RISK- OCH SÅRBARHETSANALYS FÖR TELEKOM

BASHOT TELEKOM

ROBUSTHETSVECKAN
MAJ 2022

Jimmy Persson
Utveckling- och säkerhetschef
Jimmy.persson@ssnf.org
073-274 26 15

ROBUST DIGITAL INFRASTRUKTUR

RDI BASHOT TELEKOM

- **Säkerhetsarbete för nätägare**
- **Hotkatalogen**
  - Site och nod
  - Säker fysisk förbindelse
  - Övriga
- **Genomgång Excelmall RSA**
- **Instruktion för RSA**

Jimmy Persson
Utveckling- och säkerhetschef
Jimmy.persson@ssnf.org
073-274 26 15

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

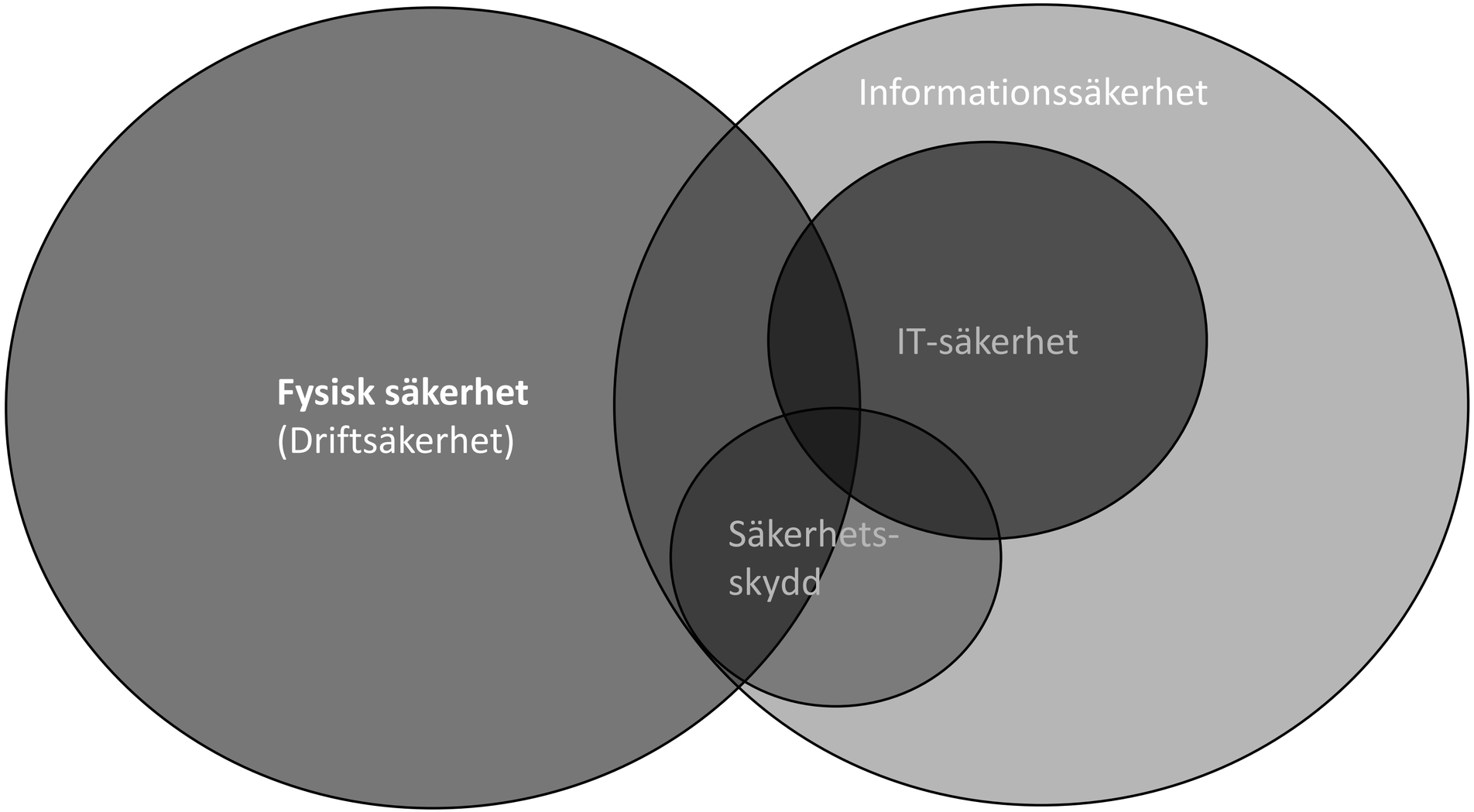
Säkerhetsarbete för nätägare

IoT/OT-SÄKERHET

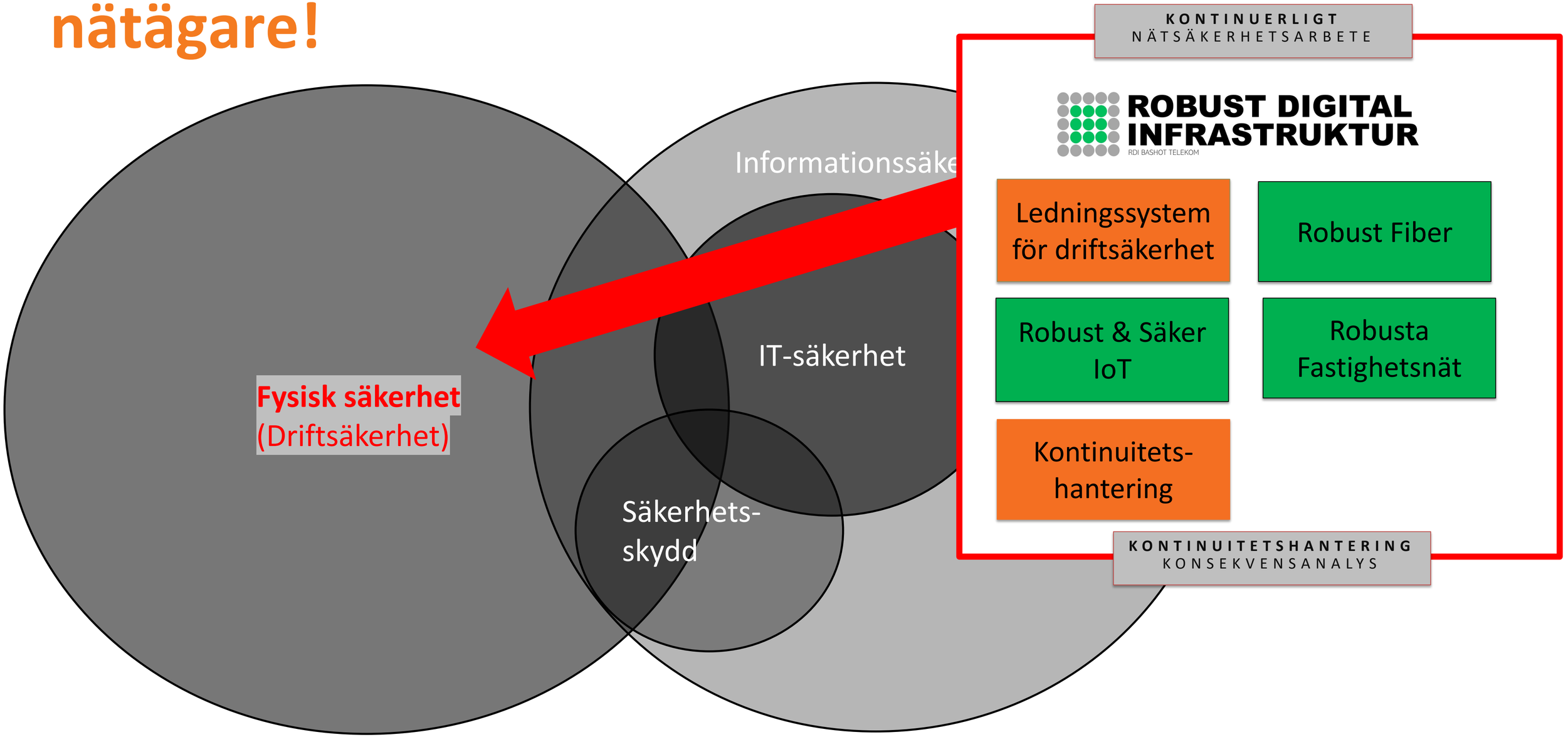
SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

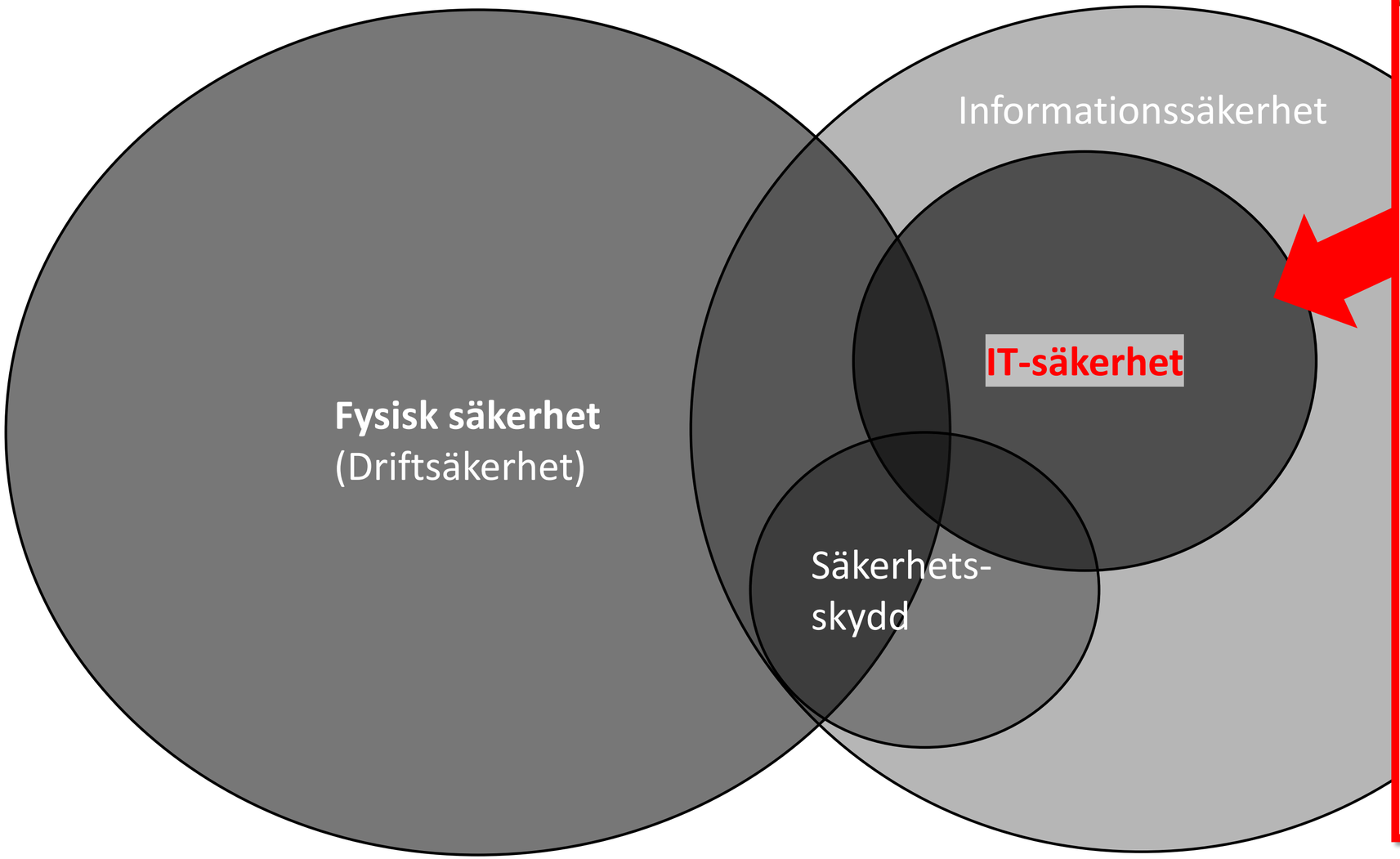
Säkerhetsområden för nätägare att förhålla sig till!



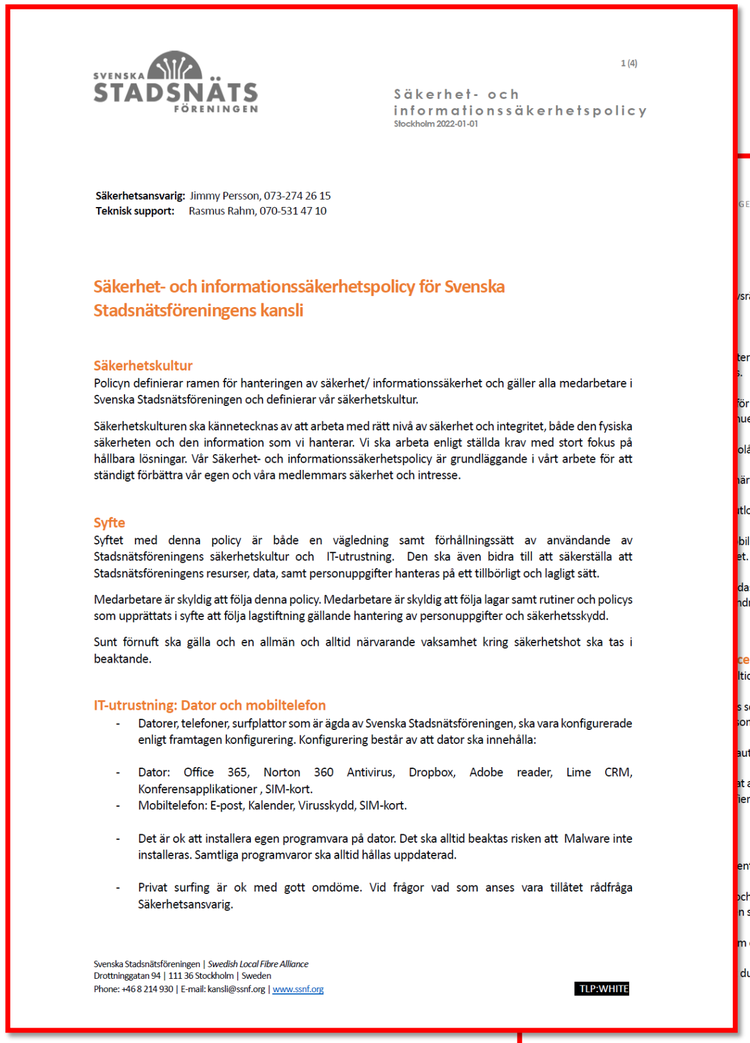
Säkerhetsområden för nätägare!



