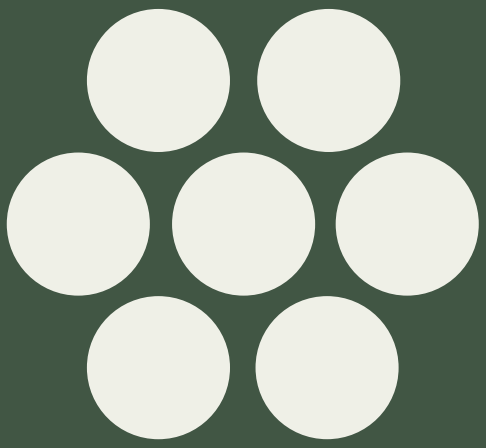
Instruktion för RSA inom Bashot Telekom

Version 2.2



Hotkatalog
Risk- och sårbarhetsanalys

Innehåll

1. Inledning

1.1 Allmänt

Detta dokument utgör en instruktion och handledning för en nätägares Risk- och sårbarhetsanalyser (RSA) och Riskhantering.

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

1.2 Bakgrund

En verksamhetsutövare av kommunikationsnät eller kommunikationstjänster har en skyldighet att upprätta risk- och sårbarhetsanalyser i enlighet Cybersäkerhetslagen (CSL) och Lagen om elektronisk kommunikation (LEK). I LEK används begreppet tillhandahållare vilket motsvarar verksamhetsutövare enligt CSL.

Verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder).

Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken.

Baserat på detta har Svenska Stadsnätsföreningen utarbetat denna **Instruktion för RSA inom Bashot Telekom.**

1.3 Verksamhetsledning

Riskhantering ska utgöra en integrerad del av Verksamhetsutövarens strategiska planering och beslutsfattande.

Verksamhetsledningens roll och förankring av RSA-arbetet är avgörande för att säkerställa effektivitet och genomslagskraft i risk- och sårbarhetsanalysprocessen.

Genom att vara informerad om de identifierade riskerna och delaktig i beslutsprocessen för att vidta lämpliga åtgärder skapar Verksamhetsutövaren en stark kultur för riskmedvetenhet och ansvarstagande på alla nivåer inom organisationen.

1.4 Övergripande planering

Verksamhetsutövaren ska upprätta en *Plan för riskanalyser* och ange vid vilka tidpunkter och i vilka situationer riskanalyser ska genomföras. Riskanalyserna ska genomföras minst en gång per år samt:

1. i samband med att sådana säkerhetsincidenter som ska rapporteras har inträffat
2. inför anskaffning av tillgångar, informationsbehandlingstillgångar, förbindelser och anlitande av uppdragstagare,

3. efter att tidigare okända hot som är relevanta för riskanalysen identifierats
4. inför planerade förändringar.

Verksamhetsutövaren ska inrätta en löpande bevakning och analys av hot och risker i omvärlden.

1.5 Analysobjekt

Analysobjekten omfattar:

Verksamhet nätdrift
Del av verksamhetsutövarens organisation med ansvar för säkerhet, förvaltning och drift av nät, tjänster och relevanta IT-system.

Passiv säker förbindelse
Del av ett allmänt elektroniskt kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett sådant kommunikationsnät.

Site och nod
Ett fysiskt utrymme som innehåller en eller flera noder. Till site räknas bland annat följande funktioner: skalskydd, elsystem, reservkraftsystem och klimatsystem.

IT-system
Sammanhängande helhet av programvara, hårdvara, nätverk och databaser som stödjer en eller flera verksamhetsfunktioner.

Aktiv utrustning
Utrustning i elektroniska nät som bearbetar, förstärker, styr eller omvandlar signaler.

Passiva optiska nät
Ett fibernätverk utan aktiva (strömförsörjda) komponenter mellan site och kund.

Robusta radionät
Med robusta radionät avses trådlös överföring av information mellan fast monterade sändare och mottagare.

Robust och säker IoT
System av sammankopplade sensorer och ställdon vilket möjliggör intelligent informationsinhämtning och styrning.

