetsåtgärder som kan vara bra att starta med. Säkerhetsåtgärderna innefattar inventering av berörda nätverk och informationssystem, riskbedömning med prioritering och en första åtgärdsplan för att styra arbetet.

3.1 Inventering

6 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för inventering av nätverk och informationssystem, i syfte att identifiera vilka nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Syftet med kravet är att organisationen ska etablera ett systematiskt sätt att kartlägga IT-miljön så att det är möjligt att identifiera vilka informationstillgångar och nätverk som omfattas av NIS-regleringen och vilka som inte gör det.

För att kunna etablera ett systematiskt arbetssätt för att införa säkerhetsåtgärder, förvalta dem, följa upp dem och utvärdera om de är tillräckliga, är det viktigt att det finns tillräcklig dokumentation om nätverk och informationssystem. Dokumentationen kan exempelvis utgöras av systemskisser med logisk och fysisk placering av utrustning, arkitekturbeskrivningar och dataflödesdiagram med logiska samband och nätverksmässiga sammankopplingar mellan komponenter och delsystem.

Inventeringen bör även tydliggöra eventuella beroenden mellan olika informationssystem. Det kan vara olika interna system som är beroende av varandra, men också interna system som är beroende av informationssystem hos externa aktörer. Gränsytor kan leda till ökade sårbarheter då de bidrar till fler möjliga exponeringar och attackytor.

3.2 Förteckning av informationstillgångar

7 § Leverantören ska utifrån den inventering som genomförts enligt 6 § upprätta förteckning över informationstillgångar. Förteckningen ska innehålla de informationstillgångar som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Förteckningen ska hållas uppdaterad.

Allmänna råd:

Exempel på informationstillgångar är
1. information (data, dokument etc.),
2. program (applikationer, operativsystem etc.),
3. tjänster (kommunikationstjänster, abonnemang etc.),
4. fysiska tillgångar (datorer, datamedier, lokaler, lokala nätverk etc.), och
5. befattningar, roller och funktioner.

Syftet med att upprätta och underhålla en förteckning av informationstillgångar är att alltid ha kontroll över vilka tillgångar som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Alla informationstillgångar som är nödvändiga för tjänsten ska förtecknas, inte bara informationssystem eller nätverkskomponenter. Det är bra om det för varje informationstillgång finns information om syfte, vad för typ av information som behandlas och informationsklassning, vem som är ansvarig, ingående hård- och mjukvara, beroenden till andra system, vilka som har behörighet och informationstillgångens prioritet för verksamheten. Även eventuella externa tjänster, till exempel molntjänster, bör ingå i förteckningen.

Av MSB:s föreskrifter om informationssäkerhet framgår struktur och arbetssätt för informationsklassning.

Kom ihåg att även identifiera eventuella system som används för att styra och övervaka fysiska processer och system i realtid, så kallade industriella styrsystem (exempelvis system för att lägga om växlarna på järnvägsrälsen) som kan ingå i den samhällsviktiga tjänsten.[3] Detta eftersom denna typ av system ofta är sårbara och svårare att skydda.

Förteckningen över informationstillgångar bör ses över regelbundet, minst årligen.

3.3 Omvärldsbevakning

8 § Leverantören ska bedriva omvärldsbevakning för att identifiera hot mot och sårbarheter i de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Syftet med att systematiskt arbeta med omvärldsbevakning är

- att bevaka den tekniska utvecklingen för att uppmärksamma sårbarheter för berörda informationssystem och för att identifiera förbättrade eller nya säkerhetsfunktioner som är lämpliga för verksamheten

[3] Se även MSB:s Vägledning till ökad säkerhet i industriella informations- och styrsystem https://rib.msb.se/filer/pdf/29984.pdf.

- att följa förändringar i hotbild och andra aspekter som berör transportsektorn, exempelvis incidenter som har inträffat eller förändrade regelverk.

Som utgångspunkt för omvärldsbevakningen finns en rad nationella och internationella hotbedömningar som görs av svenska och europeiska myndigheter, till exempel MSB (CERT-SE[4]), Säkerhetspolisen, Försvarets radioanstalt (FRA), Militära underrättelse- och säkerhetstjänsten (MUST), NIST[5] och ENISA[6]. Verksamheten bör utan onödigt dröjsmål hantera information som skickas ut av nationella myndigheter om incidenter, sårbarheter, hot och relevanta kartläggningar.

Omvärldsbevakningen bör ske löpande och vara en integrerad del av verksamheten.

Exempel på områden att bevaka:

- Säkerhetspolitiska hot mot samhällsviktiga tjänster i Sverige.

- Allmänna trender kring IT-lösningar och IT-säkerhet.

- Tekniska sårbarheter i hårdvara och mjukvara som används för verksamhetens samhällsviktiga tjänster, t.ex.sårbarhet för skadlig kod, hur skadlig kod utvecklas och sprids, vilka konsekvenser den får och vilka informationssystem som utsätts.

- Allmänt använda tekniska intrångsmönster och icke-tekniska angreppsmetoder för hotaktörer.

- Större IT-incidenter.

Omvärldsbevakningen bör fokusera på transportsektorns förutsättningar. Beroende på undersektor (lufttransport, järnvägstransport, sjöfart eller vägtransport) kan vissa risker kräva mer eller mindre analys. Vilken information som är relevant beror även på vilka informationssystem som verksamheten använder och hur sårbara dessa är.

Omvärldsbevakningens analyser och slutsatser bör ligga till grund för beslut om aktuell risknivå och prioriteringar av säkerhetsåtgärder för den samhällsviktiga tjänsten. Dels kan omvärldsbevakningen identifiera åtgärder

[4] Sveriges nationella CSIRT (Computer Security Incident Response Team).
[5] National Institute of Standards and Technology (USA).
[6] European Union Agency for Cyber Security.

som behöver genomföras direkt (exempelvis säkerhetsuppdateringar) och dels säkerhetsåtgärder som behöver hanteras mer långsiktigt (exempelvis att support kommer att upphöra för äldre versioner av en programvara).

3.4 Riskanalys

9 § Av 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantören ska genomföra en riskanalys. I riskanalysen ska leverantören beakta den förteckning av informationstillgångar som upprättats, resultatet av den omvärldsanalys som genomförts, sårbarheter som identifierats och incidenter som inträffat.

Syftet med riskanalysen är

- att man i en cyklisk process ska identifiera och värdera de hot som riktas mot verksamheten
- att prioritera arbetet med säkerhetsåtgärder så att de risker som har störst påverkan på verksamheten hanteras först.

Riskanalysen ska omfatta samtliga samhällsviktiga nätverk och informationssystem, och med fördel kan en eller flera riskanalyser genomföras per informationssystem för att täcka in fler detaljer. Det kan också vara nödvändigt att upprepa processen flera gånger med olika detaljeringsgrad.

En riskanalys kan genomföras på en mängd olika sätt men bör förslagsvis innehålla följande steg:[7]

1. **Etablering av kontext** – innebär att verksamheten definierar omfattning av analysobjektet (informationstillgången, det samhällsviktiga systemet, nätverket eller verksamheten) med eventuella begränsningar och de inre och yttre ingångsvärden som kan påverka riskbedömningen. Ett exempel på inre ingångsvärde är genomförd informationsklassning och ett exempel på yttre ingångsvärde är krav enligt lag eller föreskrift.