Säkerhetsområden för nätägare!



Säkerhetsområden för nätägare!



1 (4)

SVENSKA STADSNÄTS FÖRENINGEN

Säkerhet- och informationssäkerhetspolicy
Stockholm 2022-01-01

Säkerhetsansvarig: Jimmy Persson, 073-274 26 15
Teknisk support: Rasmus Rahm, 070-531 47 10

Säkerhet- och informationssäkerhetspolicy för Svenska Stadsnätsföreningens kansli

Säkerhetskultur

Policyn definierar ramen för hanteringen av säkerhet/ informationssäkerhet och gäller alla medarbetare i Svenska Stadsnätsföreningen och definierar vår säkerhetskultur.

Säkerhetskulturen ska kännetecknas av att arbeta med rätt nivå av säkerhet och integritet, både den fysiska säkerheten och den information som vi hanterar. Vi ska arbeta enligt ställda krav med stort fokus på hållbara lösningar. Vår Säkerhet- och informationssäkerhetspolicy är grundläggande i vårt arbete för att ständigt förbättra vår egen och våra medlemmars säkerhet och intresse.

Syfte

Syftet med denna policy är både en vägledning samt förhållningssätt av användande av Stadsnätsföreningens säkerhetskultur och IT-utrustning. Den ska även bidra till att säkerställa att Stadsnätsföreningens resurser, data, samt personuppgifter hanteras på ett tillbörligt och lagligt sätt.

Medarbetare är skyldig att följa denna policy. Medarbetare är skyldig att följa lagar samt rutiner och policys som upprättats i syfte att följa lagstiftning gällande hantering av personuppgifter och säkerhetsskydd.

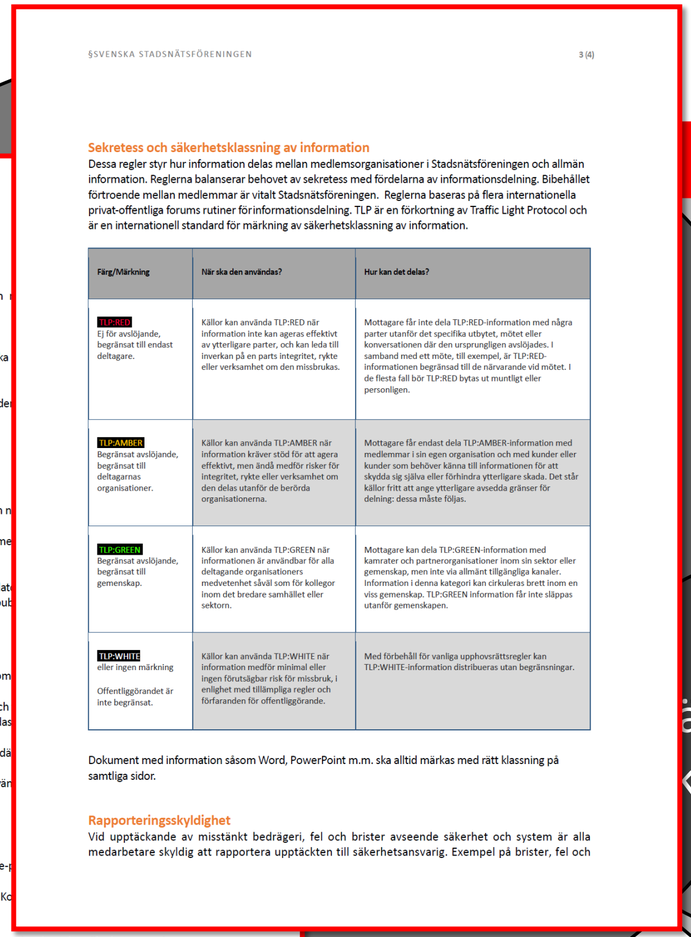
Sunt förnuft ska gälla och en allmän och alltid närvarande vaksamhet kring säkerhetshot ska tas i beaktande.

IT-utrustning: Dator och mobiltelefon

- Datorer, telefoner, surfplattor som är ägda av Svenska Stadsnätsföreningen, ska vara konfigurerade enligt framtagen konfigurering. Konfigurering består av att dator ska innehålla:
- Dator: Office 365, Norton 360 Antivirus, Dropbox, Adobe reader, Lime CRM, Konferensapplikationer , SIM-kort.
- Mobiltelefon: E-post, Kalender, Virusskydd, SIM-kort.
- Det är ok att installera egen programvara på dator. Det ska alltid beaktas risken att Malware inte installeras. Samtliga programvaror ska alltid hållas uppdaterad.
- Privat surfing är ok med gott omdöme. Vid frågor vad som anses vara tillåtet rådfråga Säkerhetsansvarig.

Svenska Stadsnätsföreningen | *Swedish Local Fibre Alliance*
Drottninggatan 94 | 111 36 Stockholm | Sweden
Phone: +46 8 214 930 | E-mail: kansli@ssnf.org | www.ssnf.org

TLP:WHITE



§SVENSKA STADSNÄTSFÖRENINGEN 3 (4)

Sekretess och säkerhetsklassning av information

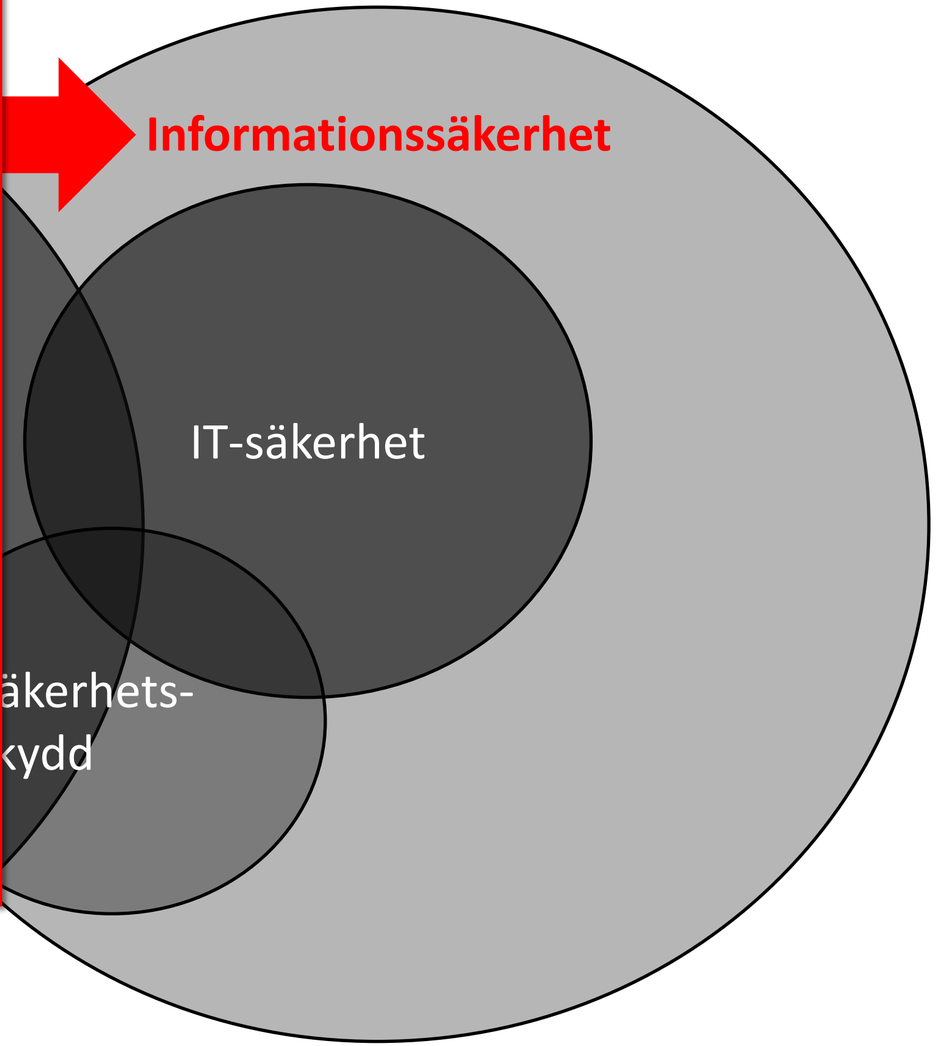
Dessa regler styr hur information delas mellan medlemsorganisationer i Stadsnätsföreningen och allmän information. Reglerna balanserar behovet av sekretess med fördelarna av informationsdelning. Bibehållet förtroende mellan medlemmar är vitalt Stadsnätsföreningen. Reglerna baseras på flera internationella privat-offentliga forums rutiner för informationsdelning. TLP är en förkortning av Traffic Light Protocol och är en internationell standard för märkning av säkerhetsklassning av information.

Färg/Märkning	När ska den användas?	Hur kan det delas?
TLP:RED Ej för avslöjande, begränsat till endast deltagare.	Källor kan använda TLP:RED när information inte kan ageras effektivt av ytterligare parter, och kan leda till inverkan på en parts integritet, rykte eller verksamhet om den missbrukas.	Mottagare får inte dela TLP:RED-information med några parter utanför det specifika utbytet, mötet eller konversationen där den ursprungligen avslöjades. I samband med ett möte, till exempel, är TLP:RED-informationen begränsad till de närvarande vid mötet. I de flesta fall bör TLP:RED bytas ut muntligt eller personligen.
TLP:AMBER Begränsat avslöjande, begränsat till deltagarnas organisationer.	Källor kan använda TLP:AMBER när information kräver stöd för att agera effektivt, men ändå medför risker för integritet, rykte eller verksamhet om den delas utanför de berörda organisationerna.	Mottagare får endast dela TLP:AMBER-information med medlemmar i sin egen organisation och med kunder eller kunder som behöver känna till informationen för att skydda sig själva eller förhindra ytterligare skada. Det står källor fritt att ange ytterligare avsedda gränser för delning: dessa måste följas.
TLP:GREEN Begränsat avslöjande, begränsat till gemenskap.	Källor kan använda TLP:GREEN när informationen är användbar för alla deltagande organisationers medvetenhet såväl som för kollegor inom det bredare samhället eller sektorn.	Mottagare kan dela TLP:GREEN-information med kamrater och partnerorganisationer inom sin sektor eller gemenskap, men inte via allmänt tillgängliga kanaler. Information i denna kategori kan cirkuleras brett inom en viss gemenskap. TLP:GREEN information får inte släppas utanför gemenskapen.
TLP:WHITE eller ingen märkning Offentliggörandet är inte begränsat.	Källor kan använda TLP:WHITE när information medför minimal eller ingen förutsägbar risk för missbruk, i enlighet med tillämpliga regler och förfaranden för offentliggörande.	Med förbehåll för vanliga upphovsrättsregler kan TLP:WHITE-information distribueras utan begränsningar.

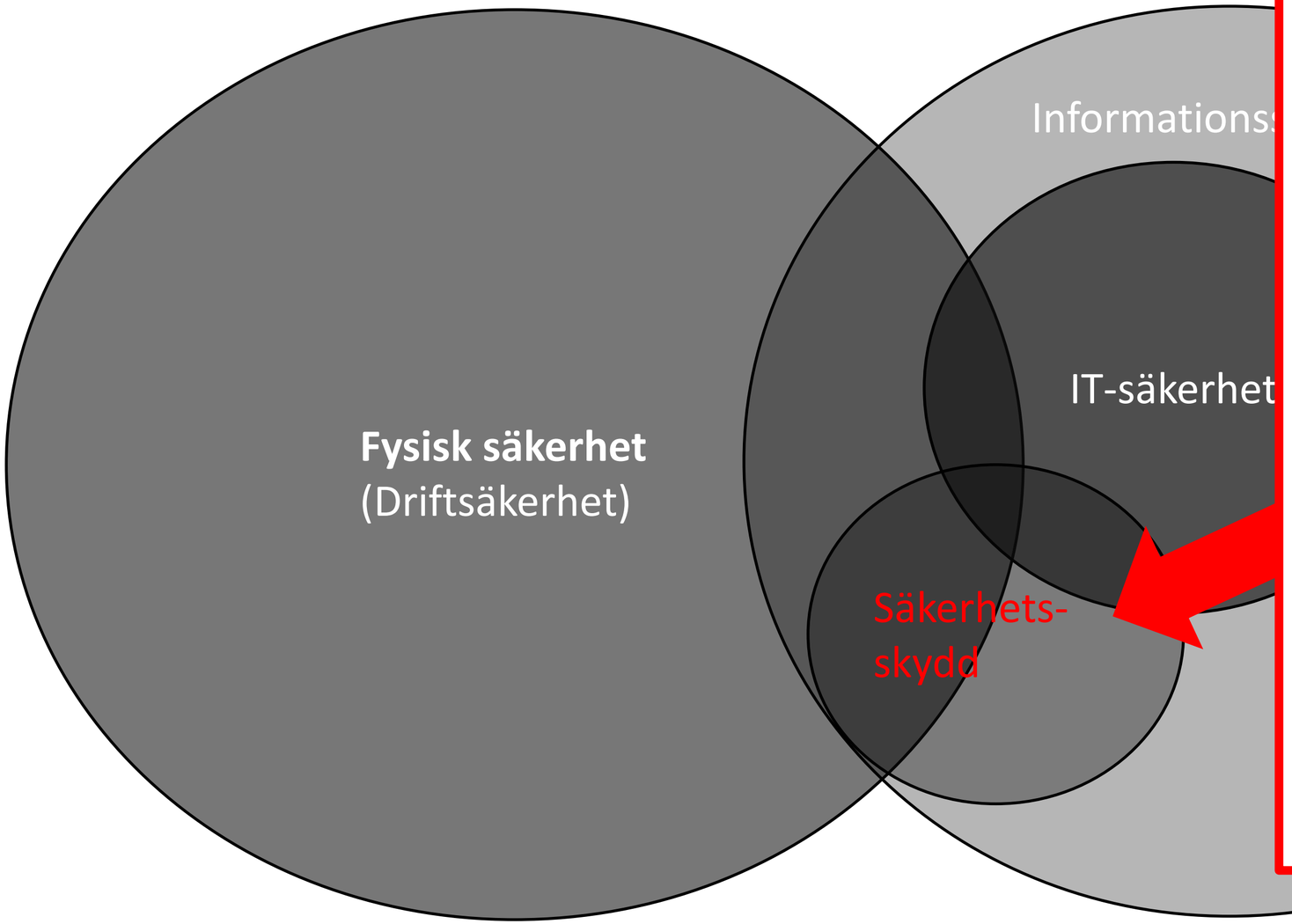
Dokument med information såsom Word, PowerPoint m.m. ska alltid märkas med rätt klassning på samtliga sidor.