Robusta Fastighetsnät
Fastighetsnät utgör den sista delen av den infrastruktur som krävs för att en tjänsteleverantör eller operatör ska nå en slutkund.

1.6 Syfte

Syftet med risk- och sårbarhetsanalyserna är att reducera risker, minska sårbarheter och förbättra förmågan att förebygga, motstå och avhjälpa störningar och avbrott samt hantera kriser och extraordinära händelser.

1.7 Avgränsningar

Risk- och sårbarhetsanalyserna i detta dokument avser inte:

- kundernas utrustning eller deras hantering/agerande
- planerade förändringar som inte påverkar kommunikationsnätets funktion.

1.8 Metod

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 nät- och informationsbehandlingstillgångarnas sårbarheter samt bedömer förmågan att hantera olika påfrestningar.
Metoden bygger på kraven i ISO 27001-standarden och på underlag från MCF (Myndigheten för civilt försvar).

RSA-metoden omfattar nedanstående steg:

Figur 1 RSA-metoden

1.9 Sekretess

Det är viktigt att beakta att det ifyllda verktyget enligt kapitel 4 kan innehålla känslig information och att det därför ska hanteras med lämplig försiktighet.
Själva verktyget klassificeras som TLP: Green enligt Trafic Light Protocol (en internationell standard för märkning av säkerhetsklassning av information) medan ifyllda riskanalyser ska klassificeras som TLP: Amber + Strict eftersom de kan innehålla känslig information. Se tabell nedan.

Färg	Definition
TLP:CLEAR	Informationen är opersonlig och kan delas fritt utan begränsningar.
TLP:GREEN	Informationen är begränsat känslig och kan delas med en bredare krets av mottagare. Detta kan inkludera exempelvis kollegor eller andra inom samma bransch.
TLP:AMBER	Informationen är känslig och bör endast delas med de personer eller organisationer som har ett legitimt behov av att känna till den. Detta kan inkludera exempelvis samarbetspartners eller andra relevanta aktörer.
TLP:AMBER+STRICT	Denna information får endast delas med medlemmar inom den egna organisationen. Mottagare kan endast sprida detta på ett behov-av-att-veta-basis endast inom sin organisation.
TLP:RED	Informationen är extremt känslig och bör endast delas med de personer eller organisationer som absolut behöver veta. Detta kan inkludera exempelvis nationella säkerhetsmyndigheter eller andra auktoriserade mottagare.

Tabell 2 Trafic Light Protocol 2.0

OBSERVERA: Material utan märkning betraktas som TLP: CLEAR

2. Definitioner

Hotkategori
Hotkategori är en strukturerad klassificering av identifierade hot och beskriver hotet utifrån fyra nivåer: kategori, typ, källa och hot. Syftet är att skapa en enhetlig struktur för analys, riskvärdering och jämförelse av hot.

- Kategori, övergripande indelning av hot baserat på dess natur eller egenskaper: fysiska hot, logiska hot, organisatoriska hot.
- Typ, hur hotet uppstår: oavsiktligt, avsiktligt
- Källa, vem/vad orsakar hotet: människa, natur, teknik, organisation, flera olika källor
- Hot, själva hotet: grävning, sabotage, intrång, m.m

Påverkan
Den negativa påverkan på verksamhet, leveransförmåga, säkerhet, ekonomi eller förtroende som kan uppstå om en oönskad händelse inträffar.

Risk
En sammanvägd bedömning av sannolikheten att en oönskad händelse inträffar och hur allvarliga konsekvenser den kan medföra för stadsnätets funktion och tillgångar.

Riskanalys
En systematisk metod för att identifiera, värdera och prioritera risker genom bedömning av sannolikhet och konsekvens.

Risk- och åtgärdshantering
En strukturerad process för att besluta om, planera, genomföra och följa upp åtgärder baserat på resultat från riskanalyser, i syfte att reducera risk till acceptabel nivå.

Resulterande sårbarhet (kvarstående sårbarhet)
De svagheter eller riskexponeringar som återstår efter att beslutade skyddsåtgärder har införts.