[7] Denna riskhanteringsprocess bygger på ISO31000/ISO27005. Andra exempel på processer finns på www.informationssakerhet.se.

2. **Riskbedömning** – innefattar att man identifierar, kvantifierar och prioriterar risker i förhållande till de ingångsvärden som organisationen satt upp i steg ett.

   Arbetet sker i tre delaktiviter:

   a. Riskidentifiering
   b. Riskuppskattning
   c. Riskvärdering

   Riskidentifiering innebär att identifiera möjliga händelser som kan påverka verksamheten negativt samt hur, var och varför dessa händelser kan uppstå. Både interna och externa sårbarheter och hot bör beskrivas åtminstone inom områdena administrativa, tekniska och fysiska sårbarheter.

   Exempel på tekniska sårbarheter är

   - fel och brister i hårdvara eller mjukvara
   - osäkra fjärrstyrningstjänster och nätverksanslutningar.

   Exempel på administrativa sårbarheter är

   - bristande dokumentation
   - personberoenden och personalbortfall
   - otillräcklig kompetensförsörjning
   - brister i behörighets- och åtkomsthantering.

   Exempel på fysiska sårbarheter är

   - bristfällig tillträdesbegränsning
   - brandskydd och redundans vid strömavbrott (till exempel reservkraft).

   Med fördel kan hotscenarier eller generella hotkataloger användas som utgångspunkt för att identifiera sårbarheter. Man bör även beakta beroenden av underleverantörer (till exempel utkontrakterade informationssystem eller drift- och supporttjänster) och följdeffekter som kan uppkomma i övriga samhället. Ytterligare bra input kan vara från tidigare incidenter och händelser inom organisationen, som man kan dra lärdom från.

Riskuppskattning innebär att varje identifierat hot därefter bedöms utifrån konsekvensen för verksamheten om hotet förverkligas. Skalan för konsekvens kan se ut på många olika sätt, oftast beskrivs den med textuella värden som hög/medel/låg kombinerat med siffervärden, till exempel 1-5.

Konsekvensen kan beskrivas utifrån aspekterna konfidentialitet, riktighet och tillgänglighet för den samhällsviktiga tjänsten. För att kunna bedöma konsekvensens storlek bör det finnas bedömningskriterier för varje nivå av skalan.

För varje hot bedöms även sannolikheten att hotet inträffar. En uppskattning av sannolikhet bör åtminstone baseras på hur frekventa de negativa händelserna är (”inträffar x gånger på y dagar/månader/år”). Ett exempel på en parameter som har betydelse för bedömning av frekvensen är hur enkelt en sårbarhet kan utnyttjas.

Riskvärdering innebär att man kombinerar uppskattade värden för konsekvens och sannolikhet och slutligen får ett riskvärde. Vanligtvis gör man detta genom att multiplicera sannolikhet med konsekvens. Baserat på riskvärdet får man därmed en prioritering som styr nästa steg, riskbehandling.

3. **Riskbehandling –** detta steg innebär att organisationen tar fram en plan för införande av säkerhetsåtgärder för att sänka sannolikheten eller konsekvensen, eller både och.
Ett exempel på riskbehandling som beskrivs nedan och som finns i ISO 31000 utgår från fyra alternativ, där något alternativ måste väljas:

   - *Reducera* innebär att man vidtar eller förbättrar någon säkerhetsåtgärd för att sänka risknivån.
   - *Undvika* innebär att man avstår från eller avbryter en viss aktivitet eftersom risknivån bedöms vara för hög, även om säkerhetsåtgärder skulle införas.
   - Att *dela risktagande* innebär att man involverar en tredje part, exempelvis ett försäkringsbolag, för att få hjälp att hantera risken.

- *Godta* innebär att verksamheten accepterar aktuell risknivå.

4. **Riskacceptans –** När riskbehandlingen är klar är det viktigt att ansvariga i organisationen sätter sig in i och fattar ett beslut om riskhanteringsplanen, kvarstående risker och vem som äger risken i organisationen. Beslutet ska dokumenteras. Om riskvärdena är höga, kan det krävas att högsta ledningen fattar acceptansbeslut.

5. **Löpande kommunikation, övervakning och uppföljning –** När riskhanteringen väl är genomförd behöver man löpande informera relevanta roller, till exempel ledningen och andra intressenter, om aktuell risknivå i förhållande till den nivå ledningen bestämt som acceptabel, om status på planerade och genomförda åtgärder eller om förutsättningarna har förändrats.

   Listan över identifierade risker bör ses över kontinuerligt, minst en gång per år, för att fånga upp till exempel förändringar i hotbilden, förändrad värdering av informationstillgångar, nya eller förändrade sårbarheter, nya underleverantörer eller erfarenheter från eventuella incidenter. Med fördel kan detta planeras samtidigt som ledningens genomgång[8], då ledningen tar ställning till om verksamhetens systematiska informationssäkerhetsarbete inklusive dess styrning är ändamålsenligt, tillräckligt och har avsedd verkan.

3.5 Åtgärdsplan

10 § Av 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att riskanalysen ska innehålla en åtgärdsplan. I åtgärdsplanen ska det minst framgå vilka åtgärder som motverkar vilka risker, vilka nätverk och informationssystem som åtgärderna avser, vilka tidigare åtgärder som genomförts, hur risknivån förväntas förändras och när åtgärderna senast ska vara genomförda.

[8] Från informationssäkerhet.se: ” Med ledningens genomgång avses att ledningen ser över verksamhetens systematiska informationssäkerhetsarbete och dess styrning för att säkerställa dess fortsatta lämplighet, tillräcklighet och verkan.”. Se även kapitlet ”Ledningens genomgång” i ISO 27001.

Syftet med åtgärdsplanen är att hantera de risker som identifierats och prioriterats vid riskanalysen. Åtgärdsplanen ingår därmed i den riskhantering som beskrivs i avsnittet ovan. Det är därför viktigt att åtgärdsplanen har tydliga kopplingar till identifierade risker och även innehåller en bedömning av hur riskvärdet påverkas när åtgärden är införd.

Av åtgärdsplanen ska åtminstone följande framgå:

1. Vilken risk åtgärden behandlar och vilken informationstillgång som berörs.
2. Vilka tidigare åtgärder som genomförts.
3. Hur risknivån förväntas förändras. Detta görs genom en förnyad bedömning av riskvärde om åtgärderna genomförs. Om riskvärdet inte bedöms sjunka tillräckligt kan man behöva se över åtgärderna igen.
4. När åtgärden senast ska vara genomförd.

Det bör även framgå:

5. Vem i verksamheten som är ansvarig för respektive åtgärds införande.
6. Hur åtgärden ska följas upp när den är införd.

3.6 Uppföljning

11 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för uppföljning och analys av vidtagna säkerhetsåtgärders effektivitet.

Syftet med uppföljning är att säkerställa att säkerhetsarbetet för de samhällsviktiga tjänsterna bedrivs systematiskt och med ett riskbaserat arbetssätt präglat av ständiga förbättringar. Ett exempel där det är viktigt med uppföljning är arbetet med de åtgärder som identifierats i verksamhetens riskanalyser enligt tidigare avsnitt (3.4 Riskanalys).

Tillvägagångssätt och metodik för uppföljning ska dokumenteras och genomföras på ett sådant sätt att det är möjligt att utvärdera säkerhetsåtgärdernas effektivitet.