Rapporteringsskyldighet

Vid upptäckande av misstänkt bedrägeri, fel och brister avseende säkerhet och system är alla medarbetare skyldig att rapportera upptäckten till säkerhetsansvarig. Exempel på brister, fel och



Säkerhetsområden för nätägare!



- Skydd av säkerhetskänslig verksamhet **(VAD)**
- mot spioneri, sabotage, terroristbrott och andra brott som kan hota verksamheten **(MOT)**
- samt skydd i andra fall av säkerhetsskydds-klassificerade uppgifter **(VAD)**
- Ett system av förebyggande åtgärder **(HUR)**

SÄKERHETSARBETE FÖR NÄTÄGARE AV DIGITAL INFRASTRUKTUR

LAGRUM

Driftsäkerhet
IT-säkerhet
Informationssäkerhet

Säkerhetsskydd

Lagen om elektronisk kommunikation **(LEK) 2003:389**
Förordning om elektronisk kommunikation **2003:396**

PTS Driftsäkerhetsföreskrifter
PTSFS 2015:2 och **PTSFS 2020:1**

Offentlighets- och sekretesslagen **(OSL) 2009:400**

Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Lag (1992:1403) om totalförsvar och höjd beredskap

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)

Säkerhetsskyddslagen **2018:585**
Säkerhetsförordning **2021:955**
PMFS 2022:1 Säkerhetspolisens föreskrifter om säkerhetsskydd
PTSFS 2021:2 Post- och telestyrelsens föreskrifter om säkerhetsskydd

Risk- och sårbarhetsanalys
På anläggningstillgångar
1

Konsekvensanalys på
Verksamhetsdel nätdrift
2

Säkerhetsskyddsanalys
3

VERKTYG

Åtgärder av olika slag
- Direkta åtgärder
- Schemalagda åtgärder
- Periodiska åtgärder
- Förbättringar
- Förstärkningar

Driftsäkerhet
IT-säkerhet
Informationssäkerhet
Säkerhetsskydd

Driftsplan
Investeringsplan
IT- och infosäkpolicy
Säkerhetsskyddsplan

Risk- och sårbarhetsanalyser
BASHOT TELEKOM

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

Hotkataloger: Allmänt

Hotkatalogen består av:

- Händelserubriker och specifika händelser
- RSA prefix; Hänvisning till excelmall och flik
- Beskrivning av primär skada, funktionsstörning eller avbrott

Var kan jag hitta RSA för specifik händelse

Beskrivningar av skada, störning eller avbrott

Händelserubrik

Specifik händelse

Naturliga händelser	Förb (RSA prefix)	Primär skada, funktionsstörning eller avbrott
Väder (se även PTSFS 2020:1 5§)		
- Storm (vind)		
-- *Fällskador (träd, stam och rotvältor).*	Vä 1	Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftkabel, radiomaster
-- *Erodering (strand)*	Vä 2	Kanalisationrör/kablar, brunnar, skåp, stolplinjer/luftledningar
-- *Vinkelfel antenner och antennbärare*	Vä 3	Radioförbindelser
- Blixtnedslag		
-- *Avbrott i telekablar (direktträff)*	Vä 4	Kanalisationsrör/kabel
-- *Antennsystem*	Vä 5	Signalstyrka
-- *Vegetationsbrand / Undermarksbrand*	Vä 6	Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
- Extrem kyla		En sammanhängande period då dygnets lägsta temperatur är lägre än -25 grader minst 2-3 dagar i sträck". (geografiska utmaningar)
-- *Isbildning Kanalisation*	Vä 7	Kanalisationsrör/kablar, brunnar, skåp
- Skyfall eller långvarig nederbörd		
-- Översvämningar - vatteninträngning- pelartryck	Vä 8	Kanalisationsrör/kablar, brunnar. skåp
-- Erodering- ras och skred	Vä 9	Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar

Hotkatalog: Passiv säker förbindelse

Naturliga händelser	Förb (RSA prefix)	Primär skada, funktionsstörning eller avbrott
Väder (se även PTSFS 2020:1 5§)		
- Storm (vind)		
-- *Fällskador (träd, stam och rotvältor).*	Vä 1	Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftkabel, radiomaster
-- *Erodering (strand)*	Vä 2	Kanalisationrör/kablar, brunnar, skåp, stolplinjer/luftledningar
-- *Vinkelfel antenner och antennbärare*	Vä 3	Radioförbindelser
- Blixtnedslag		
-- *Avbrott i telekablar (direktträff)*	Vä 4	Kanalisationsrör/kabel
-- *Antennsystem*	Vä 5	Signalstyrka
-- *Vegetationsbrand / Undermarksbrand*	Vä 6	Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
- Extrem kyla		En sammanhängande period då dygnets lägsta temperatur är lägre än -25 grader minst 2-3 dagar i sträck". (geografiska utmaningar)
-- *Isbildning Kanalisation*	Vä 7	Kanalisationsrör/kablar, brunnar, skåp
- Skyfall eller långvarig nederbörd		
-- Översvämningar - vatteninträngning- pelartryck	Vä 8	Kanalisationsrör/kablar, brunnar. skåp
-- Erodering- ras och skred	Vä 9	Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
- Snöfall		
-- *Snö på stolplinjer*	Vä 10	Luftledningar
-- *Snö på antenner och antennbärare*	Vä 11	Signalstyrka - Vinkelfel
- Isbildning		Isbildning blir som störst vid lite högre temperatur alltså runt nollan i kombination med hög luftfuktighet.
-- *Isbildning på stolplinjer*	Vä 12	Luftledningar
-- *Isbildning på antenner och antennbärare*	Vä 13	Signalstyrka- Vinkelfel

Skadedjur		Primär skada, funktionsstörning eller avbrott
- *Skador på kanalisation/kablar/tätning*	Sk 1	Kanalisationsrör/kablar anlagda i mark, bro, tunnel, kulvert
Olyckshändelser (oavsiktligt orsakade)	**Förb**	**Primär skada, funktionsstörning eller avbrott**
- Anläggningar/transporter i närmiljön		Transformatorstationer, vindkraftverk, radioanläggningar,
-- Elektromagnetiska störningar	Oh 1	Radioförbindelser
- Grävning		
-- *Skador på kanalisation/kablar*	Oh 2	Förbindelser
- Påkörning		
-- *Skåp/stolpar/ledning/master/brunnar*	Oh 3	Förbindelser
- Telenätsarbeten		Olyckor i eget transmissionsnät
-- *Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation, felaktig/otydlig märkning i skarvenheter, brunnar, skåp*	Oh 4	Förbindelser
- Sitearbeten		Verksamhet i egen site
-- *Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation för kopplingsutrustning*	Oh 5	Förbindelser
-- *Brand (även sekundärskador, gasexplosion och släcksystem)*	Oh 6	Kopplingsutrustning.
- Påverkan från omgivande fastighet		Verksamhet och material i omgivande fastighet (inplacerad site)
-- *Kabelskador tele*	Oh 7	Kanalisationsrör/kablar
-- *Brand*	Oh 8	Kanalisationsrör/kablar

Fysiska attacker/grov brottslig verksamhet/terrorism [se även PTS: Sabotage (PTSFS 2020:1 5§), Intrång (PTSFS 2020:1 5§). Annan yttre påverkan (PTSFS 2020:1 5§)]	**Förb**	**Primär skada, funktionsstörning eller avbrott**
- Sabotage yttre		
-- *Avgrävning/skada på kanalisation/telekablar*	Fa 1	Kanalisationsrör/kablar i: mark, bro, tunnel, kulvert, stolplinje, sjö*
-- *Kapning av telekablar i kabelintag*	Fa 2	Kanalisationsrör/kablar
-- *Stöld av kablar*	Fa 3	Förbindelser
-- *Störsändning*	Fa 4	Radioförbindelser
-- *Radiofrekventa störningar (RFI)*	Fa 5	Radioförbindelser

Hotkatalog: Site och Nod

Naturliga händelser	Site (RSA prefix)	Primär skada, funktionsstörning eller avbrott
Tekniskt fel		
- Tekniskt fel i extern strömförsörjning	Te 1	Elektrisk-och elektronisk utrustning
- Tekniskt fel i intern strömförsörjning	Te 2	Elektrisk-och elektronisk utrustning
- Tekniskt fel i interna elektroniksystem	Te 3	Elektrisk-och elektronisk utrustning
- Tekniskt fel i klimatanläggning	Te 4	Elektrisk-och elektronisk utrustning
- Tekniskt fel i brandanläggning	Te 5	Elektrisk-och elektronisk utrustning
Väder (se även PTSFS 2020:1 5§)		
- Storm (vind)		
-- Avbrott extern strömförsörjning	Vä 1	Elektrisk-och elektronisk utrustning
-- Fällskador (träd och stamvältor).	Vä 2	Teknikbodar
- Blixtnedslag		(till RSA site - åtgärder) Nätfilter. Separation el och telekablar. Transientskydd
-- Avbrott i extern elförsörjning	Vä 3	Elektrisk-och elektronisk utrustning
-- Avbrott i yttre elverk	Vä 4	Elektrisk-och elektronisk utrustning
-- Avbrott i yttre elcentral	Vä 5	Elektrisk-och elektronisk utrustning
-- Överspänning i extern strömförsörjningen	Vä 6	Elektrisk-och elektronisk utrustning
-- Elnätstransienter i extern strömförsörjning	Vä 7	Elektrisk-och elektronisk utrustning
-- Obalans i extern strömförsörning	Vä 8	Elektrisk-och elektronisk utrustning
-- Överspänning via skärmad kabel	Vä 9	Elektrisk-och elektronisk utrustning
-- Överspänning, genom fel i anläggningens jord/potentialutjämning	Vä 10	Elektrisk-och elektronisk utrustning
-- Avbrott i Yttre klimatanläggning)	Vä 11	Elektrisk-och elektronisk utrustning
-- Avbrott radioförbindelse	Vä 12	Elektrisk-och elektronisk utrustning
-- Brand i anläggning	Vä 13	Elektrisk-och elektronisk utrustning, kablar och kopplingsutrustning
-- Vegetationsbrand	Vä 14	Anläggningsskada, elektrisk-och elektronisk utrustning (frätande rök)
-- Elektrostatiska störningar (ESD)	Vä 15	Elektronisk utrustning
- Värmebölja		En sammanhängande period då medeltemperaturen är minst 25.0°C
-- Elbrist	Vä 16	Elektrisk-och elektronisk utrustning
-- Funktionsproblem klimatanläggning	Vä 17	Elektrisk-och elektronisk utrustning. (temperatur, fukt, luftkvaliét, lufttryck)
- Värmetopp - solinstrålning/bränder		> 60 grader. Kan även uppstå vid extrem solstrålning vid kallare temperatur.
-- Funktionsproblem klimatanläggning	Vä 18	Elektrisk-och elektronisk utrustning (temperatur, fukt, luftkvaliét, lufttryck)
- Extrem kyla		En sammanhängande period då dygnets lägsta temperatur är lägre än -
-- Funktionsproblem klimatanläggning	Vä 19	Elektrisk-och elektronisk utrustning
-- Isbildning ventilation	Vä 20	Klimatanläggning (temperatur, fukt, förorenad luft)
-- Elverk kan inte startas	Vä 21	Batteri/bränsle
-- Elbrist	Vä 22	Elektrisk- och elektronisk utrusning
- Skyfall eller långvarig nederbörd		
-- Översvämningar - vatteninträngning	Vä 23	Elektrisk-och elektronisk utrustning, kopplingsutrustning
-- Erodering- ras och skred	Vä 24	Anläggningsskador
- Snöfall		
-- Täppt ventilation	Vä 25	Klimatanläggning. (temperatur, fukt, luftkvaliét, lufttryck)
- Isbildning		Isbildning blir som störst vid lite högre temperatur alltså runt nollan i kombination med hög luftfuktighet.
-- Isbildning på antenner och antennbärare	Vä 26	Fallskador på Site/teknikbod

Skadedjur		Primär skada, funktionsstörning eller avbrott
- Skador i anläggning	Sk 1	Elektrisk-och elektronisk utrustning, kopplingsutrustning.
Olyckshändelser (oavsiktligt orsakade)	**Site**	**Primär skada, funktionsstörning eller avbrott**
-- Elnätstransienter	Oh 1	Elektrisk-och elektronisk utrustning.
-- Explositioner	Oh 2	Elektrisk-och elektronisk utrustning.
- Grävning		
-- Skador på elkablar	Oh 3	Elektrisk-och elektronisk utrustning
- Påkörning		
-- Site	Oh 4	Anläggning
- Elnätsarbeten		Olyckor i anslutet elnät
-- Elavbrott	Oh 5	Elektrisk-och elektronisk utrustning
-- Överspänning	Oh 6	Elektrisk-och elektronisk utrustning
-- Elnätstransienter	Oh 7	Elektrisk-och elektronisk utrustning
-- Obalans i strömförsörning	Oh 8	Elektrisk-och elektronisk utrustning
- Telenätsarbeten		Olyckor i eget transmissionsnät
-- Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation, felaktig/otydlig märkning i skarvenheter, brunnar, skåp	Oh 9	Förbindelser
- Sitearbeten		Verksamhet i egen site
-- Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation för kopplingsutrustning	Oh 10	Förbindelser
-- Elektrostatiska störningar (ESD). Användning av felaktiga verktyg/maskiner	Oh 11	Elektronisk utrustning
-- Elektrostatiska störningar (ESD). Fel i interna system t.ex. växelriktare	Oh 12	Elektronisk utrustning
-- Elavbrott, felaktig bortkoppling/kortslutning	Oh 13	Elektrisk-och elektronisk utrustning
-- Brand (även sekundärskador, gasexplosition och släcksystem)	Oh 14	Elektrisk-och elektronisk utrustning samt kopplingsutrustning.
-- Överhettning (avslagen miljöanläggning)	Oh 15	Elektrisk-och elektronisk utrustning, kopplingsutrustning
-- Vattenskada i vätskebärande installationer	Oh 16	Elektrisk-och elektronisk utrustning, kopplingsutrustning
-- Elektromagnetiska störningar (EMI). Användning av felaktiga verktyg/maskiner	Oh 17	Elektronisk utrustning
- Påverkan från omgivande fastighet		Verksamhet och material i omgivande fastighet (inplacerad site)
-- Elnätstransienter	Oh 18	Elektrisk-och elektronisk utrustning
-- Elektromagnetiska störningar	Oh 19	Elektrisk-och elektronisk utrustning
-- Explositioner	Oh 20	Anläggning
-- Kabelskador el	Oh 21	Elektrisk-och elektronisk utrustning
-- Brand	Oh 22	Anläggning och/eller kanalisationsrör/kablar
-- Vatteninträngning genom släcksystem eller skada på vätskebärande installationer	Oh 23	Elektrisk-och elektronisk utrustning samt kopplingsutrustning