Sannolikhet
Bedömning av hur troligt det är att ett identifierat hot eller en oönskad händelse inträffar inom en given tidsperiod.

Sårbarhet
En brist, svaghet eller otillräcklig skyddsnivå i teknik, processer, organisation eller kompetens som kan utnyttjas eller leda till störningar i stadsnätets funktion.

Verksamhetsutövare (i LEK användes begreppet tillhandahållare)
Den organisation eller juridiska person som ansvarar för drift, förvaltning och leverans av stadsnätets infrastruktur och tjänster.

3. Förberedelser inför RSA

3.1 Förberedelser

För att risk- och sårbarhetsanalysen (RSA) ska ge ett relevant och användbart beslutsunderlag krävs en strukturerad och väl förankrad förberedelsefas. Arbetet ska planeras så att det stödjer verksamhetens behov av riskhantering, kontinuitet och stärkt robusthet.

Förberedelserna omfattar:

- säkerställande av tillräckliga resurser (kompetens, tid och stödverktyg)
- tydlig metodik och avgränsning av analysen
- koppling till gällande regelverk och interna styrdokument
- samordning med närliggande processer såsom kontinuitetshantering, informationssäkerhet och säkerhetsskydd

Analysen bör utformas så att resultaten kan omsättas i konkreta åtgärder inom både krisberedskap och, där relevant, civilt försvar.

3.2 Analysgrupp och underlag

Analysledare

En analysledare ska utses med ansvar för planering, genomförande och kvalitetssäkring av analysen.

Analysledaren bör ha:

- god förståelse för verksamheten och det aktuella analysobjektet
- kunskap om vald analysmetod
- förmåga att sätta samman en relevant analysgrupp
- överblick över vilka underlag som krävs
- tydlig bild av analysens syfte och förväntade resultat

Analysgrupp

Analysgruppen ska vara ändamålsenligt sammansatt och inte större än att ett effektivt arbete kan bedrivas.

Följande funktioner bör normalt ingå:

- ansvariga för drift och förvaltning av aktuella system och infrastrukturer
- kompetens inom nät/IT/OT, informationssäkerhet och fysisk säkerhet
- verksamhetsrepresentanter
- vid behov kompetens inom juridik, upphandling och ekonomi

Sammansättningen ska spegla både tekniska, organisatoriska och verksamhetsmässiga perspektiv.

Dokumentation

En dokumentationsansvarig ska utses. Denna funktion ansvarar för att:

- dokumentera analysens genomförande och resultat
- säkerställa spårbarhet och kvalitet i underlaget
- hantera använda verktyg och mallar

Underlag

Inför analysen ska relevanta underlag samlas in, kvalitetssäkras och tillgängliggöras för analysgruppen.

Exempel på underlag:

- beskrivning av analysobjekt (tillgångar, funktioner och beroenden), inklusive dokumentation enligt gällande krav i Lagen om elektronisk kommunikation (LEK) och Cybersäkerhetslagen (CSL).
- tillämpliga lagar, föreskrifter och interna styrdokument (t.ex. LEK, säkerhetsskyddslagstiftning, MCF:s föreskrifter)
- tidigare genomförda analyser och uppföljningar
- incidentrapporter, avbrottsstatistik och erfarenheter
- aktuella hot- och riskbedömningar (inklusive cyberhot och antagonistiska hot)

Analysledaren ansvarar för att säkerställa att deltagarna har tillgång till och förståelse för underlaget.

3.3 Lokal och utrustning

- Lokal med bra miljö där ni kan arbeta ostört.
- Tryck upp eller skriv upp begrepp och definitioner synligt i lokalen.

3.4 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.

3.5 Genomförande

Samordna gärna arbetet med annat arbete, till exempel budget- eller verksamhetsplanering

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. *Några tips att beakta under genomförandet är:

- 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.

3.6 Kommunicera resultatet

Gör en utvärdering av de brister som identifierats som en konsekvens av felaktiga lösningar, dålig funktion, otydliga ledningsfunktioner, felaktiga rutiner och/eller handhavande. Dokumentera och kommunicera resultat och åtgärdsförslag till berörda funktioner i enlighet med Rutin för riskrapportering till ledningen.