Uppföljningen kan med fördel integreras med övrigt kvalitets- och efterlevnadsarbete inom organisationen. Redan befintliga rutiner för planering, genomförande och uppföljning genom till exempel internrevision kan utvidgas till granskning av informationssäkerheten i de samhällsviktiga

tjänster som tillhandahålls. Ytterligare aktiviteter som kan ingå i uppföljningen är oberoende säkerhetsgranskning, sårbarhetsskanning eller penetrationstest som utförs av tredje part.

4 Administrativa säkerhetsåtgärder

4.1 Driftsgodkännande

12 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för driftsgodkännande av de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Av de dokumenterade reglerna ska det framgå vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning.

Syftet med ett driftsgodkännande (ibland benämnt ackreditering) är

- att verksamheten ska säkerställa att kraven på säkerhetsåtgärder är uppfyllda innan informationssystemet eller nätverket tas i drift
- att säkerhetsåtgärderna ger avsedd effekt
- att ledningen ska känna till eventuella kvarvarande risker, inklusive sårbarheter.

Kravet på driftsgodkännande är därmed ett sätt att tydliggöra ledningens ansvar att informationssystemet eller nätverket uppfyller krav på säkerhet och kontinuitet samt att eventuella brister är kända. Godkännandet bör tillämpas vid såväl nyanskaffning som förändring av de samhällsviktiga nätverken och informationssystemen.

Vid nyanskaffning bör godkännandet innefatta flera avstämningspunkter under införandeprojektets gång så att det är möjligt att justera utformningen av informationssystemet eller nätverket om någon förutsättning förändras. I införandets slutfas bör en oberoende part genomföra någon form av verifiering eller acceptanstest innan informationssystemet eller nätverket tas i drift. Med oberoende part avses en part som inte deltagit i utformningen av systemet, gärna en extern tredje part, såsom en IT-revisor eller ett företag specialiserat på säkerhetsgranskning. Själva driftsgodkännandet bör grundas på dokumenterade kriterier eller krav för att säkerhetsåtgärderna ska bedömas som tillräckliga, detta innefattar tekniska, administrativa och fysiska säkerhetsåtgärder.

4.2 Ändringshantering, uppgradering och uppdatering

13 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för de planerade tekniska eller organisatoriska förändringar som kan påverka de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.
De interna reglerna ska minst innehålla krav på att
1. mjukvara, i de system där det är möjligt, löpande uppdateras till senaste version
2. hård- och mjukvara som inte längre uppdateras eller stöds av leverantören, om möjligt, byts ut eller uppgraderas.

Syftet med ett systematiskt arbetssätt för ändringshantering och uppdateringar är

- att säkerställa att verksamheten håller informationssystem och nätverk uppdaterade med senaste versioner av programvaror
- att man inte gör några odokumenterade förändringar som kan öka risknivån.

Förändringstakten inom IT är generellt mycket hög, och många leverantörer uppdaterar löpande sina produkter. Samtidigt är utnyttjande av kända sårbarheter i mjukvara ett av de vanligaste sätten att genomföra it-attacker. Detta innebär att det ställs mycket höga krav på verksamheten att omvärldsbevaka och följa med i utvecklingen för att hålla nätverk och informationssystem uppdaterade.

Eftersom tillgänglighet är den viktigaste aspekten att beakta för många samhällsviktiga tjänster, bör man genom sitt arbetssätt säkerställa att eventuella förändringar eller uppdateringar inte medför driftstörningar eller andra incidenter. Denna riskminimering bör omfatta både riskbedömningar innan förändringen görs och uppföljning efteråt. För tekniska förändringar bör användning av testmiljöer eller successiv utrullning användas, och för organisatoriska förändringar, så som utkontraktering eller sammanslagningar, bör dessa förändringar kvalitetssäkras med hjälp av exempelvis avtalsuppföljning.

Arbetet med att uppgradera informationssystem bör inledas genom att verksamheten tar fram en plan för hur ny hård- och mjukvara ska anskaffas och hanteras under sin livstid, och hur och när den ska ersättas. I samband med detta bör man analysera beroenden till andra informationssystem och hur dessa system påverkas av en uppgradering. Det är viktigt att planera i tid

för att uppgradera hård- och mjukvara, annars riskerar verksamheten att sitta med föråldrade informationssystem med kända sårbarheter som kan utnyttjas av en angripare.

Vid utkontraktering bör det säkerställas att eventuella åtgärder som riskbedömningen resulterar i kravställs även mot underleverantören genom avtal. Generellt bör stor vikt läggas på avtalsskrivandet vid utkontraktering, så att det är tydligt vilka servicenivåer som förväntas av leverantören (*Service Level Agreement, SLA*). Avtalet bör också löpande följas upp så att avtalad nivå upprätthålls. Även övriga relevanta säkerhetsåtgärder i föreskriften bör också framgå tydligt i avtalet.

4.3 Säkerhetstester och revision

14 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för säkerhetstester och granskningar av nätverk och informationssystem. Säkerhetstester och granskningar ska möjliggöra identifiering av sårbarheter som kan påverka kontinuiteten i den samhällsviktiga tjänsten.

Syftet med säkerhetstester och revision är

- att verifiera att införda säkerhetsåtgärder är rätt utformade
- att upptäcka eventuella sårbarheter som inte har varit kända för verksamheten tidigare.

Testning och granskning kan antingen genomföras internt, om kompetens och lämpliga verktyg finns, eller av en extern part, exempelvis en IT-revisor eller ett företag specialiserat på säkerhetsgranskning. Så långt det är möjligt bör en oberoende granskning eftersträvas, det vill säga att den som utformat och implementerat säkerhetsåtgärden inte ensam granskar resultatet. Om en extern part anlitas är det viktigt att avtala vad som gäller vid testet och hur information från testerna ska hanteras.

Säkerhetstester bör särskilt genomföras inför driftsättning och innan större förändringar. Behovet av granskningsintervall styrs av risknivån och lösningens betydelse för att upprätthålla kontinuitet för den samhällsviktiga tjänsten. Det innebär att störst granskningsinsats bör läggas på kritiska eller exponerade resurser. Ett upplägg med olika ”djup” i granskningarna rekommenderas. Exempelvis kan man kombinera löpande månadsvis automatiserade sårbarhetsskanningar med hjälp av speciella programvaror avsedda för snabb insamling av standardiserad information om sårbarheter

med manuella penetrationstester där en särskilt utbildad person genomför simulerade attacker för att försöka utnyttja de sårbarheter som identifierats med hjälp av sårbarhetsskanningen. Sådana mer avancerade tester kan göras med längre intervall, exempelvis halvårsvis på prioriterade tillgångar. Om det är en tredje part som gör testerna, bör verksamheten se till att testarna roteras för att få in nya perspektiv och angreppssätt.

Granskningen bör också samordnas med andra uppföljningsaktiviteter, exempelvis internrevision eller extern revision av befintliga certifierade ledningssystem (kvalitet, miljö, arbetsmiljö etc.). Kodgranskning är ytterligare en granskningsmetodik som kan behövas, där en genomgång görs av framtagen kod för en applikation. Även här kan automatiserade sökningar efter osäker kod kombineras med fördjupad, manuell granskning.