Hotkatalog: Site och Nod - Antagonistiskt

Fysiska attacker/grov brottslig verkasmhet/terrorism (se även PTS: Sabotage (PTSFS 2020:1 5§), Intrång (PTSFS 2020:1 5§). Annan yttre påverkan (PTSFS 2020:1 5§)]	**Site**	**Primär skada, funktionsstörning eller avbrott**
- Sabotage yttre		
-- Sprängning i närmiljön (Polis- brandstationer, bensinstationer, m.m.)	Fa 1	Anläggning och/eller sekundärskador
-- Sprängning site	Fa 2	Anläggning
-- *Skador på matande elsystem*	Fa 3	Elektrisk-och elektronisk utrustning
-- *Skador på elskåp utvändig placering*	Fa 4	Elektrisk-och elektronisk utrustning
-- *Skador på anslutningshandske för extern kraft*	Fa 5	Elektrisk-och elektronisk utrustning
-- *Avgrävning eller kapning av serviskablar i kabelintag*	Fa 6	Elektrisk-och elektronisk utrustning
-- *Skador på yttre klimatanläggning*	Fa 7	Elektrisk-och elektronisk utrustning
-- *Direktinjesering*	Fa 8	Elektrisk-och elektronisk utrustning
-- *Kapning av telekablar i kabelintag*	Fa 9	Kanalisationsrör/kabel
-- *Avsiktlig anläggningsbrand (även sekundärskador, gasexplosition, släcksystem)*	Fa 10	Elektrisk-och elektronisk utrustning samt kopplingsutrustning
-- *Stöld av utrustning*	Fa 11	Anläggningen. (I särklass vanligast: Stöld av jordlinor/jordnät. Vikigt med rutinmässig kontroll av dessa, minst vartannat år.
-- *Stöld av drivmedel*	Fa 12	Reservelverk.
-- *Kontaminering*	Fa 13	Sekundärskador elektronisk utrustning med fläkt
-- *Elektromagnetisk puls (EMP)*	Fa 14	Elektronisk utrustning
-- *High Power Microwaves (HPM)*	Fa 15	Elektronisk utrustning
- Sabotage i egen site		Inre sabotage i site (inte egen personal)
-- *Obehörigt intrång /Inbrott*	*Fa 16*	
-- *Fysisk skadegörelse (strömförsörjning)*	*Fa 17*	Elektrisk-och elektronisk utrustning
-- *Fysisk skadegörelse (utrustning…)*	*Fa 18*	Elektrisk-och elektronisk utrustning och kopplingsutrustning (ODF/Patch)
-- *(Mord)Brand (även sekundärskador, gasexplosition, släcksystem)*	*Fa 19*	Elektrisk-och elektronisk utrustning och kopplingsutrustning (ODF/Patch)
-- *Vattenskada*	*Fa 20*	Elektrisk-och elektronisk utrustning och kopplingsutrustning (ODF/Patch)
-- *Stöld av utrustning*	*Fa 21*	Elektrisk-och elektronisk utrustning och kopplingsutrustning (ODF/Patch)
-- *Inplacering av enhet för "brottslig aktivitet"*	*Fa 22*	Elektrisk-och elektronisk utrustning
-- *Skadegörelse/stöld inplacerad utrustning*	*Fa 23*	Elektrisk-och elektronisk utrustning och kopplingsutrustning (ODF/Patch)

Site. Ett fysiskt utrymme som innehåller en eller flera noder. Till site räknas bl.a. följande funktioner: skalskydd [*mekaniskt och elektroniskt (övervakning/larm/tillträde)*], elsystem, reservkraftsystem och klimatsystem. *Brandskyddssystem (larm och släcksystem)*
Nod är en spridningspunkt där trafikflöden vidarekopplas koncentreras och/eller fördelas. Kan vara spridningspunkt för fiber eller spridningspunkt där fiber kopplas mot andra typer av nät. ODF och aktiv kommunikationsutrustning är exempelvis placerade i en nod.
Elektrisk utrustning: en anordning, apparat eller annat föremål som producerar, överför, använder eller förbrukar el (Elsäkerhetslag 2016:732)
Elektronisk utrustning. Elektrisk utrustning som innehåller aktiva komponenter.

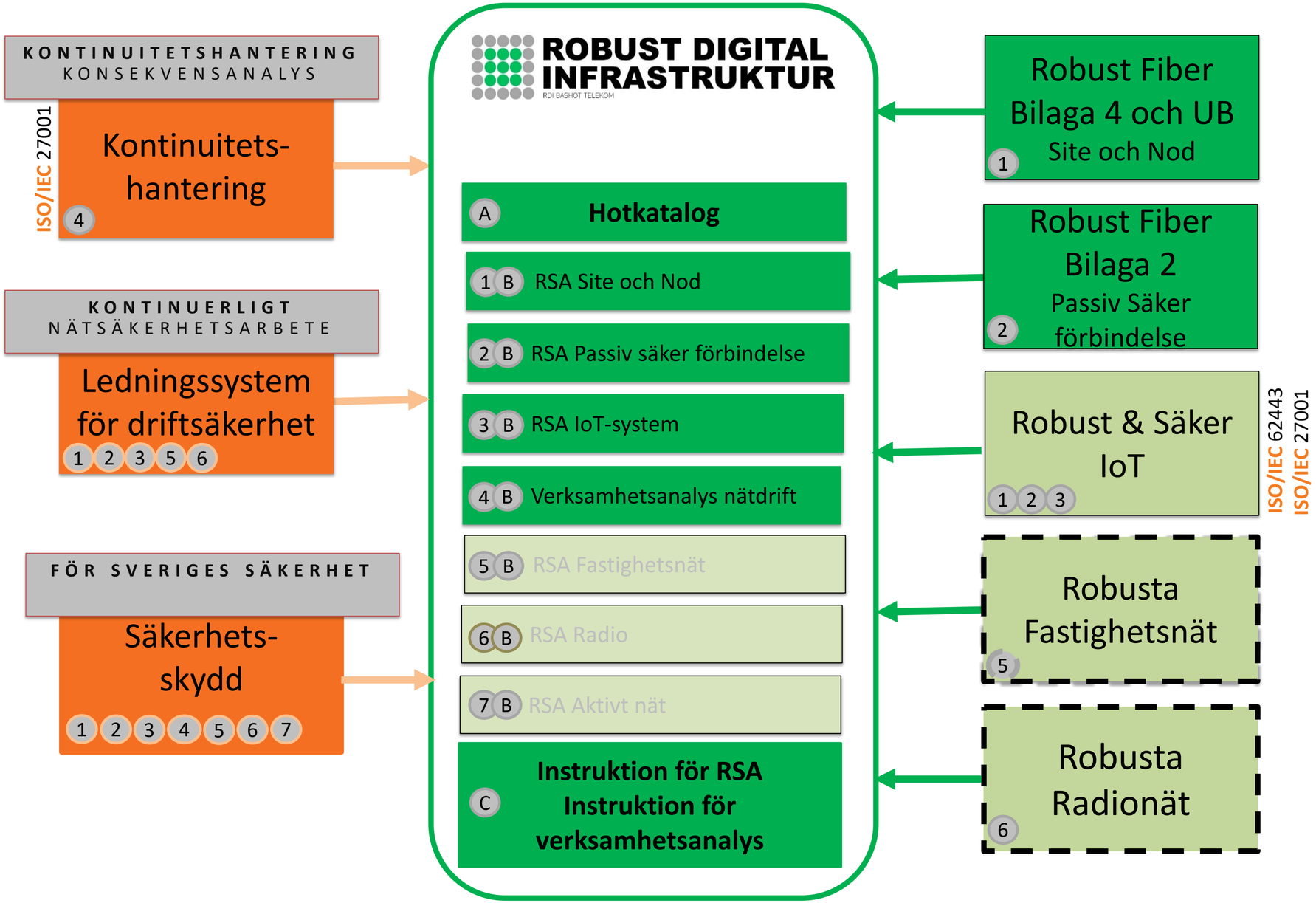
Pågående arbete

- RSA för fasta radionät
- RSA för Fiberbaserade fastighetsnät

Det finns en RSA för IoT men ännu inte inlagd i katalogen

Bladnamn		Definition av de hot som utgör grund för de fördefinerade hotflikarna i arbetsboken	
Prefix	**Index**	**Grupp**	**Hot**
FS	1	**Skadlig aktivitet (Nefarious activity / abuse)**	Kapning av IoT-kommunikationsprotokoll (IoT communication protocol hijacking)
FS	2		Överbelastningsattacker (DDoS)
FS	3	**Avlyssning/inhätning/kapning (Eavesdropping/Interception/Hijacking)**	Attack mot användares integritet (Attacks on privacy)
FS	4		Manipulering av information (Modification of information)
FS	5		Skanning av nätverk (Network reconnaissance)
FS	6		Upprepning av meddelanden (Replay of messages)
FS	7		Skadlig kod (Malware)
FS	8		Kod som utnyttjar svagheter (Exploit Kits)
FS	9		Målinriktade attacker (Targeted attacks)
FS	10		Skador genom förfalskade enheter (Counterfeit by malicious devices)
FS	11		Mannen-i-mitten (Man in the middle)
FS	12		Informationsinsamling (Interception of information)
FS	13		Sessionskapning (Session hijacking)
FS	14		Informationsinsamling (Information gathering)
NH	1	**Fel / Störningar (Failures / Malfunctions)**	Tredje parts fel (Third parties failures)
SF	1	**Skada Förlust (Damage / Loss)**	Sårbarhet i programvara (Software vulnerabilities)
SF	2		Läckage av data/känslig information (Data / Sensitive information leakage)
EO	1	**Katastrof (Disaster)**	Naturkatastrofer (Natural Disaster)
EO	2		Miljökatastrof (Environmental Disaster)
TF	1	**fysiska attacker (Physical attacks)**	Sabotage av enhet/er (Device destruction/sabotage)
TF	2		Enhetsmodifiering (Device modification)
OH	1	**Driftavbrott (Outages)**	Förlust av supporttjänster (Loss of support services)
OH	2		Fel i system (Failure of system)
OH	3		Avbrott i nätverk (Network Outage)
OH	4		Fel på enheter (Failures of devices)

Hotkataloger: Bashot Telekom



Risk- och sårbarhetsanalyser
Execelmallen

IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

Excelmall: Kriterier

Sannolikhet-För att händelsen inträffar	**Mycket hög**	Händelsen kommer nästan säkert att inträffa
	Hög	Händelsen med stor sannolikhet att inträffa
	Medel	Händelsen kan inträffa
	Låg	Händelsen förväntas inte inträffa
	Mycket låg	Händelsen är mycket osannolik
Sannolikhet-För negativa konsekvenser	**Mycket hög**	Om händelsen inträffar är det närmast säkert att händelsen får negativa konsekvenser.
	Hög	Om händelsen inträffar är det sannolikt att händelsen får negativa konsekvenser
	Medel	Om händelsen inträffar är det möjligt att händelsen får negativa konsekvenser.
	Låg	Om händelsen inträffar är det osannolikt att händelsen får negativa konsekvenser
	Mycket låg	Om händelsen inträffar är det mycket osannolikt att händelsen får negativa konsekvenser

Avbrott - Avbrottets geografiska omfattning	**Nationellt**	Avbrottet påverkar stora delar av landet.
	Regionalt	Avbrottet påverkar ett större eller flera mindre områden som sammanlagt motsvarar en mindre del av landet. Exempel: en yta som motsvarar ett läns storlek
	Lokalt	Avbrottet påverkar mindre geografiskt område. Exempel: del av kommunhuvudort.
Avbrott - Avbrottets längd	**Lång**	Avbrottet kan förväntas pågå under längre tid Exempel: avbrottet varar flera dygn
	Medel	Avbrottet kan förvänats pågå under en begränsad tid Exempel: avbrottet varar en stor del av ett dygn
	Kort	Avbrottet kan förväntas pågå under en kort tid Exempel: avbrottet varar någon eller några timmar
Avbrott - Avbrottets omfattning	**Hög**	Avbrottet påverkar en bred skara av samhälleliga kommunikationstjänster hos aktörer med en betydande marknadsandel inom det berörda området
	Medel	Avbrottet påverkar ett antal aktörer med en begränsad sammanlagd marknadsandel och delar av det samhällsviktiga tjänsteutbudet
	Låg	Aktörer med en mindre sammanlagd marknadsandel påverkas av avbrottet som samtidigt påverkar delar av det samhällsviktiga tjänsteutbudet

Samhällskonsekvenser	**Mycket hög**	Katastrofala direkta eller mycket stora indirekta hälsoeffekter, extrema störningar i samhällets funktionalitet, grundmurad misstro mot samhällsinstitutioner och allmän instabilitet, katastrofala skador på egendom och miljö
	Hög	Mycket stora direkta eller betydande indirekta hälsoeffekter, mycket allvarliga störningar i samhällets funktionalitet, bestående misstro mot flera samhällsinstitutioner och förändrat beteende, mycket allvarliga skador på egendom och miljö
	Medel	Betydande direkta eller måttliga indirekta hälsoeffekter, allvarliga störningar i samhällets funktionalitet, bestående misstro mot flera samhällsinstitutioner eller förändrat beteende, allvarliga skador på egendom och miljö
	Låg	Måttliga direkta hälsoeffekter, begränsade störningar i samhällets funktionalitet, övergående misstro mot flera samhällsinstitutioner, begränsade skador på egendom och miljö
	Mycket låg	Små direkta hälsoeffekter, mycket begränsade störningar i samhällets funktionalitet, övergående misstro mot enskild samhällsinstitution, mycket begränsade skador på egendom och miljö
Osäkerhet	**Hög**	Osäkerheten i bedömningen av hotet bedöms som hög, d v s ytterligare arbete behöver utföras för att få en säkrare bedömning
	Medel	Osäkerheten i bedömningen av hotet bedöms som 50/50
	Låg	Osäkerheten i bedömningen av hotet bedöms som låg