3.7 Utbildning och övning

Ta fram utbildningar för personalen med inriktning på förbättrad riskmedvetenhet.

Ta fram övningsmoment för att träna på rutiner och/eller handhavande.

4. RSA med hjälp av verktyget

4.1 Allmänt

Genom att noggrant analysera hot, sårbarheter och konsekvenser kan man skapa en helhetsbild av risklandskapet. Denna process ger insikter som möjliggör strategisk planering och implementering av åtgärder för att effektivt minimera och hantera dessa risker, vilket i sin tur säkerställer en pålitlig och säker drift av nät-och informationsbehandlingstillgångar.

Stadsnätsföreningen har bearbetat MCF:s verktyg för risk- och sårbarhetsanalys (RSA) för att möta behoven inom telekomsektorn.

Verktyget Hotkatalog, risk och sårbarhetsanalys har flera tillämpningar med prefabricerade data för hot och riksbeskrivningar för dessa. Verktyg finns för analysobjekt enligt kapitel 1.5.
Utöver dessa dedikerade verktyg finns det också en tom mall som kan användas för behov som inte omfattas av de dedikerade verktygen.

Verktyget *Hotkatalog, risk och sårbarhetsanalys* och mallen finns under
Robust digital infrastruktur - Stadsnätsföreningen

Detta kapitel beskriver steg för steg hur verktyget ska användas vid genomförandet av en risk-och sårbarhetsanalys.
Vid genomförande av riskanalyser ska utförarna beakta erfarenheter från tidigare inträffade incidenter.

4.2 Verktygsöversikt

Verktyget omfattar hotkatalog, riskanalys, åtgärdsförslag och underlag för riskägarens beslut om vilka risker som ska åtgärdas.

Verktyget består av följande flikar:

Info
Här finns kortfattad information om verktyget och dess Informations-säkerhetsklassning.

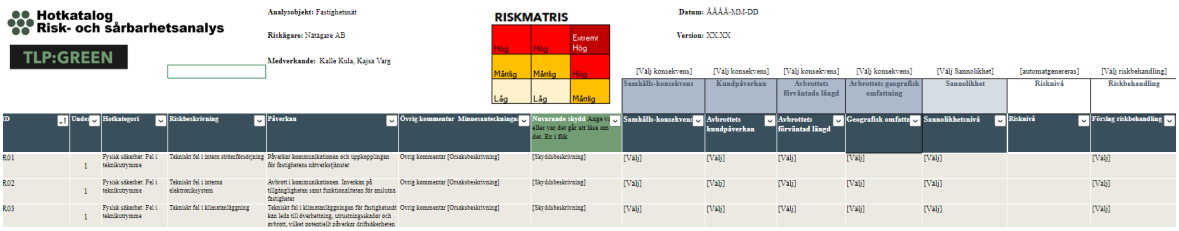
Definitioner och begrepp
Här definieras de begrepp som är aktuella för verktyget.

Riskanalys
Fliken riskanalys är uppdelad på två delar Riskanalys respektive Åtgärdshantering enligt nedanstående bilder.

Riskanalys omfattar de olika stegen för att identifiera relevanta hot, genomföra riskanalyser och för att besluta om lämplig riskbehandling.

Riskanalys omfattar:

- hotkategori (kategori – typ – källa – hot)
- riskbedömning
- riskmatris för att visuellt visa erhållen risknivå
- riskbehandling
- beskrivning av, eller hänvisning till, nuvarande skydd.