4.4 Utbildningsplan

15 § Leverantören ska ta fram, fastställa och tillämpa en utbildningsplan för de befattningar, roller och funktioner som har ansvarsuppgifter kopplade till de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Planen ska innefatta informationssäkerhetshöjande utbildningar, repetitionsutbildningar, övningar och beskrivningar av utbildningsinsatsers målgrupper, mål och syften. Genomförda utbildningar, repetitionsutbildningar och övningar ska dokumenteras.

Syftet med en utbildningsplan är att höja säkerhetsmedvetandet hos den personal som jobbar med de samhällsviktiga tjänsterna. Utbildningen bör målgruppsanpassas och planeras noggrant så att alla berörda har kunskap om vad som krävs och vem som gör vad. Utbildningsunderlag och vem som gått de olika kurserna vid olika tillfällen ska dokumenteras och sparas.

Notera att även externa aktörer kan behöva utbildning, exempelvis driftspersonal vid utkontraktering eller inhyrda konsulter.

Utbildningen bör minst omfatta

- hotbild för verksamheten
- regelverket kring NIS
- interna policies, regler, rutiner och processer kopplade till informationssäkerhet
- hantering av incidenter

- specifik och anpassad information för olika roller, t.ex. krishantering.

Andelen medarbetare som har genomgått utbildning bör vara en punkt att följa upp för att säkerställa att alla får ta del av utbildningen och att den genomförs enligt fastställt intervall.

4.5 Identiteter

20 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för upprättandet av unika identiteter för användare, systemadministratörer, och automatiserade processer. Leverantören ska löpande föra förteckning över tilldelade identiteter. Identiteter ska avaktiveras när de inte längre används eller behövs.

Syftet med en strukturerad och dokumenterad identitetshantering är

- att säkerställa att en individ är den person den utger sig att vara innan man tilldelar personen behörigheter
- att kunna identifiera vilka åtkomsträttigheter en viss individ eller ett visst subjekt tilldelas, något som också gör det möjligt att spåra vem som till exempel gjort en förändring i systemet.

Identitetshanteringen bör täcka *onboarding*, när en individ börjar, *off-boarding,* när en individ slutar eller får andra arbetsuppgifter och *re-boarding*, när en tidigare medarbetare återkommer i tjänst.

En identitet bör endast tilldelas en person. Om en identitet inte längre ska användas, bör inte kontot raderas. I stället bör man inaktivera det, eftersom detta gör det möjligt att knyta händelser långt tillbaka i tid till specifika konton. Beakta dock de rättsliga förutsättningarna för att spara personuppgifter över tid.

4.6 Behörigheter

21 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för hantering av behörigheter. De interna reglerna ska beskriva när behörigheter ska följas upp och på vilka grunder de tilldelas, ändras, och återkallas. Leverantören ska löpande föra förteckning över tilldelade behörigheter. En användare eller automatiserad process ska endast tilldelas den behörighet som är nödvändigt för arbetsuppgiften.

Syftet med en strukturerad behörighetsstyrning är

- att säkerställa att användare endast har åtkomst till informationstillgångar de är behöriga till.
- att den som inte ska ha åtkomst, inte har rätt behörighet eller inte har rätt kompetens inte ska kunna göra oplanerade förändringar i IT-miljön.
- att beslut avseende åtkomsträttigheter sker på ett av verksamheten definierat sätt.

Ur ett angreppsperspektiv är det också viktigt att användare inte har onödigt höga behörigheter som en angripare kan utnyttja. Detta gäller särskilt systemadministrativa behörigheter. En annan viktig aspekt är att en användare inte ska kunna tilldela sig själv nya eller utökade behörigheter, utan flera attester bör ske innan behörigheten tilldelas.

Behörighetsstyrningen bör omfatta alla typer av användarkonton: individer på alla behörighetsnivåer, systemkonton samt automatiserade processer och användargrupper. Det innebär att en kartläggning av roller och grupper bör genomföras för att underlätta behörighetshantering och uppföljning. Om fjärråtkomst till kritiska nätverk och informationssystem är möjlig bör autentisering av åtkomststbehörighet baseras på flera faktorer (flerfaktorautentisering). Flerfaktorautentisering kan utgöras av exempelvis en kombination av smart kort, lösenord och/eller fingeravtryck.

Behörigheterna bör vara tidsbegränsade, med automatiska påminnelser när tidsbegränsningen håller på att gå ut. Tilldelning och förändring av behörigheter bör kunna kopplas till en ansvarig person, och det bör framgå när beslut om behörigheter fattades.

4.7 Systemadministrativa behörigheter

22 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för hantering av systemadministrativa behörigheter. De interna reglerna ska beskriva när systemadministrativa behörigheter ska följas upp och på vilka grunder de tilldelas, ändras, och återkallas. Systemadministrativa behörigheter ska endast användas för systemadministrativa uppgifter. Tilldelning av systemadministrativa behörigheter ska vara restriktiv och endast tilldelas om det är nödvändigt för arbetsuppgiften. Leverantören ska löpande föra förteckning över tilldelade systemadministrativa behörigheter.

Syftet med att begränsa användningen av konton med höga behörigheter, som ger mycket omfattande åtkomst till IT-miljön, är

- att undvika att misstag eller fel av medarbetare med otillräcklig kompetens får stora konsekvenser
- att försvåra för angripare att utöka sina behörigheter vid ett intrång.

Förteckningar över kontobehörigheter för användare, automatiserade processer och administratörer bör skyddas från oavsiktliga förändringar eller raderingar, i syfte att upprätthålla informationens riktighet.

Vid till exempel ransomware-attacker[9] innebär höga behörigheter spridda i organisationen en högre risknivå, eftersom den skadliga koden då lättare kan spridas med hjälp av administratörsbehörighet. Man bör därför ha som målsättning att vara mycket restriktiv med att tilldela höga behörigheter. Helst bör man också använda flerfakturautentisering. Eftersom det hela tiden sker förändringar i vem som administrerar olika system är det viktigt att ha en aktuell förteckning över administrativa konton och följa upp så att behörigheterna är korrekta.

4.8 Systemadministrativt arbete

23 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för systemadministrativt arbete i nätverk och informationssystem. Av det dokumenterade arbetssättet ska det framgå hur hårdvaru- och mjukvarutillgångar som används för systemadministrativa uppgifter underhålls och konfigureras.

Syftet med kravet på dokumenterade arbetssätt vid systemadministrativt arbete är att säkerställa att endast behörig personal kan installera, konfigurera och underhålla informationssystem som är nödvändiga för att tillhandahålla den samhällsviktiga tjänsten.

Dokumentationen kring systemadministrativt arbete ska även innefatta hur eventuella särskilda administratörsverktyg (hård- och mjukvara, till exempel särskilda administratörsdatorer med applikationer för felsökning, konfigurering etc.) underhålls och ställs in. Om man avtalar om systemadministrativa tjänster med underleverantörer bör man även upprätta

[9] En attack som genom skadlig kod krypterar och låser filer och datorer. Attackerna utförs i syfte att begära en lösenordsumma för att den som angrips ska få tillbaka de låsta filerna eller datorerna.

ett arbetssätt för godkännande av detta ur behörighets- och säkerhetssynpunkt där arbetet kan utföras med minsta möjliga risk t.ex. genom att tidsbegränsa aktiviteter att ske vid specifika tidpunkter. På det sättet har verksamheten kontroll över när det är en underleverantör – alltså en tredje part – som utför systemadministration och hur systemadminstrationen går till.