Excelmall: Flik för bashot

Bladnamn		Definition av de hot som utgör grund för de fördefinerade hotflikarna i arbetsboken			Fliken är ej tillämpbar på objektet
Prefix	Index	Grupp	Hot	ölj (	Anledning till bedömning
Vä	1	Naturliga händelser	Väder (PTSFS 2020:1 5§): Storm (vind) - Fällskador (träd, stram och rotvältor)		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftkabel, radiomaster
Vä	2	Genererar yttre hot	Väder (PTSFS 2020:1 5§): Storm (vind) - Erodering		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
Vä	3		Väder (PTSFS 2020:1 5§): Storm (vind) - Vinkelfel antenner och antennbärare		Radioförbindelser
Vä	4		Väder (PTSFS 2020:1 5§): Blixtnedslag - Avbrott i telekablar (direktträff)		Kanalisationsrör/kabel
Vä	5		Väder (PTSFS 2020:1 5§): Blixtnedslag -Antennsystem (direktträff)		Signalstyrka
Vä	6		Väder (PTSFS 2020:1 5§): Blixtnedslag -Vegetationsbrand		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
Vä	7		Väder (PTSFS 2020:1 5§): Extrem kyla -Isbildning kanalisation		Kanalisationsrör/kablar, brunnar, skåp
Vä	8		Väder (PTSFS 2020:1 5§): Skyfall eller långvarig nederbörd -Översvämmningar - vatteninträngning - pelartryck		Kanalisationsrör/kablar, brunnar, skåp
Vä	9		Väder (PTSFS 2020:1 5§): Skyfall eller långvarig nederbörd - Erodering / ras / Skred		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
Vä	10		Väder (PTSFS 2020:1 5§): Snöfall - Snö på stolplinjer		Luftledningar
Vä	11		Väder (PTSFS 2020:1 5§): Snöfall - Snö på antenner antennbärare		Signalstyrka - Vinkelfel
Vä	12		Väder (PTSFS 2020:1 5§): Isbildning - Isbildning på stolplinjer		Luftledningar
Vä	13		Väder (PTSFS 2020:1 5§): Isbildning på antenner och antennbärare		Signalstyrka - Vinkelfel
Sk	1	Skadedjur	Skadedjur: Skador på kanalisation/kablar/tätning		Kanalisationsrör/kablar anlagda i mark, bro, tunnel, kulvert.
Oh	1	Olyckhändelser (oavsiktligt orsakade)	Anläggningar/Transport i närmiljön: Elektromagnetiska störningar		Radioförbindelser
Oh	2		Grävning: Skador på kanalisation/kablar		Förbindelser
Oh	3		Påkörning: Skador på skåp/stolpar/ledning/master/brunnar		Förbindelser
Oh	4		Telenätsarbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation, felaktig/otydlig märkning i skarvenheter, brunnar skåp		Förbindelser
Oh	5		Sitearbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation för kopplingsutrustning		Förbindelser
Oh	6		Sitearbeten: Brand (även sekundärskador, gasexplosition och släcksystem)		Kopplingsutrustning
Oh	7		Påverkan från omgivande fastighet: Kabelskador tele		Kanalisationsrör/kablar
Oh	8		Påverkan från omgivande fastighet: Brand		Kanalisationsrör/kablar
Fa	1	Fysiska attacker	Sabotage: Avgrävning/skada på kanalisation/telekablar		Kanalisationsrör/kablar i: mark, bro, tunnel, kulvert, stolplinje, sjö
Fa	2	Grov brottslig verksamhet/terrorism	Sabotage: Kapning av telekablar i kabelintag		Kanalisationsrör/kabel
Fa	3		Sabotage: Störsändning		Radioförbindelser
Fa	4		Sabotage: Radiofrekventa störningar (RFI)		Radioförbindelser
Fa	5		Stöld: Kablar		Förbindelser

Excelmall: Framsidan

Hot. Detaljer finns i flikar.

Summering Risk och sannolikhet

RISK- OCH SÅRBARHETSANALYS

Passiv säker förbindelse

Ver 1.0

ROBUST DIGITAL INFRASTRUKTUR

RDI BASHOT TELEKOM

Objekt:	trrunk CC101- OEW22
Beskrivning:	Trunk mellan två huvudsiter med meetMe. Kategori S3
Upprättad:	2022-05-18
Av:	Jimmy Persson

Reviderad:	
Av:	

Revision:	0.1

Administrativa detaljer.
Objektsnamn, beskrivning

Uppdatera sammanställning

Vid klick så uppdateras tabeller Hot, Risk och Sannolikhet

Börja med att arbeta igenom nivåerna för Sannolikt/Konsekvens (klicka på rubrikraden) och se om de är användbara för er. Egna definitioner anges på bladet Kriterier i resp. fält.

Ta en kopia av bladet **"Mall"** för varje enskilt identifierat hot mot objektet och arbeta därefter igenom respektive blad.

Tryck på knappen **"Uppdatera sammanställning"** för att uppdatera listan med hot och de bedömningar ni kommit fram till.

SAMMANSTÄLLNING AV HOT

Hot	Risk	Sannolikhet
Väder (PTSFS 2020:1 5§): Storm (vind) - Fällskador (träd, stram och rotvältor)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Erodering (strand)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Vinkelfel antenner och antennbärare	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Blixtnedslag - Avbrott i telekablar (direktträff)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Blixtnedslag - Antennsystem (direktträff)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Blixtnedslag -Vegetaionsbrand/Undermarksbrand	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Extrem kyla -Isbildning kanalisation	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Skyfall eller långvarig nederbörd -Översvämmningar - vatteninträngning - pelartryck	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Skyfall eller långvarig nederbörd - Erodering- ras och skred	Mycket Låg	Mycket Låg
…§): Snöfall - Snö på stolplinjer	Mycket Låg	Mycket Låg
…§): Snöfall - Snö på antenner och antennbärare	Mycket Låg	Mycket Låg
…§): Isbildning - Isbildning på stolplinjer	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Isbildning - Isbildning på antenner och antennbärare	Mycket Låg	Mycket Låg
Skadedjur: Skador på kanalisation/kablar	Mycket Låg	Mycket Låg
Anläggningar/Transport i närmiljön: Elektromagnetiska störningar	Mycket Låg	Mycket Låg
Grävning: Skador på kanalisation/kablar	Mycket Låg	Mycket Låg
Påkörning: Skador på site/skåp/stolpar/ledning	Mycket Låg	Mycket Låg
Telenätsarbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentatio, felaktig/otydlig märkning i skarvenheter, brunnar, skå	Mycket Låg	Mycket Låg
Sitearbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation för kopplingsutrustning	Mycket Låg	Mycket Låg
Sitearbeten: Brand (även sekundärskador, gasexplosition och släcksystem)	Mycket Låg	Mycket Låg
Påverkan från omgivande fastighet: Kabelskador tele	Mycket Låg	Mycket Låg
Påverkan från omgivande fastighet: Brand	Mycket Låg	Mycket Låg
Sabotage: Avgrävning/skada på kanalisation/telekablar	Mycket Låg	Mycket Låg
Sabotage: Kapning av telekablar i kabelintag	Mycket Låg	Mycket Låg
Stöld: Kablar	Medel	Medel
Sabotage: Störsändning	Mycket Låg	Mycket Låg
Sabotage: Radiofrekventa störningar (RFI)	Mycket Låg	Mycket Låg

Sammanställning | Vä 1 | Vä 2 | Vä 3 | Vä 4 | Vä 5 | Vä 6 | Vä 7 | Vä 8 | Vä 9 | Vä 10 | Vä 11 | Vä 12 | Vä 13 | Sk 1 | Oh1 | Oh 2 | Oh 3 | Oh 4 | Oh 5 | Oh 6 | Oh 7 | Oh 8 | Fa 1 | Fa 2 | Fa 3 | Fa 4 | Fa 5 | Krite …

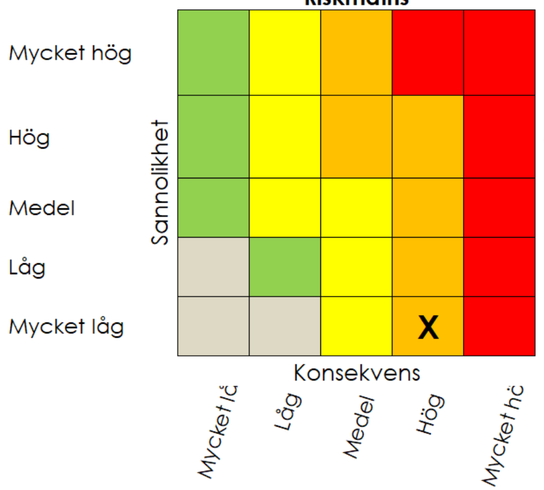
Excelmall: Analysflik för hot

Benämning	**Väder (PTSFS 2020:1 5§): Storm (vind) - Fällskador (träd, stram och rotvältor)**
Beskrivning	Naturliga händelser. Genererar yttre hot

Analys görs genom dubbelklick på alternativ i denna box

Sannolikhet					
Händelsen inträffar	Mycket låg	Låg	Medel	Hög	Mycket hög
För negativa konsekvenser	Mycket låg	Låg	Medel	Hög	Mycket hög
Tekniska konsekvenser					
Avbrottets geografiska omfattning			Lokalt	Regionalt	Nationellt
Avbrottets förväntade längd			Kort	Medel	Lång
Avbrottets omfattning			Låg	Medel	Hög
Samhällskonsekvenser	Mycket låg	Låg	Medel	Hög	Mycket hög
Osäkerhet			Låg	Medel	Hög

Riskmatris



Krysset i riskmatrisen flyttas automatiskt efter val av sannolikhet och tekniska konsekvenser.

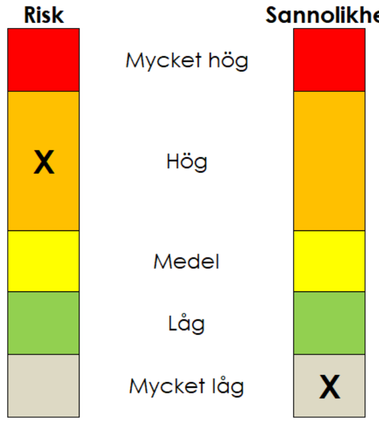
Minnesanteckningar:

Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftkabel, radiomaster

Konsekvenser av det inträffade Konsekvenser kan exempelvis vara verksamhets, ekonomiska,goodwill med flera	
1	Avbrott i trafik.
2	Otillgänglig förbindelse
3	
4	
5	
6	
7	
8	
9	
10	

Beskriv konsekvensen om hotet händer.

Krysset i riskmatrisen flyttas automatiskt efter val av sannolikhet och tekniska konsekvenser.



Krysset i riskmatrisen flyttas automatiskt efter val av sannolikhet och tekniska konsekvenser.

Till Startsidan

Nuvarande skydd	
1	Extra kanalisationsskydd
2	
3	
4	
5	
6	

Ytterligare skydd som behövs	
1	Flytt av förbindelse till bättre geografi
2	
3	
4	
5	
6	

Beskriv åtgärder för att minimera hotet!

Excelmall: Efter uppdatera!

Summering Risk och sannolikhet

RISK- OCH SÅRBARHETSANALYS

Passiv säker förbindelse

Ver 1.0

ROBUST DIGI INFRASTRUK

RDI BASHOT TELEKOM

Objekt:	trrunk CC101- OEW22
Beskrivning:	Trunk mellan två huvudsiter med meetMe. Kategori S3
Upprättad:	2022-05-18
Av:	Jimmy Persson

Reviderad:	
Av:	

Revision:	0.1

Uppdatera sammanställning

Börja med att arbeta igenom nivåerna för Sannolikt/Konsekvens (klicka på rubrikraden) och se om de är användbara för er. Egna definitioner anges på bladet Kriterier i resp. fält.

Ta en kopia av bladet **"Mall"** för varje enskilt identifierat hot mot objektet och arbeta därefter igenom respektive blad.

Tryck på knappen **"Uppdatera sammanställning"** för att uppdatera listan med hot och de bedömningar ni kommit fram till.

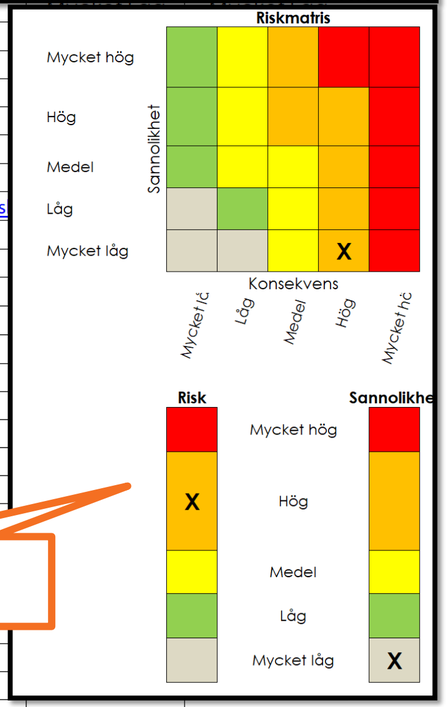
SAMMANSTÄLLNING AV HOT

Hot	Risk	Sannolikhet
Väder (PTSFS 2020:1 5§): Storm (vind) - Fällskador (träd, stram och rotvältor)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Erodering (strand)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Vinkelfel antenner och antennbärare	Mycket Låg	Mycket Låg

SAMMANSTÄLLNING AV HOT

Hot	Risk	Sannolikhet
Väder (PTSFS 2020:1 5§): Storm (vind) - Fällskador (träd, stram och rotvältor)	Hög	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Erodering (strand)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Vinkelfel antenner och antennbärare	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Snöfall - Snö på antenner och antennbärare		
Väder (PTSFS 2020:1 5§): Isbildning - Isbildning på stolplinjer		
Väder (PTSFS 2020:1 5§): Isbildning - Isbildning på antenner och antennbärare		
Skadedjur: Skador på kanalisation/kablar		
Anläggningar/Transport i närmiljön: Elektromagnetiska störningar		
Grävning: Skador på kanalisation/kablar		
Påkörning: Skador på site/skåp/stolpar/ledning		
Telenätsarbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentatio, felaktig/otydlig märkning i skarvenheter, brunnar, s		
Sitearbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation för kopplingsutrustning		
Sitearbeten: Brand (även sekundärskador, gasexplosition och släcksystem)		
Påverkan från omgivande fastighet: Kabelskador tele		
Påverkan från omgivande fastighet: Brand		
Sabotage: Avgrävning/skada på kanalisation/telekablar		
Sabotage: Kapning av telekablar i kabelintag		
Stöld: Kablar		
Sabotage: Störsändning		
Sabotage: Radiofrekventa störningar (RFI)		

Ny status på risk.
Från Mycket låg till hög



Ny status på risk.
Från Mycket låg till hög

Sammanställning | Vä 1 | Vä 2 | Vä 3 | Vä 4 | Vä 5 | Vä 6 | Vä 7 | Vä 8 | Vä 9 | Vä 10 | Vä 11 | Vä 12 | Vä 13 | Sk 1 | Oh1 | Oh 2 | Oh 3 | Oh 4 | Oh 5 | Oh 6 | Oh 7 | Oh 8 | Fa 1 | Fa 2 | Fa 3 | Fa 4 | Fa 5 | Krite ...