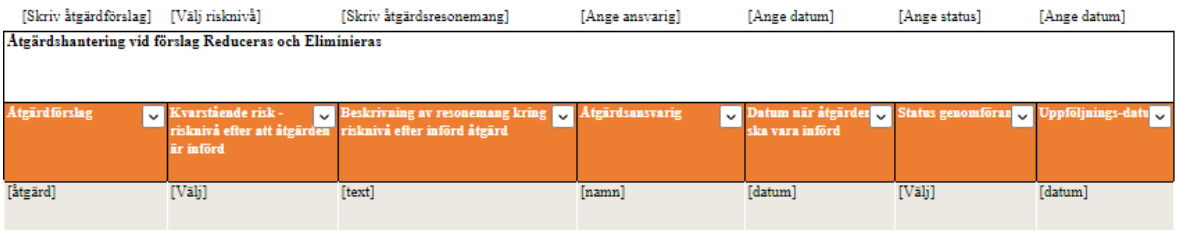


Figur 2 Övergripande bild av riskanalys

Åtgärdshantering används för att ange hur identifierade risker ska åtgärdas, till vilken risknivå risken kommer att minska om åtgärden genomförs samt för att bestämma åtgärdsplan.

Åtgärdshantering omfattar:

- åtgärdsförslag
- åtgärdsplan



Figur 3 Åtgärdshantering

Nuvarande skydd

Nuvarande Skydd används för att beskriva det nuvarande skyddet och tidigare vidtagna skyddsåtgärder.

ID-åtgärd	ID-risk	Riskbeskrivning	Skydd	Ansvarig	Datum när skyddet infördes	Datum uppföljning skydd
S01	[från fliken Riskanalys, kolumn X]	[från fliken Riskanalys]	[åtgärd]	[namn]	[datum]	[datum]
S02			[åtgärd]	[namn]	[datum]	[datum]

Figur 4 Flik Nuvarande skydd

Kriterier för riskbedömning
Kriterier för riskbedömning definierar de kriterier och parametrar som används för att bedöma och klassificera konsekvenser, sannolikhet och risker.

Data
Data redovisar data och formeln för riskanalys. **Uppgifterna används vid beräkning av risknivån och får inte ändras då de påverkar alla beräkningar i verktyget.**

4.3 Att använda verktyget

Detta avsnitt beskriver arbetsgången för en riskanalys med hjälp av ett prefabricerat verktyg *Hotkatalog, risk och sårbarhetsanalys*.

Verktyget kan användas interaktivt, exempelvis genom att projicera det under workshops för att möjliggöra deltagarnas visualisering av arbetsresultatet.

Tänk på att ifyllt verktyg kan vara känsligt och behöver klassas och hanteras i enlighet med kap 1.9 Sekretess.

4.3.1 Identifiera hot och beskriv risker

Det första steget i arbetet med en risk- och sårbarhetsanalys är att deltagarna gemensamt går igenom objektbeskrivningen för analysobjektet(n) i den aktuella tillämpningen till exempel RSA Site och nod. Beskrivningen ska vara kortfattad men tydlig nog för andra att förstå utanför analysgruppen.

Därefter genomförs en hot och riskanalys enligt nedanstående steg:

ID	Under-ID	Hotkategori	Riskbeskrivning
R01	1	Fysiskt hot - Flera möjliga källor - Avbrott i extern strömförsörjning	Avbrott i extern strömförsörjning orsakar bortfall av el till site, vilket påverkar elektriska och elektroniska system.
R02	1	Fysiskt hot - Flera möjliga källor - Överspänning i externt elnät	Överspänning i externt elnät orsakar förhöjda spänningsnivåer

Figur 5 Bashot i verktyget

Kolumn **ID** i verktyget utgörs av ett ID för riskanalysen.

Kolumn **Under ID** används när det finns behov av att definiera flera konsekvenser för samma hot. För att lägga in ett *under ID* kopierar man raden för aktuellt, markerar hela raden under hotet och väljer *Infoga kopierade celler*.

- **Den befintliga raden flyttas ett steg nedåt** och den kopierade raden läggs in.

- **Markera cellen med ID nummer i den kopierade raden**, ändra numret och lägg markören i cellens nedra hörn.

- **Håll in vänster musknapp och dra markeringen i kolumnen ända till sista raden,** släpp knappen och ID kolumnen numreras om.

- **Därefter anges aktuellt under ID i kolumnen**, aktuella kolumner revideras varefter riskanalysen genomförs enligt instruktionen.