4.9 Återställningsförmåga

30 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för återställningsförmåga i händelse av en incident i de nätverk och informationssystem som används för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Interna regler och arbetssätt ska tydliggöra hur återställning av de informationstillgångar som upprättats enligt 7 § omhändertas i syfte att återställa kontinuiteten i den samhällsviktiga tjänsten.

Syftet med kravet på återställningsförmåga är att säkerställa den samhällsviktiga tjänstens kontinuitet även under störningar eller avbrott.

Av de interna reglerna och arbetssätten bör det framgå vad som ska säkerhetskopieras, hur ofta detta ska ske, hur länge säkerhetskopior ska bevaras, hur informationstillgångarna ska prioriteras vid återställningen, hur lång tid en återställning får ta och den maximala mängd data som får gå förlorad vid en återställning.

För att verksamheten ska kunna säkerställa återställningsförmågan för den samhällsviktiga tjänsten bör de dokumenterade arbetssätten vidare innehålla verktyg för återställning av säkerhetskopior samt verifiering genom tester. Verifieringen ska visa att arbetssätt och verktyg verkligen gör det möjligt att återställa systemen inom den tid verksamheten bestämt, utan att någon information går förlorad eller att redundansen påverkas.

4.10 Organisation och hantering av kris vid incidenter

31 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt gällande organisation och hantering av kriser som kan uppstå till följd av incidenter i de nätverk och informationssystem som används för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Syftet med denna säkerhetsåtgärd är att tydliggöra

- att verksamheter som tillhandahåller samhällsviktiga tjänster måste veta vilka nätverk och informationssystem som är kritiska och ska prioriteras vid en kris
- att verksamheten ska vara organiserad så att kriser kan hanteras med bibehållen tillgänglighet, riktighet och konfidentialitet.

För att leverantörens arbetssätt ska fungera vid kriser, krävs det att leverantören har interna regler och arbetssätt dels för att upptäcka en incident, dels för att vidta åtgärder för att minimera konsekvenserna av incidenten (se 11 § MSB:s föreskrifter om informationssäkerhet).

För att effektivt kunna hantera en incident som övergår i en kris bör det finnas en tillgänglig krisorganisation som är övad. Av dokumentationen bör det framgå vilka de kritiska och prioriterade informationssystemen är, vem som tillhör incident- och krishanteringsorganisationen, vem som är behörig att fatta beslut vid en kris eller incident samt hur man ska agera vid olika typer av incidenter och kriser. Vidare bör det finnas tydliga, dokumenterade incidentkategorier och kriterier för när en incident övergår till en kris. Kris- och incidenthanteringsplaner bör även testas regelbundet för att säkerställa att de fungerar. Om en kris eller incident inträffar är det av betydelse att man genomför ”*lessons learned*” i syfte att ta lärdom av inträffade händelser.

5 Tekniska säkerhetsåtgärder

5.1 Härdning

16 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för inaktivering av ej använda tjänster och protokoll (härdning) i de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Allmänna råd:

Leverantörens arbetssätt för härdning bör följa produktleverantörens rekommendationer och etablerade standarder för härdning.

Syftet med härdning av mjuk- och hårdvara är att så långt det är möjligt försvåra angrepp. Härdningen görs genom att man avinstallerar eller inaktiverar funktioner och applikationer som inte är nödvändiga eller på annat sätt konfigurerar på ett så säkert sätt som möjligt.

Arbetet med härdning ska ske enligt ett dokumenterat arbetssätt där man i första hand bör utgå från produktleverantörernas rekommendationer och verksamhetens behov. Dessa kan med fördel kombineras med etablerade generella ramverk för härdningskontroll, exempelvis CIS Benchmarks. Varje avsteg från rekommendationer bör motiveras och dokumenteras.

Rutiner bör finnas på plats för att granska och höja säkerheten för både nyinköpt och redan implementerad hård- eller mjukvara. Därmed bör härdningen kopplas till aktuell systemförteckning och riskanalys så att inga informationstillgångar eller komponenter ”glöms bort”. Högst krav på härdning bör ställas på de informationssystem som är mest kritiska för att den samhällsviktiga tjänsten ska fungera.

5.2 Segmentering

17 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för segmentering av de nätverk som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Allmänna råd:

Nätverket bör segmenteras utifrån informationssystemens funktion och värdet på informationen som hanteras i dem.

Syftet med segmentering är

- att separera delsystem som hanterar information med olika informationsklassning och exponering
- att försvåra en angripares möjligheter att ta över hela nätverket efter en lyckad attack på ett delsystem.

Segmentering underlättar dessutom i ett övervakningsperspektiv, eftersom det blir mer överskådligt vilken information som flödar i ett visst segment.

Indelningen av nätverk i olika segment bör baseras på vilken typ av information som finns i segmentet, vilka säkerhetsfunktioner som är införda

och om segmentet kommunicerar externt. Aspekter som bör beaktas för segmentering av informationstillgångar innefattar

- olika känslighet med avseende på konfidentialitet
- olika krav på tillgänglighet
- olika krav på kommunikationssätt
- olika nivå av exponering
- olika funktion eller användningsområde
- informationssystem som används av specifika roller.

Exempelvis är det lämpligt att placera gästnätverk i ett eget segment och att placera servrar med särskilt känslig information i egna segment, exempelvis genom att placera en central säkerhetsloggserver i ett eget segment.

Det finns olika tekniska säkerhetslösningar för att hantera segmentering, antingen via brandväggsregler, virtuell indelning (VLAN) eller kan man använda sig av fysisk indelning med hjälp av olika nätverksprodukter. Det finns även tekniker för mjukvarubaserad segmentering (*Software Defined Networking*, SDN).

5.3 Filtrering

18 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för filtrering av nätverkstrafik, så att endast nödvändiga dataflöden förekommer mellan de nätverkssegment som behövs för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Syftet med filtrering av nätverkstrafik är

- att minska attackmöjligheterna genom att ta bort överflödiga kommunikationssätt, så att endast nödvändig trafik[10] ingår i dataflödet
- att underlätta övervakningen.

[10] ”Nödvändig trafik” är den trafik som behövs för att systemet ska fungera och vara säkert.

Filtrering kan exempelvis ske med hjälp av brandväggsregler eller särskilda applikationer för övervakning av nätverkstrafik.

Av de dokumenterade arbetssätten bör det framgå hur man gör en noggrann analys och utvärdering av vilka portar och protokoll som behöver användas av ett nytt system eller en ny applikation. Analysen och utvärderingen bör göras innan systemet eller applikationen tas i drift.

5.4 Kryptering

19 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för att hantera behovet av kryptering, i syfte att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

Syftet med kryptering är att skydda information mot obehörig åtkomst och obehörig förändring både under lagring och i kommunikationsutbyte (*data at rest, data in use, data in transit*). Kryptering kan även användas för att verifiera en avsändare eller för att verifiera ett skickat meddelandes integritet.

Ofta krävs en kombination av olika krypteringslösningar, både kryptering av enskilda filer eller hårddiskar och kryptering av webbsidor och kommunikation med hjälp av olika protokoll eller lösningar som TLS[11]/HTTPS, VPN[12] eller IPsec[13] för att skydda informationen. Val av krypteringslösningar behöver baseras på verksamhetens behov och tekniska förutsättningar.