Risk- och sårbarhetsanalyser
Instruktion för RSA

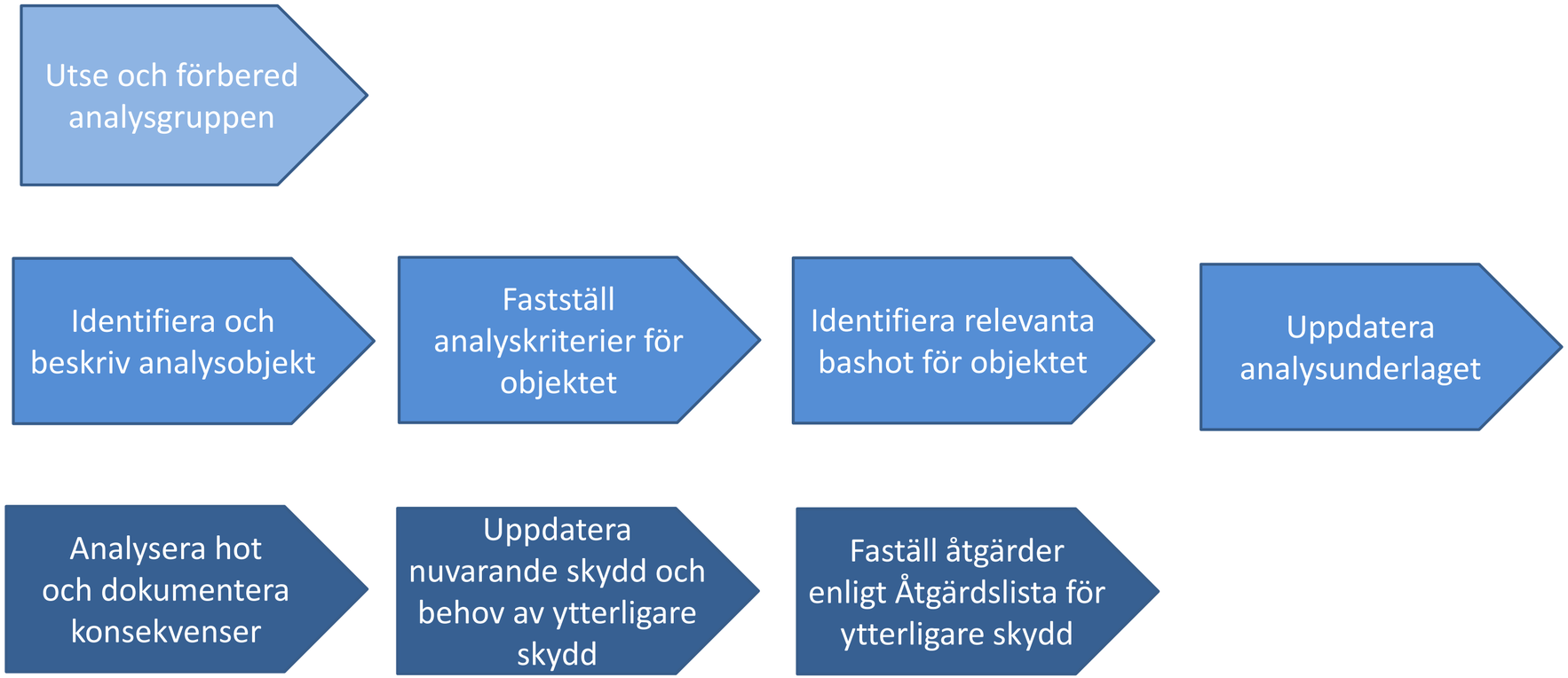
IoT/OT-SÄKERHET

SÄKER FYSISK FÖRBINDELSE

SITE FÖR KRITISK VERKSAMHET

Översikt arbetsgång för Riskanalys och konsekvensanalys

ROBUST DIGITAL INFRASTRUKTUR
RDI BASHOT TELEKOM



ROBUST DIGITAL INFRASTRUKTUR

RDI BASHOT TELEKOM

Instruktion för RSA inom Bashot Telekom

Ver 1.1

INNEHÅLLSFÖRTECKNING

1. **INLEDNING** 4
2. **Referenser** 4
   - 2.1 Referensdokument 4
   - 2.2 Revisionshistorik 4
3. **Omfattning och syfte** 4
   - 3.1 Omfattning 4
   - 3.2 Syfte 4
4. **Avgränsningar** 5
5. **Återkommande RSA** 5
6. **Planerade förändringar** 5
7. **Sekretess** 5
8. **Revidering och ansvar** 5
9. **Handledning risk- och sårbarhetsanalys** 6
   - 9.1 Allmänt 6
   - 9.2 Förberedelser 6
     - 9.2.1 Analysgrupp 6
     - 9.2.2 Lokal och utrustning: 7
     - 9.2.3 Tidsplanering 7
   - 9.3 Metod för RSA 7
     - 9.3.1 Inför genomförandet 7
     - 9.3.2 Metodens delar 8
   - 9.4 Riskhantering och kontinuitetsplanering 11
     - 9.4.1 Riskhantering 11
     - 9.4.2 Kontinuitetsplanering 11
10. **RISk- och sårbarhetsanalys MALL** 12

Instruktion RSA

1. INLEDNING

Detta dokument utgör en rutin och en handledning för Risk- och sårbarhetsanalyser (RSA).

Anm. Benämningar och beteckningar som kan vara unika för olika nätägare anges med (företagsspecifik).

2. REFERENSER

2.1 Referensdokument

Nedanstående referensdokument ska upprättas innan arbetet med risk-och sårbarhetsanalyser genomförs.

Referens	Dokumentnummer, datum
Omvärldsanalys (företagsspecifik)	
Dokumentation och klassificering av analysobjektets tillgångar (företagsspecifik)	
Sammanställning Incidentrapporter (företagsspecifik)	

2.2 Revisionshistorik

Utgåva	Datum	Handläggare	Beskrivning
1.0	2021-12-21	L Björkman	Lansering
1.1	2022-02-03	L Björkman	Justering av avsnitt handledning

3. OMFATTNING OCH SYFTE

3.1 Omfattning

Analyserna ska omfatta:

- Identifiering av samtliga relevanta hot mot det aktuella objektet.
- Kvalificerad bedömning av konsekvenser i händelse av att identifierade risk inträffar
- Kvalificerad bedömning av sannolikheten för att identifierade risker inträffar.
- Kvalificerad sammanvägd bedömning av sannolikheten för att identifierade risker inträffar och de konsekvenser det kan medföra om de inträffar (riskbedömning).
- Åtgärdsförslag på identifierade risker

Vid genomförande av riskanalyser ska utförarna beakta erfarenheter från tidigare inträffade incidenter.

3.2 Syfte

Syftet med risk- och sårbarhetsanalyserna är att minska sårbarheten i analysobjektet.

4. AVGRÄNSNINGAR

Risk- och sårbarhetsanalyserna i detta dokument avser inte:

- kundernas utrustning eller deras hantering/agerande
- drift- och förvaltningsorganisationens interna system och resurser.
- Planerade förändringar som inte påverkar objektets funktion.

5. ÅTERKOMMANDE RSA

Minst en gång per år ska det göras en översyn och bedömning av och om förändringar i omvärld och/eller i företagets tekniska system innebär ett behov av förnyade risk- och sårbarhetsanalyser. Denna riskbedömning ska vara en avvägning mellan vad som kan inträffa, vilka konsekvenser detta kan få och hur troligt det är att det sker. Riskbedömningen ska vara skriftlig. Det ska upprättas en löpande tidplan för återkommande RSA.

Instruktion RSA

6. PLANERADE FÖRÄNDRINGAR

Vid förändringar i företagets tekniska system ska det genomföras en riskbedömning. Denna riskbedömning ska vara en avvägning mellan vad som kan inträffa vad gäller funktionell påverkan, vilka konsekvenser detta kan få och hur troligt det är att det sker.

Metoden för riskbedömningen är den samma som för återkommande RSA med tillägget att riskbedömningen ska vara skriftlig och finnas tillgänglig innan förändringen genomförs. Detta gäller både den förändring som införs i anläggningen och själva jobbet. Utförande tekniker eller beställare ansvarar för att en riskbedömning genomförs.

7. SEKRETESS

Risk- och sårbarhetsanalyserna ska säkerhetsklassas som ”Intern” och hänsyn ska tas till sekretesskrav för gällande lagrum. Intern innebär att informationen endast ska vara tillgänglig för dem som behöver informationen för att kunna fullfölja sina åtaganden rörande ägandeskap, drift och förvaltning av analyserade tillgångar och förbindelser.

8. REVIDERING OCH ANSVAR

Risk- och sårbarhetsanalysen revideras en gång per år eller då väsentliga förändringar gjorts i det elektroniska kommunikationsnätet och/eller de elektroniska tjänsterna. Driftansvarig ansvarar för att detta görs.

9. HANDLEDNING RISK- OCH SÅRBARHETSANALYS

9.1 Allmänt

Risk- och sårbarhetsanalysen ska tydliggöra orsaker till och verkan av olika typer av händelser som kan påverka nätens och tjänsternas funktionalitet negativt. Syftet är att ökad medvetenhet om de egna riskerna, sårbarheterna och förmågan att motstå dessa samt ge underlag för vilka eventuella förbättringsåtgärder som kan vidas för förbygga störningar och avbrott.

Riskanalyser kan göras i många olika situationer och på många olika nivåer. För en verksamhet som helhet, för en särskild informationstillgång, för en specifik applikation, för en serverhall, för en verksamhetsprocess och så vidare. Denna handledning fokuserar på det elektroniska kommunikationsnätet.

Det finns många olika metoder för att göra en riskanalys och det är till stor del ett hantverk som helt enkelt måste utföras av de personer som vet hur fibernäten är anlagda, hur drift och underhåll sköts samt har kunskaper om förvaltningen av nät och tjänster. Att ha goda kunskaper om omgivningarna och de risker som dessa kan utgöra för fibernätens funktionalitet är också viktigt när en riskanalys görs.

9.2 Förberedelser

För att resultaten av risk- och sårbarhetsanalyserna ska bli bra och leda till korrekta förebyggande åtgärder och förbättringsåtgärder krävs förberedelser.

Instruktion RSA

9.2.1 Analysgrupp

En analysledare ska utses som sedan leder den analysgrupp som sätts samman för att genomföra risk och sårbarhetsanalysen.

Analysledaren bör ha vetskap om:

- Hur verksamheten och analysobjektet fungerar på ett övergripande plan
- Hur metoden fungerar
- Vilka som bör ingå i analysgruppen
- Vilket underlag som behövs för analysen
- Vilket resultat som förväntas

Experter av olika slag kan behövas i gruppen, exempelvis inom områden som drift, nätplanering, teknik, ekonomi, säkerhetssamordning, och juridik.

Storleken på analysgruppen kan variera men bör inte vara fler än åtta deltagare eftersom det kan vara svårt att hantera.

En dokumentationsansvarig bör utses och är den som håller i pennan eller IT-stödet, och som måste kunna metoden och de hjälpmedel som används vid analysen.

Inför en riskanalys är det viktigt att ha tillgång till den information som behövs för att lösa uppgiften. Analysledarens uppgift är att se till att medlemmarna i analysgruppen har tagit del av och förberett sig för detta och har tagit reda på alla nödvändiga fakta.

Nödvändig information som ska sammanställas och delges deltagarna inför risk- och sårbarhetsanalysen utgörs av:

- Beskrivning av analysobjektet(n). Aktuella objekt utgörs av definierade tillgångar och förbindelser i enlighet med dokumentet *Dokumentation och klassificering av samtliga tillgångar och förbindelser* (företagsspecifik).
- Författningskrav, föreskrifter och andra styrande dokument som direkt kan påverka riskanalysen
- Statistik som underlättar analysgruppens bedömning
- Liknande riskanalyser som kan vara av stort värde för arbetet
- Allmänna hotbilder som kan vara till stöd och hjälp för att identifiera hot
- Dokument och dokumentation som beskriver aktuella tillgångar och förbindelser.

9.2.2 Lokal och utrustning:

- Bra om det finns en skrivtavla och/eller bläddерblock.
- Bra om det finns datorstöd och projektor.
- Välj gärna en lokal med bra miljö där ni kan arbeta ostört.
- Tryck upp eller skriv upp begrepp och definitioner synligt i lokalen.
- Tryck upp eller rita matrisen i en lämplig storlek.

9.2.3 Tidsplanering

Ta fram en realistisk tidsplan inför analysarbetet. Vissa delar kan visa sig ta längre tid än beräknat, men det är ändå viktigt att ha ett ”grundschema” att falla tillbaka på för att säkert bli klar i tid. Att genomföra den initiala analysen kan ta avsevärd tid så dela upp arbetet i etapper, avsätt tid för flera korta pauser och se till att deltagarna inte springer i väg och jobbar med annat under pauserna. Analysgruppens fokusering är helt avgörande för resultatet.

Exempel på tidsschema för analysen:

Etapp 1

- Inledning med presentation av deltagarna 5–10 minuter
- Genomgång och beskrivning av metoden 10–20 minuter
- Beskrivning av valt analysobjekt 10–30 minuter
- Genomgång av hotlista, lägg till, ta bort, beskriv 30–60 minuter

Etapp 2 (eventuellt uppdelad på två etapper beroende av omfattningen)

- Riskbedömning – konsekvens och sannolikhet 120–240 minuter
- Framtagning av åtgärdsförslag 30–60 minuter

Etapp 3 (eventuellt uppdelad på två etapper beroende av omfattningen)

- Sammanställning av rapport 60–240 minuter

Tidsschema för en RSA, kan vara mycket varierande beroende på objektet och analysgruppens ambitionsnivå.

Instruktion RSA

9.3 Metod för RSA

Metoden som presenteras i det här dokumentet beskriver hur man systematiskt identifierar olika oönskade händelser, bedömer hur troligt det är att händelserna inträffar, bedömer de omedelbara negativa konsekvenserna, analyserar det elektroniska kommunikationsnätets och tjänsternas sårbarheter samt bedömer förmågan att hantera olika påfrestningar.
Metoden bygger på kraven i 27001-standarden och på underlag från MSB (Myndigheten för Samhällsskydd och Beredskap).

9.3.1 Inför genomförandet

Erfarenheterna visar att metodiken inte är det svåra med en analys, utan administrationen. Därför är det väldigt viktigt att följa upp att deltagarna är förberedda och har satt av tid för analysen.
Innan genomförandet av risk- och sårbarhetsanalyser måste man också fastställa vissa utgångspunkter som ska ligga till grund för det fortsatta analysarbetet. Sammanfattningsvis bör risk- och sårbarhetsanalysens utgångspunkter klargöra:

Roll och ansvarsområde
Ansvariga för förvaltning och drift av analysobjekten samt, beroende av analysobjekt, experter inom nätplanering, teknik, säkerhetssamordning, ekonomi och juridik .