Eftersom teknikutvecklingen går snabbt, behöver verksamheten omvärldsbevaka valda lösningar för att få vetskap om eventuella sårbarheter. Man bör också aktivt arbeta med att fasa ut äldre protokoll eller tekniska lösningar som används, eftersom det innebär stora risker att förlita sig på svag kryptering.

För att bedöma när kryptering ska användas och vilken krypteringsmetod som är lämplig behöver verksamheten förstå vilken information som behandlas i respektive nätverkssegment och systemkomponent. Bedömningen förutsätter också att verksamheten har analyserat

[11] Transport Layer Security.
[12] Virtuellt privat nätverk.
[13] Internet Protocol Security.

konsekvenserna av röjande eller manipulation av sin information genom informationsklassning.

De interna reglerna och arbetssätten bör innefatta hur krypteringslösningar väljs, en beskrivning av vad krypteringsmetoden innebär, hur krypteringslösningar godkänns och förvaltas samt hur krypteringsnycklar ska hanteras och förvaras.

5.5 Autentisering

24 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för autentisering av identiteter enligt 20 §. Vid fjärr- eller systemadministrativ åtkomst till de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten, ska autentiseringen baseras på flera faktorer (flerfaktorsautentisering).

Syftet med kravet på autentisering är

- att säkerställa att det endast är behöriga individer och systemkonton som har åtkomst till informationstillgångar
- att försvåra för en angripare som försöker ta över ett användarkonto.

Reglerna för autentiseringsuppgifter bör minst omfatta krav på lösenords längd och komplexitet, hur ofta lösenord ska bytas samt hur distribution och skydd av autentiseringsinformation ska ske. Kraven bör anpassas till aktuell riskbedömning

Det är särskilt viktigt att autentisering sker på ett säkert sätt vid systemadministration eller annan användning av höga behörigheter, därav kravet på flerfaktorsautentisering för sådana roller. Detsamma gäller fjärråtkomst, där användaren ansluter från okänd plats med medföljande högre risknivå.

Med flerfaktorsautentisering avses minst en faktor utöver användarnamn och lösenord. Vanliga tekniska lösningar är engångslösenord via sms eller appar, och certifikat lagrade på smarta kort eller särskilda usb-minnen. Val av lösning kan bl.a. bero på hur känslig informationstillgången är. Utöver användning av flerfaktorsautentisering är någon form av VPN-lösning starkt rekommenderad vid fjärråtkomst.

5.6 Skydd av utrustning

25 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för skydd av utrustning mot skador av och obehörig fysisk åtkomst till utrustning för de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Allmänna råd:

Leverantören bör skydda utrustning för de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten, genom att
1. placera centrala servrar och central nätverksutrustning i särskilda IT-utrymmen,
2. restriktivt tilldela behörighet till att tillträda särskilda IT-utrymmen,
3. identifiera och hantera behovet av övervakning och larm i särskilda IT-utrymmen,
4. på individnivå registrera tillträde till särskilda IT-utrymmen och spara dokumentationen under fastställd bevarandetid, och
5. ha interna regler för hur mobil utrustning ska skyddas.

Syftet med detta krav är att verksamheten ska ha dokumenterade och enhetliga krav på hur det fysiska skyddet ska vara utformat så att skador, förlust eller obehörig åtkomst till utrustning förhindras.

Åtgärderna för att skydda utrustning behöver väljas och utformas utifrån organisationens behov och informationsklassning, men bör minst omfatta följande:

- Sektorindelning i besökszoner, särskilda utrymmen för hantering av känslig information etc.
- Fysiskt skydd av serverrum, korskopplingsskåp och liknande utrymmen (it-utrymmen), både vad gäller obehörig åtkomst och olyckshändelser som brand, värme eller fukt, eller störningar i elförsörjningen.
- Åtkomstbegränsning; åtkomst till it-utrymmen bör endast beviljas om det är nödvändigt för att kunna lösa en arbetsuppgift.
- Larm och övervakningsensorer för it-utrymmen.
- Administrativa rutiner vid tillträde till utrymmen, exempelvis besöksliggare.

- Regler för hantering av mobila enheter såsom bärbara datorer, lagringsmedia, surfplattor och telefoner. Reglerna bör omfatta hantering med kvittenser, märkning, krav på skärmlås etc. och hantering av utrustning som inte befinner sig inom skalskyddet, exempelvis vid resa. Det kan exempelvis vara i vilka situationer den mobila enheten får tas med, användas och förvaras samt beteenden för att förhindra att obehöriga ser eller hör information
- Förvaringplatser för information, t.ex. säkerhetsskåp, brandskåp och låsbara utrymmen.

Innan utrustning kasseras, återanvänds eller lämnas in på service bör den information som finns på utrustningen raderas för att obehöriga inte ska kunna ta del av informationen. Av de interna reglerna bör det därför tydligt framgå att det inte ska gå att återskapa information som finns på it-utrustning som ska kasseras, återanvändas eller lämnas in på service, Det ska också tydligt framgå hur man åstadkommer detta (destruktion genom förbränning, nermalning av utrustning osv.).

Vid utkontraktering är det viktigt att leverantören är medveten om och uppfyller verksamhetens krav på fysiskt skydd, detta bör därmed ingå i avtalet.

5.7 Detektering av dataintrång

26 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för identifiering av dataintrång. Där det är lämpligt ska leverantören anskaffa och använda intrångsdetekteringssystem (IDS) för de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten.

Syftet med intrångsdetektering är att upptäcka problem eller oönskade aktiviteter i nätverk och informationssystem så tidigt som möjligt, för att därefter kunna vidta åtgärder för att begränsa eller förhindra skadan.

Alla säkerhetsrelevanta händelser i nätverk och informationssystem bör detekteras och generera larm.

För en framgångsrik implementering av intrångsdetektering krävs både tekniska lösningar och interna regler och arbetssätt för att identifiera säkerhetsrelaterade händelser, hantera larm och bemöta oönskade aktiviteter som upptäcks.

Rent tekniskt finns det en lång rad olika lösningar för antingen intrångsdetekteringssystem (IDS) eller intrångsförhindrande system (IPS). Lösningarna kan installeras på värdsystem (*Hosted-Based Intrusion Detection*, HIDS) eller på nätverkskomponenter (*Network-Based Intrusion Detection*, NIDS). Intrångsdetekteringssystem bör undersöka nätverkstrafik både inom organisationens nätverk samt kommunikation som lämnar organisationens nätverk eller mottas från externt nätverk. Trafik till och från informationssystem samt säkerhetskomponenter (exempelvis brandväggar) bör omfattas av intrångsdetekteringssystemet. Kunskap om normalbilden, det vill säga vilka dataflöden och vilken trafik som normalt förekommer, är en viktig del av förmågan att detektera intrång.

Upptäckta angrepp behöver hanteras som incidenter enligt definierade rutiner och vid eskalering till en kris för organisationen ska detta hanteras enligt framtagna rutiner för krishantering (se ovan avsnitt 4.10).

5.8 Skydd mot skadlig kod

27 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för skydd mot skadlig kod i de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Där mjukvara för skydd mot skadlig kod inte är lämplig eller tillgänglig ska andra åtgärder vidtas för att uppnå ett motsvarande skydd.

Syftet med denna säkerhetsåtgärd är

- att alla systemdelar ska ha ett fungerade teknisk skydd mot skadlig kod
- att det ska finnas administrativa rutiner för att hålla skyddet uppdaterat.