Avgränsningar och perspektiv
Det är även viktigt att förstå begreppen risk och sårbarhet för att kunna sätta korrekta avgränsningar och utgå från ett korrekt perspektiv. Följande definitioner har hämtats från PTS, Post och Telestyrelsens Risk- och Sårbarhetsanalys för sektorn elektronisk kommunikation 2015.

Risk = Osäkerhetens effekt på mål
Riskanalys = Process för att förstå riskens natur och för att avgöra risknivån.
Sårbarhet = Kritiskt beroende av en tillgång eller brist i skyddet av en tillgång exponerad för hot.
Resulterande sårbarhet = Sårbarheter som återstår efter införande av skyddsåtgärder

9.3.2 Metodens delar

När analysgruppen är samlad genomförs analysen med hjälp av följande steg som beskrivs mer utförligt under respektive punkt samt i kapitel 9.4.

- **Genomgång av analysobjektet(n)**
- **Identifiera hot**
- **Klassificeringsmodell**
- **Genomför en riskanalys**
- **Sammanställning och rapport**
- **Handlingsplan – åtgärdslista**
- **Riskhantering**
- **Kontinuitetsplanering**

9.3.2.1 *Genomgång av analysobjekt(n)*

Det första steget i arbetet med en risk- och sårbarhetsanalys är att deltagarna gemensamt går igenom objektbeskrivningen för analysobjektet(n), beskrivningen ska vara kortfattad men tydlig nog för andra att förstå utanför analysgruppen.

9.3.2.2 *Identifiera hot*

Ett viktigt moment är att identifiera de hot som finns mot analysobjekten.

Utifrån analysobjektets omfattning görs ett urval av vilka hot (bashot) om kan anses relevanta och dessa ska sedan till ligga grund för risk- och sårbarhetsanalyserna. Urvalet av bashot bör göras för varje nytt analysobjekt. Se figur 1 *Exempel på tabell bashot nedan*.

Vill man själv indentifiera hoten kan man använda sig av "brainstorming" där varje deltagare på en lapp skriver ner hot som kan inträffa eller saker som redan har hänt. Alla hot samlas sedan in och gås igenom.

Det är viktigt att deltagarna försöker beskriva hoten så att alla förstår. Det blir då lättare att bedöma risken i kommande steg. Alla måste förstå och vara överens om innebörden i hoten.

När man arbetar med identifiering av hot bör man tänka på följande:

- Lyssna extra noga på de personer som arbetar aktivt med den berörda verksamheten.
- Vad har hänt som kan hända igen?
- Fokusera på hoten – undvik att tänka i lösningar!
- Undvik för långa diskussioner om det befintliga skyddet.
- Låt alla komma till tals.
- Experter måste tänka på att tala så att alla förstår.

Instruktion RSA

***Figur 1**. Exempel på tabell över bashot.*

Bladnamn		Definition av de hot som utgör grund för de fördefinierade hottlikarna i arbetsboken		Fliken är ej tillämpbar på objektet
Prefix	Index	Grupp	Hot	Dölj (x)	Anledning till bedömning
Vä	1	Naturliga händelser	Väder (PTSFS 2020:1 §§): Storm (vind) - Fälskador (träd, stam och rotvältor)		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftkabel, radiomaster
Vä	2	Genererar yttre hot	Väder (PTSFS 2020:1 §§): Storm (vind) - Erodering		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
Vä	3		Väder (PTSFS 2020:1 §§): Storm (vind) - Vinkelfel antenner och antennbärare		Radioförbindelser
Vä	4		Väder (PTSFS 2020:1 §§): Blixtnedslag - Avbrott i telekablar (direktträff)		Kanalisationsrör/kabel
Vä	5		Väder (PTSFS 2020:1 §§): Blixtnedslag -Antennsystem (direktträff)		Signalstyrka
Vä	6		Väder (PTSFS 2020:1 §§): Blixtnedslag -Vegetationsbrand		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
Vä	7		Väder (PTSFS 2020:1 §§): Extrem kyla -Isbildning kanalisation		Kanalisationsrör/kablar, brunnar, skåp
Vä	8		Väder (PTSFS 2020:1 §§): Skyfall eller långvarig nederbörd -Översvämmningar - vatteninträngning - pelartryck		Kanalisationsrör/kablar, brunnar, skåp
Vä	9		Väder (PTSFS 2020:1 §§): Skyfall eller långvarig nederbörd - Erodering / ras / Skred		Kanalisationsrör/kablar, brunnar, skåp, stolplinjer/luftledningar
Vä	10		Väder (PTSFS 2020:1 §§): Snöfall - Snö på stolplinjer		Luftledningar
Vä	11		Väder (PTSFS 2020:1 §§): Snöfall - Snö på antenner antennbärare		Signalstyrka - Vinkelfel
Vä	12		Väder (PTSFS 2020:1 §§): Isbildning - Isbildning på stolplinjer		Luftledningar
Vä	13		Väder (PTSFS 2020:1 §§): Isbildning på antenner och antennbärare		Signalstyrka - Vinkelfel
Sk	1	Skadedjur	Skadedjur: Skador på kanalisation/kablar/fästning		Kanalisationsrör/kablar anlagda i mark, bro, tunnel, kulvert.
Oh	1	Olyckhändelser (oavsiktligt orsakade)	Anläggningar/Transport i närmiljön: Elektromagnetiska störningar		Radioförbindelser
Oh	2		Grävning: Skador på kanalisation/kablar		Förbindelser
Oh	3		Påkörning: Skador på skåp/stolpar/ledning/master/brunnar		Förbindelser
Oh	4		Telenättsarbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation, felaktig/otydlig märkning i skarvenheter, brunnar skåp		Förbindelser
Oh	5		Sitearbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation för kopplingsutrustning		Förbindelser
Oh	6		Sitearbeten: Brand (även sekundärskador, gasexplosion och släcksystem)		Kopplingsutrustning
Oh	7		Påverkan från omgivande fastighet: Kabelskador tele		Kanalisationsrör/kablar
Oh	8		Påverkan från omgivande fastighet: Brand		Kanalisationsrör/kablar
Fa	1	Fysiska attacker	Sabotage: Avgrävning/skada på kanalisation/telekablar		Kanalisationsrör/kablar i: mark, bro, tunnel, kulvert, stolplinje, sjö
Fa	2	Grov brottslig verksamhet/terrorism	Sabotage: Kapning av telekablar i kabelintag		Kanalisationsrör/kabel
Fa	3		Stöld: Kablar		
Fa	4		Sabotage: Stösändning		Radioförbindelser
Fa	5		Sabotage: Radiofrekventa störningar (RFI)		Radioförbindelser

9.3.2.3 *Klassificeringsmodell*

För att kunna bedöma risken med ett hot görs en sammanvägning av konsekvensen av att hotet inträffar och en bedömning av sannolikheten för att hotet inträffar. För att göra detta krävs att kriterierna för konsekvenser och sannolikhet definieras och beskrivs så att alla i analysgruppen förstår och är överens om innebörden.

Sannolikheten anger hur troligt det är att hotet kommer att inträffa enligt följande kategorier med exempel på definitioner av kriterierna:

- **Mycket låg**
  Händelsen förväntas inte inträffa under den närmaste 20 åren alternativ En gång på 20 år eller obefintlig sannolikhet att händelsen inträffar över huvud taget.
- **Låg**
  Händelsen förvänts inte inträffa under närmaste 10 åren alternativt En gång på 10 år eller mycket sällan.
- **Medel**
  Händelsen kan inträffa alternativt En gång på 5 år eller sällan.
- **Hög**
  Händelsen kommer med stor sannolikhet att inträffa alternativt årligen eller regelbundet,
- **Mycket hög**
  Händelsen kommer nästan säkert att inträffa alternativt Mer än en gång per år eller ofta.

Konsekvensen är ett mått på hur mycket verksamheten skadas om hotet blir verklighet. Påverkan kan exempelvis vara direkt eller indirekt, ekonomisk eller medmänsklig. Modellen innehåller följande fem nivåer med exempel på definitioner av kriterierna:

- **Mycket låg**
  Om händelsen inträffar är det osannolikt att händelsen får negativa konsekvenser eller försumbar skada.
- **Låg**
  Om händelsen inträffar är det möjligt att händelsen får negativa konsekvenser eller måttlig skada.
- **Medel**
  Om händelsen inträffar är det närmast säkert att händelsen får negativa enklare konsekvenser och kan vara en måttlig skada.
- **Hög**
  Om händelsen inträffar är det sannolikt att händelsen får negativa konsekvenser kan vara en betydande skada.
- **Mycket hög**
  Om händelsen inträffar är det närmast säkert att händelsen får negativa konsekvenser kan vara en allvarlig skada.

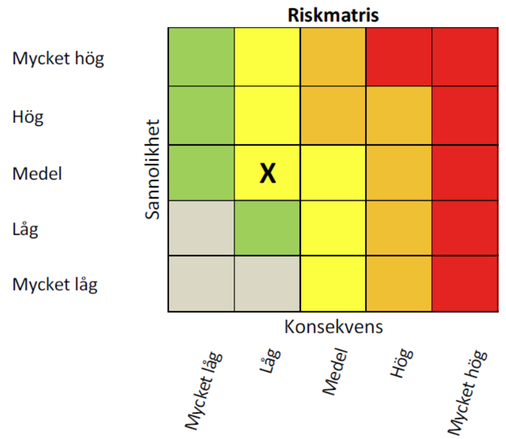
Definitionerna av konsekvens och sannolikhet är ett riktmärke och kan förändras, och det är viktigt att gruppen går igenom definitionerna och ändrar om det behövs. Eventuella förändringar ska dokumenteras och tas med i slutrapporten.

Instruktion RSA

9.3.2.4 *Riskanalys*

När alla kriterier för sannolikheter och konsekvenser är bestämda ska analysgruppen bedöma risken (konsekvensen och sannolikheten) för ett hot, t. ex genom att använda en Konsekvens- och sannolikhetsmatris (fig 2) där man med färger indikerar allvarlighetsgraden av att ett hot inträffar, från grönt (acceptabel risk till röd (måste åtgärdas). Matrisens resultat kan senare att ligga till grund för bland annat prioriteringen av olika åtgärder.

Figur 2. Konsekvens- och sannolikhetsmatris



9.3.2.5 *Sammanställning och rapport*

Resultatet tas sedan om hand av analysledaren som sammanställer en slutgiltig rapport. Förutom själva analysresultatet är det viktigt att rapporten innehåller all tänkbar information, alla avsteg som gruppen har gjort från analysobjektet och eventuella nya definitioner. Rapporten kan också omfatta annan viktig information, till exempel styrdokument, produktbeskrivningar och ritningar som är värdefulla för resultatet.

Det är viktigt att skriva en bra och kortfattad sammanfattning som på ett enkelt sätt beskriver de risker som analysgruppen funnit. Sammanställningen ska även innehålla eventuella förslag till åtgärder och rekommendationer till den som ska fatta besluten.

Rapporten kan dels innehålla generella delar för olika typer av anläggningar och specifika delar för enskild anläggning med särskild hotbild.

Den färdiga slutrapporten ska ut på "remiss" till deltagarna som ska ges möjlighet att ge sina

9.4.1 Riskhantering

Med riskanalysen som utgångspunkt görs en bedömning om risken ska begränsas med skyddsåtgärder eller om den ska accepteras och hanteras i kontinuitetsplanen. Förslag på åtgärder ska dokumenteras i ett dokument, ***Åtgärdsplan riskanalys,*** där en riskansvarig anges samt om möjligt en uppskattad kostnad för respektive åtgärd.

Det finns två sätt att arbeta med åtgärderna.

Alternativ 1: Riskerna ska hanteras senare

Ett alternativ är att riskerna inte ska mötas med några åtgärder ännu utan man förbereder sig endast genom att dokumentera på vilket sätt hotet ska hanteras om det skulle inträffa, det vill säga en kontinuitetsplanering, se avsnitt 9.4.2. Men om deltagarna har bra förslag på åtgärder kan man ändå dokumentera dem.

Alternativ 2: Riskerna ska hanteras nu

Det andra alternativet går ut på att ta hand om riskerna på en gång. Den framtagna matrisen visar vilka hot som är allvarligast – de med högst sannolikhet och störst konsekvenser. Med den informationen som utgångspunkt är det sedan dags att diskutera eventuella åtgärdsförslag och prioritetsordningen för dem. Analysgruppen tar fram ett förslag på lämpliga åtgärder och anger i vilken ordning de bör hanteras.

Beslut om genomförande av åtgärd bör föregås av en riskhanteringsprocess, d.v.s. att bedöma på vilket sätt identifierade risker ska hanteras i verksamheten.

Först efter att en bedömning av kostnaden för genomförande av åtgärder har vägts mot kostnaden för att hantera ett inträffat hot bör beslut tas.

Om beslut fattas om att inte vidta åtgärder ska en kontinuitetsplan upprättas för minimera effekterna om hotet skulle inträffa.

Instruktion RSA

10. RISK- OCH SÅRBARHETSANALYS MALL

Detta avsnitt beskriver handhavandet av ett verktyg för risk- och sårbarhetsanalys (RSA Mall) som kan användas för att dokumentera analysarbetet samt för stöd under genomförandet. Nedan följer en handledning i användandet av verktyget.

Stadsnätsföreningen har erhållit tillstånd från Finspångs Stadsnät, Finet AB och Maintrac AB att tillhandahålla verktyget till Stadsnätsföreningens medlemmar.

Arbetsgång

Analysobjekt

Starta med att identifiera och prioritera de objekt som ska analyseras.

Arbetsdokument

Gör en kopia av Bilaga 1, *Verktyg RSA* för varje objekt som ska analyseras.

Fliken Sammanställning

Under fliken Sammanställning ska valt objekt beskrivas, det ska också framgå när den är upprättad och vem som har upprättat den. Det finns också fält för revideringsdatum, vem som reviderat dokumentet samt ett revisionsnummer.

Figur 3. Exempel på fliken sammanställning

RISK- OCH SÅRBARHETSANALYS
Passiv säker fysisk förbindelse
Ver 1.0
ROBUST DIGITAL INFRASTRUKTUR

Objekt:	
Beskrivning:	
Upprättad:	
Av:	
Reviderad:	
Av:	
Revision:	

Uppdatera sammanställning

Börja med att arbeta igenom nivåerna för Sannolikt/Konsekvens (klicka på rubrikraden) och se om de är användbara för er. Egna definitioner anges på bladet Kriterier i resp. fält.

Ta en kopia av bladet "**Mall**" för varje enskilt identifierat hot mot objektet och arbeta därefter igenom respektive blad.