Med skadlig kod avses både datorvirus och annan exekverbar kod som syftar till att en angripare ska kunna kontrollera en eller flera enheter eller på annat sätt påverka en informationstillgångs konfidentialitet, riktighet eller tillgänglighet.

Observera att skydd mot skadlig kod inte bara behöver innebära traditionella anti-virusprogram. Skyddet kan även bestå av exempelvis vitlistning, som innebär att en programvara ser till att endast godkända applikationer kan exekvera kod i systemet, eller av olika typer av tekniska lösningar för att övervaka aktiviteter eller oväntade beteenden på enskilda enheter. Det kan

också vara olika typer av webbfilter eller spamfilter. I skyddet bör det även ingå en begränsning av möjligheten att ansluta okontrollerade externa lagringsmedier via USB. Om det finns begränsade möjligheter att installera skydd mot skadlig kod för ett visst system eller en viss enhet bör andra säkerhetsåtgärder vidtas, exempelvis kan systemet placeras i ett eget nätverkssegment.

Interna regler och arbetssätt bör tydliggöra hur larm om skadlig kod ska hanteras beroende på allvarlighetsgrad (risk för spridning och risk för skada).

5.9 Säkerhetsloggning

28 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för att säkerställa spårbarhet i säkerhetsrelaterade händelser avseende de nätverk och informationssystem som är nödvändiga för att upprätthålla kontinuiteten i den samhällsviktiga tjänsten. Av arbetssättet ska det framgå hur säkerhetsloggar skyddas mot avsiktlig eller oavsiktlig förändring, förlust och radering.

Allmänna råd:

För att skapa en jämförbarhet bör leverantören se till att samtliga loggkällor använder gemensam tid.

Syftet med säkerhetsloggning är att spåra och upptäcka säkerhetsrelaterade händelser, i nätverk och informationssystem.

En säkerhetsrelaterad händelse kan vara en olyckshändelse, men den kan också ha orsakats av antagonistiska hot. Mer specifikt avses med säkerhetsrelaterad händelse varje typ av händelse som påverkar konfidentialitet, riktighet och tillgänglighet för den samhällsviktiga tjänsten. Det kan till exempel röra sig om försök till obehörig åtkomst, förändring av konfigurationer eller inställningar, förändring av behörigheter för användare eller dataintrång.

För varje informationssystem eller nätverkskomponent (”loggkälla”) bör det därför göras en analys av vilka händelser som behöver loggas, var loggposterna sparas och om larm ska automatgenereras när avvikelser upptäcks. Säkerhetsloggar bör innehålla den information som krävs för att kunna förstå ett händelseförlopp. Varje loggpost i en säkerhetslogg bör

minst innehålla datum och tid, vilken användare eller informationssystem som genererat händelsen samt själva händelsen.

Säkerhetsrelevanta händelser som bör registreras är exempelvis autentisering av användare, ändringar av åtkomstsbehörighet och användarroller, lyckade och misslyckade åtkomstförsök, förändringar i säkerhetsmekanismer och funktionalitet. åtkomst till filer, mappar eller andra systemresurser, ändringar av konfigurationer, raderingar och överföring av objekt. Även andra händelser kan behöva säkerhetsloggas, beroende på behovet av ytterligare spårbarhet i IT-miljön. Verksamheten bör analysera vad som kan utgöra säkerhetsrelevanta händelser utifrån respektive informationssystem.

Säkerhetsloggar ska skyddas mot avsiktliga eller oavsiktliga förändringar, förluster och raderingar. Insamlade loggar bör därför hanteras i ett eget segment i nätverket och administreras av särskilda loggadministratörer som inte samtidigt är systemadministratörer. Undvik därför att blanda vanliga driftloggar och säkerhetsloggar.

Vanligtvis utförs säkerhetsloggning i flera delsystem för att ge en helhetsbild av en specifik händelse. Verksamheten bör därför säkerställa att dessa olika loggar kan analyseras och korreleras gemensamt.

En förutsättning för korrelationsanalys är att samtliga loggkällor i respektive system har gemensam tid, till exempel UTC.

Det bör även finnas regler och rutiner i verksamheten som beskriver hur loggar ska hanteras, lagras och arkiveras i respektive informationssystem. Av dessa bör det framgå

- varför insamling av säkerhetsloggar sker
- vad man behöver kunna upptäcka
- hur säkerhetsloggarna ska användas
- hur de ska analyseras och av vem
- vilken information säkerhetsloggarna innehåller
- vilka loggkällor som finns
- hur säkerhetsloggarna lagras, inklusive eventuella mellansteg eller aggregering

- hur de skyddas mot skada, obehörig åtkomst och obehörig förändring
- hur länge de ska bevaras och kunna användas för analys.

5.10 Logganalys

29 § Leverantören ska ta fram, fastställa och tillämpa dokumenterade interna regler och arbetssätt för logganalys, i syfte att upptäcka och hantera incidenter och avvikelser som kan påverka kontinuiteten i den samhällsviktiga tjänsten.

Syftet med logganalys är

- att man ska kunna upptäcka oönskade händelser
- att man ska kunna återskapa händelsekedjor så att det är möjligt att spåra vad som hänt i ett system.

Logganalysen bör till största delen ske med hjälp av automatiserad analys och larmgenerering, då det ofta är fråga om stor mängder uppgifter som behöver analyseras. De interna reglerna och arbetssättet för att samla in och analysera loggar i syfte att upptäcka händelser som kan inverka negativt på leveransen av den samhällsviktiga tjänsten bör inkludera

- vilka roller som får hantera respektive utföra manuell analys av säkerhetsloggar
- när analys ska genomföras, exempelvis regelbundet, genom stickprovskontroller eller på förekommen anledning
- hur analys av säkerhetsloggar ska genomföras, exempelvis om det ska ske automatiskt, manuellt eller genom en kombination
- vilka tekniska stöd som används för analysen
- hur man ska agera och vem som ska kontaktas om en misstänkt händelse eller avvikelse upptäcks
- hur händelser ska struktureras och vilken data som ska tas fram för att kunna informera om inträffade händelser
- hur man arbetar med ständiga förbättringar kring arbetssättet för säkerhetsloggning.

Bilaga 1 – Hänvisningar till standarder och ramverk

Nedan redovisas hänvisningar till liknande krav på säkerhetsåtgärder i andra standarder och regelverk. Hänvisningarna kan användas som stöd vid arbetet med att implementera säkerhetsåtgärder enligt denna vägledning.

Avsnitt vägledning	**ENISA**	**ISO 27001: 2022**	**ISO 27002: 2022**	**NIST CSF**	**MSBFS 2018:8**	**MSB Vägledning**
6 § Inventering	1.1.7	A.5.9, A.5.2	5.2	ID.AM-1, ID.AM-2, ID.AM-4	6 §	2.1
7 § Förteckning av informationstillgångar	1.1.1	A.5.9, A.5.2	5.2	ID.AM-1, ID.AM-2, ID.AM-4 ID.AM-5	6 §	2.1
8 § Omvärldsbevakning	1.1.1	A.5.6	5.6	ID.RA-2	8 §	2.2
9 § Riskanalys	1.1.1	A.5.3	5.3	ID.GV-4, ID.RA-1, 3, 4, 5, 6, ID.RM-1, ID.SC-1, 2, DE.CM-8, RS.MI-3, RS.AN-5	8 §	4.2
10 § Åtgärdsplan	1.1.1	A.5.5	5.5	ID.RM-2, 3	8 §	2.2
11 § Uppföljning	1.1.1	A.5.5	5.5	ID.RM-2, 3	8 §	2.2
12 § Driftsgodkännande	1.1.3	A.5.8, A.8.27, A.8.31,	5.8, 8.27, 8.31, 5.36, 8.8	ID.RA-1, PR.PT-1, 2, 3, 4, 5,	7 §	3.1, 3.3, 4.1, 3.2, 3.6, 2.2, 2.3, 2.4

Avsnitt vägledning	ENISA	ISO 27001: 2022	ISO 27002: 2022	NIST CSF	MSBFS 2018:8	MSB Vägledning
		A.5.36, A.8.8		RS.MI-3		
13 § Ändringshantering, uppgradering och uppdatering	2.4.1	A.7.13, A.5.37, A.8.32, A.8.19, A.8.8, A.5.19, A.5.20, A.5.21, A.5.22	7.13,5.37, 8.32, 8.19, 8.8, 8.32, 5.20, 5.21, 5.22	PR.MA-2, PR.IP-1, PR.IP-3, ID.SC-4	10 §	4.13, 3.2, 4.5, 4.7, 2.2, 2.3, 2.4, 3.1
14 § Säkerhetstester och revision	1.1.5	A.8.34, A.8.8, A.8.29, A.6.8	8.34, 8.8, 8.29, 6.8	ID.RA-1, DE.CM-8, ID.SC-4, PR.PT-1, PR.IP-7 och 12	8 §, 10 §	4.6, 2.2, 2.3, 2.4, 3.2
15 § Utbildningsplan	1.1.6	A.6.3	6.3	PR.AT-1, 2, 3, 4, 5	9 § punkt 1 och 2	
16 § Härdning	2.1.1	A.8.1, A.5.37, A.8.32, A.8.7, A.8.19, A.8.8	8.1, 5.37, 8.32, 8.19, 8.8	PR.IP-1, PR.IP-3, DE.AE-1, PR.PT-3	10 §	4.13, 3.2, 4.5, 2.2, 2.3, 2.4, 4.7
17 § Segmentering	2.1.2	A.8.20, A.8.22, A.5.14	8.20, 8.22, 5.14	PR.PT-4, PR.AC-3, PR.AC-5, PR.DS-2	10 §	4.1

Avsnitt vägledning	ENISA	ISO 27001: 2022	ISO 27002: 2022	NIST CSF	MSBFS 2018:8	MSB Vägledning
18 § Filtrering	2.1.3	A.8.20, A.8.22	8.20, 8.22	PR.DS-5, PR.PT-4, PR.AC-5	11 §	4.1
19 § Kryptering	2.1.4	A.8.24, A.5.31, A.8.11	8.24, 5.31	ID.GV-3, PR.DS-1, PR.DS-2, PR.DS-5, PR.PT-4	10 §	4.4, 3.1, 5.1
20 § Identiteter	2.3.1	A.5.15, A.8.3, A.8.5, A.5.17, A.8.18	8.3, 8.5, 5.17, 8.18	PR.AC-1, PR.AC-4, PR.AC-6, PR.AC-7, PR.DS-5	10 §	4.2, 4.3
21 § Behörigheter	2.3.1	A.5.15, A.8.3, A.8.5, A.5.17, A.8.18	8.3, 8.5, 5.17, 8.18	PR.AC-1, PR.AC-4, PR.AC-6, PR.AC-7, PR.DS-5	10 §	4.2, 4.3
22 § Systemadministrativa behörigheter	2.2.1	A.8.2, A.5.18, A.8.18, A.8.15	8.2, 5.18, 8.18, 8.15	PR.AC-1, PR.AC-4, PR.AC-7, PR.AT-2, PR.AT-4	11 §	4.2, 4.10, 4.11
23 § Systemadministrativt arbete	2.2.2	A.8.18, A.8.15, A.8.19,	8.18, 8.15, 8.19,	PR.AC-3, PR.AC-4, PR.AC-6	6 §, 8 §	4.2, 4.10, 4.11, 4.5, 4.7, 3.1, 3.2, 4.7

Avsnitt vägledning	ENISA	ISO 27001: 2022	ISO 27002: 2022	NIST CSF	MSBFS 2018:8	MSB Vägledning
		A.8.26, A.8.32	8.26, 8.32			
24 § Autentisering	2.2.2	A.8.18, A.8.15, A.8.19, A.8.26, A.8.32	8.18, 8.15, 8.19, 8.26, 8.32	PR.AC-3, PR.AC-4, PR.AC-6	6 §, 8 §	4.2, 4.10, 4.11, 4.5, 4.7, 3.1, 3.2, 4.7
25 § Skydd av utrustning	2.5.1	A.8.1, A.7.1, A.7.2, A.7.3, A.7.5, A.7.6, A.7.8, A.7.9, A.7.14	8.1, 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.9, 7.14	DE.CM-2, 3, 6, PR.IP-5, 6, PR.AC-2, 3, PR.DS-3, PR.PT-2	10 §	4.13
26 § Detektering av dataintrång	3.1.1	A.7.1, A.8.15, A.8.17, A.8.20, A.8.16	7.1, 8.15, 8.17, 8.20	DE.AE-1, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-7, PR.PT-1	11 §	4.13, 4.10, 4.12, 4.8, 4.1
27 § Skydd mot skadlig kod	3.1.1	A.8.15	8.15	PR.DS-6, PR.AT-1, DE.CM-4, RS.MI-1, RS.MI-2	10 §	4.10, 4.12
28 § Säkerhetsloggning	3.1.2	A.8.15, A.8.17, A.8.16, A.5.22,	8.15, 8.17, 5.22, 5.24,	DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6,	11 §	3.1, 4.10, 4.11, 4.9, 4.8

Avsnitt vägledning	ENISA	ISO 27001: 2022	ISO 27002: 2022	NIST CSF	MSBFS 2018:8	MSB Vägledning
		A.5.24, A.5.25, A.5.33	5.25, 5.33	DE.CM-7, DE.AE-3, PR.PT-1		
29 § Logganalys	3.1.3	A.8.15, A.8.17, A.8.16, A.5.25, A.5.27, A.5.28	8.15, 8.17, 5.25, 5.27, 5.28	ID.RA-4, PR.PT-1, DE.AE -2, DE.AE -3, DE.AE -4, DE.DP-5, RS.AN-1, RS.AN-5, DE.AE-3	10 §	4.10, 4.11, 4.8, 4.6
30 § Återställningsförmåga	4.1.2	A.8.14		ID.ID.BE-5, PR.PT-5, PR.IP-9, 10, PR.DS-4, RC.IM-1, 2, RC.RP-1	12 § punkt 1-3	
31 § Organisation och hantering av kris vid incidenter	4.2.1, 4.2.2	A.5.29, A.8.14, 7.4, 9.3, 10.2, A.5.1, A.5.5, A.7.13,	5.29, 8.14, 5.1, 5.5, 7.13	PR.DS-4, ID.BE-5, RC.CO-1, 2, 3, RC.RP-1, RS.IM-1, 2, ID.SC-5, PR.IP-4, 9, 10, PR.PT-5	12 § punkt 1-3	4.14, 2.2, 4.13

TRANSPORT STYRELSEN
transportstyrelsen.se
telefon 0771-503 503