Tryck på knappen "**Uppdatera sammanställning**" för att uppdatera listan med hot och de bedömningar ni kommit fram till.

SAMMANSTÄLLNING AV HOT		
Hot	Risk	Sannolikhet
Väder (PTSFS 2020:1 5§): Storm (vind) - Fällskador (träd, stram och rotvältor)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Erodering (strand)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Storm (vind) - Vinkelfel antenner och antennbärare	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Blixtnedslag - Avbrott i telekablar (direktträff)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Blixtnedslag - Antennsystem (direktträff)	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Blixtnedslag -Vegetaionsbrand/Undermarksbrand	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Extrem kyla -Isbildning kanalisation	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Skyfall eller långvarig nederbörd -Översvämmningar - vatteninträngning - pelartryck	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Skyfall eller långvarig nederbörd - Erodering- ras och skred	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Snöfall - Snö på stolplinjer	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Snöfall - Snö på antenner och antennbärare	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Isbildning - Isbildning på stolplinjer	Mycket Låg	Mycket Låg
Väder (PTSFS 2020:1 5§): Isbildning - Isbildning på antenner och antennbärare	Mycket Låg	Mycket Låg
Skadedjur: Skador på kanalisation/kablar	Mycket Låg	Mycket Låg
Anläggningar/Transport i närmiljön: Elektromagnetiska störningar	Mycket Låg	Mycket Låg
Grävning: Skador på kanalisation/kablar	Mycket Låg	Mycket Låg
Påkörning: Skador på site/skåp/stolpar/ledning	Mycket Låg	Mycket Låg
Telenätsarbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentatio, felaktig/otydlig märkning i skarvenheter, brunn	Mycket Låg	Mycket Låg
Sitearbeten: Felaktig bortkoppling av förbindelser p.g.a. felaktig dokumentation för kopplingsutrustning	Mycket Låg	Mycket Låg
Sitearbeten: Brand (även sekundärskador, gasexplosition och släcksystem)	Mycket Låg	Mycket Låg
Påverkan från omgivande fastighet: Kabelskador tele	Mycket Låg	Mycket Låg
Påverkan från omgivande fastighet: Brand	Mycket Låg	Mycket Låg
Sabotage: Avgrävning/skada på kanalisation/telekablar	Mycket Låg	Mycket Låg
Sabotage: Kapning av telekablar i kabelintag	Mycket Låg	Mycket Låg
Stöld: Kablar	Medel	Medel
Sabotage: Störsändning	Mycket Låg	Mycket Låg
Sabotage: Radiofrekventa störningar (RFI)	Mycket Låg	Mycket Låg

Instruktion RSA

Fliken Kriterier

Se över kriterierna under fliken "Kriterier" och kontrollera att de är relevanta. Uppdatera vid behov. Under arbetes gång kan definitionerna för kriterierna hämtas genom att dubbelklicka på Konsekvens eller sannolikhet i riskmatrisen.

Anm. Det underlättar om respektive deltagare har en egen sammanställning av kriterierna eller att de presenteras på en separat gemensam skärm.

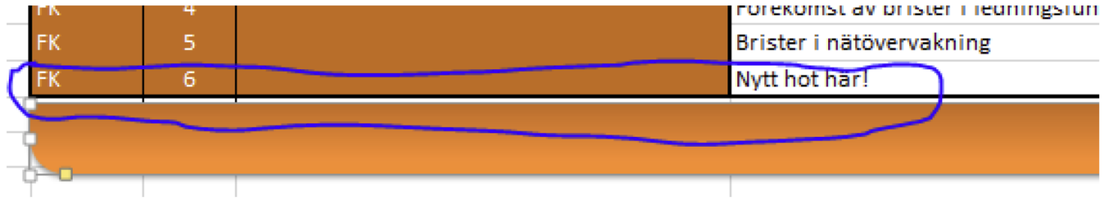
Fliken Bashot

I verktyget är varje hot listad i fliken "Bashot". För varje sådant bashot är det sedan upplagt en separat flik som hanteras i enlighet med rubriken ***Analysera hot*** nedan.

Gå igenom och ta bort de hot/flikar som inte är relevanta för analysen, dokumentera ändringar och tillägg under fliken "Bashot" och gå därefter till fliken "Sammanställning" klicka på knappen **Uppdatera sammanställning** varvid kolumnen *Sammanställning av hot för objekten* uppdateras.

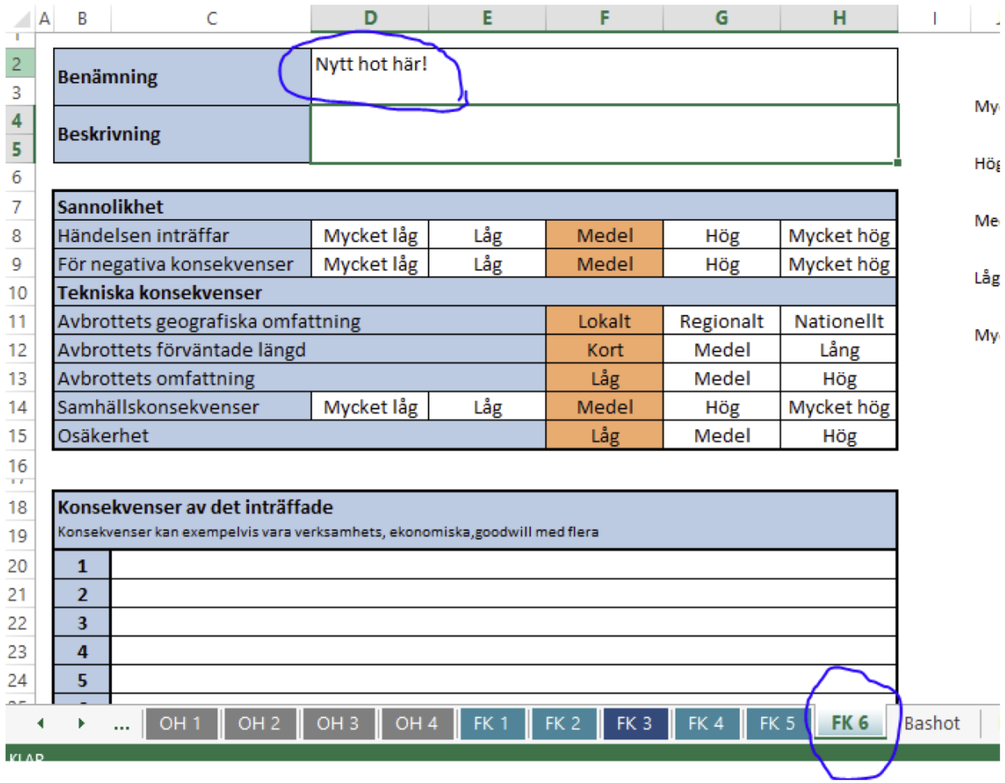
För att skapa ett nytt bashot så lägger du till en rad (Figur 4) med hjälp av "Infoga" i Excel, Ex. FK 6.

Figur 4. Infoga nytt bashot under fliken "Bashot"



Därefter skapar du en ny flik (Figur 5) med samma namn, ex FK 6 och skriver samma Benämning på hotet som du skrev under fliken "Bashot". Du kan med fördel kopiera en befintlig flik. Gå sedan till fliken "Sammanställning" (Figur 6) och tryck på knappen **Uppdatera sammanställning** och det nya bashotet läggs upp i kolumnen *Sammanställning av hot för objekten*.

Figur 5. Ny flik, ex FK 6, Benämning och Fliknamn.



Figur 6. Nytt bashot visas i listan

Instruktion RSA

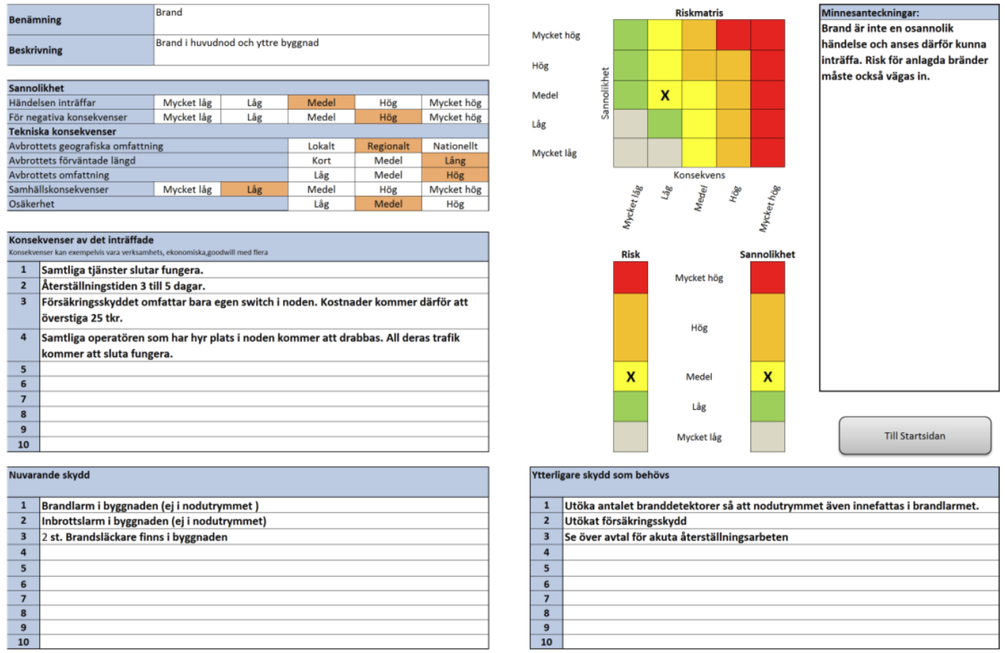
Figur 6. Nytt bashot visas i listan

Analysera hot

Benämning och beskrivning av hotet skrivs in (Figur 7).
Tabellen med sannolikhet och konsekvenser fylls i och i Riskmatrisen kommer ett kryss att automatiskt placeras på rätt plats i matrisen och ge en vägledning till hur låg eller hög risken är.

Sammanfattning av hotet får du genom att titta på Risk och Sannolikhetstaplarna under Riskmatrisen.
Ju mer samhällskonsekvens hotet har desto större risk. Allt utom grönt kräver en åtgärd direkt (röd) eller senare (orange eller gul), detsamma gäller vid Sannolikhet röd, orange, gul eller grön.

Figur 7. Fliken hot



Benämning	Brand
Beskrivning	Brand i huvudnod och yttre byggnad

Sannolikhet					
Händelsen inträffar	Mycket låg	Låg	Medel	Hög	Mycket hög
För negativa konsekvenser	Mycket låg	Låg	Medel	Hög	Mycket hög
Tekniska konsekvenser					
Avbrottets geografiska omfattning			Lokalt	Regionalt	Nationellt
Avbrottets förväntade längd			Kort	Medel	Lång
Avbrottets omfattning			Låg	Medel	Hög
Samhällskonsekvenser	Mycket låg	Låg	Medel	Hög	Mycket hög
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade	
Konsekvenser kan exempelvis vara verksamhets, ekonomiska,goodwill med flera	
1	**Samtliga tjänster slutar fungera.**
2	**Återställningstiden 3 till 5 dagar.**
3	**Försäkringsskyddet omfattar bara egen switch i noden. Kostnader kommer därför att överstiga 25 tkr.**
4	**Samtliga operatören som har hyr plats i noden kommer att drabbas. All deras trafik kommer att sluta fungera.**
5	
6	
7	
8	
9	
10	

Nuvarande skydd	
1	**Brandlarm i byggnaden (ej i nodutrymmet)**
2	**Inbrottslarm i byggnaden (ej i nodutrymmet)**
3	**2 st. Brandsläckare finns i byggnaden**
4	
5	
6	
7	
8	
9	
10	

Ytterligare skydd som behövs	
1	**Utöka antalet branddetektorer så att nodutrymmet även innefattas i brandlarmet.**
2	**Utökat försäkringsskydd**
3	**Se över avtal för akuta återställningsarbeten**
4	
5	
6	
7	
8	
9	
10	

I tabellen *Konsekvenser av det inträffade* dokumenteras konsekvenserna av att ett hot inträffar.

I tabellerna *Nuvarande skydd* och *Ytterligare skydd* anges nuvarande skydd och om det behövs ytterligare skydd för att hantera risken. Anteckningarna i tabellen *Ytterligare skydd* kommer att utgöra underlaget för åtgärder som sammanställs automatiskt i en lista under fliken **Åtgärdslista**. Även anteckningarna i tabellen *Nuvarande skydd* sammanställs automatiskt under fliken **Nuvarande skydd**.

I fältet för minnesanteckningar kan det noteras viktiga saker kring bedömningarna t.ex. hur man kommit fram till bedömningen för sannolikheten.

När analysen är klar klicka på knappen **Till Startsidan** och klicka där på knappen **Uppdatera sammanställning** varvid kolumnerna *Risk* och *Sannolikhet* uppdateras.

Riskhantering och kontinuitetsplanering

Efter analysen använd underlaget för fortsatt riskhantering i enlighet med *kapitel 9.4, Riskhantering och kontinuitetsplanering.*

SÄKERHETSARBETE FÖR NÄTÄGARE AV DIGITAL INFRASTRUKTUR

LAGRUM

Driftsäkerhet
IT-säkerhet
Informationssäkerhet

Säkerhetsskydd

Lagen om elektronisk kommunikation **(LEK) 2003:389**
Förordning om elektronisk kommunikation **2003:396**

PTS Driftsäkerhetsföreskrifter
PTSFS 2015:2 och **PTSFS 2020:1**

Offentlighets- och sekretesslagen **(OSL) 2009:400**

Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Lag (1992:1403) om totalförsvar och höjd beredskap

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)

Säkerhetsskyddslagen **2018:585**
Säkerhetsförordning **2021:955**
PMFS 2022:1 Säkerhetspolisens föreskrifter om säkerhetsskydd
PTSFS 2021:2 Post- och telestyrelsens föreskrifter om säkerhetsskydd

Risk- och sårbarhetsanalys
På anläggningstillgångar
1

Konsekvensanalys på
Verksamhetsdel nätdrift
2

Säkerhetsskyddsanalys
3

VERKTYG

Åtgärder av olika slag
- Direkta åtgärder
- Schemalagda åtgärder
- Periodiska åtgärder
- Förbättringar
- Förstärkningar

Driftsäkerhet
IT-säkerhet
Informationssäkerhet
Säkerhetsskydd

Driftsplan
Investeringsplan
IT- och infosäkpolicy
Säkerhetsskyddsplan

Tack så mycket för att du tittat och lyssnat. Frågor?

Jimmy Persson
Utveckling- och Säkerhetschef
Jimmy.persson@ssnf.org
08-214 640

TLP:WHITE