Kolumn **Hotkategori** omfattar kategori – typ – källa – hot:

- Kategori (fysiska hot, logiska hot, organisatoriska hot)
- Typ (oavsiktligt, avsiktligt, utelämna vid ej relevant)
- Källa (människa, natur, teknik, organisation, AI, flera olika källor)
- Hot (exempel: grävning, sabotage, intrång, m.m.)

Identifiera relevanta hot och ta bort icke aktuella hot.

- **Om det behövs läggas till nya hot görs det genom att kopiera raden** ovanför den rad där den nya raden ska läggas till.

- **Markera raden där den nya raden ska läggas in** och välj Infoga till kopierade celler.

- **Den befintliga raden flyttas ett steg nedåt** och den kopierade raden läggs in.

- **Markera cellen med ID nummer i den kopierade**, ändra numret och lägg markören i cellens nedra hörn.

- **Håll in vänster musknapp och dra markeringen i kolumnen ända till sista raden**, släpp knappen och ID kolumnen numreras om.

Kolumn **Riskbeskrivning** innehåller prefabricerade beskrivningar av de risker som är förknippade med valt hot. Genomför en bedömning och eventuella justeringar av de risker som kan kopplas till att identifierade hot inträffar.

4.3.2 Beskrivning av påverkan på nät och tjänster

Detta steg omfattar en analys och beskrivning av hur den analyserade risken kan påverka verksamheten.

Påverkan	Övrig kommentar [Minnesanteckningar]
Förlust av anslutning och tjänsteavbrott	Övrig kommentar [Minnesanteckningar]
Påverkan på kommunikation och funktionalitet	Övrig kommentar [Minnesanteckningar]

Figur 6 Beskrivning av påverkan på nät och tjänster

Kolumn **Påverkan** innehåller prefabricerade beskrivningar av den påverkan som den analyserade risken har på verksamheten. Analysera och justera efter egen bedömning baserat på analysobjekt och riskbeskrivningen.
Här är några aspekter som kan inkluderas i en sådan beskrivning:

- Påverkan på prestanda - kan inkludera fördröjningar, långsam dataöverföring eller minskad kapacitet.
- Påverkan på tillgänglighet - kan det leda till avbrott, låg prestanda eller begränsad tillgänglighet?
- Påverkan på integritet - finns det risk för obehörig åtkomst, manipulation eller förlust av information?
- Påverkan på konfidentialitet – här beskrivs hur hotet kan påverka konfidentialitet hos känslig information. Kan det leda till läckage av information eller exponering av känsliga data?
- Potentiella ekonomiska konsekvenserna: det kan inkludera kostnader för reparation, förlorad intäkt, förlorade förtroende från kunder och eventuella rättsliga konsekvenser.

Kolumn **Övrig kommentar** är avsedd för egna kommentarer om riskbeskrivning och påverkan samt minnesanteckningar.

4.3.3 Bedömning av konsekvens och sannolikhet

Detta steg omfattar en bedömning av konsekvenserna om beskrivna hot och risker inträffar och sannolikheten för att detta inträffar.

Först när aktuell ruta markerats finns pil för val nere till höger

[Välj konsekvens]	[Välj konsekvens]	[Välj konsekvens]	[Välj konsekvens]	[Välj Sannolikhet]
Samhällskonsekvens	**Kundpåverkan**	**Avbrottets förväntade längd**	**Avbrottets geografisk omfattning**	**Sannolikhet**
Samhälls-konsekvenser	**Avbrottets kundpåverkan**	**Avbrottets förväntad längd**	**Geografisk omfattning**	**Sannolikhetsnivå**
Medel	Medel	Medel	Lokalt	Medelhög

Figur 7 Bedömning av konsekvenser och sannolikhet

I kolumn **Samhällskonsekvens** görs en bedömning i vilken omfattning som samhället påverkas (mycket låg, låg, medel, hög, mycket hög).

I kolumn **Kundpåverkan** görs en bedömning av i vilken omfattning som kunder påverkas (liten, medel, stor).

I kolumn **Avbrottets förväntade längd** görs en estimerad bedömning av avbrottstid (kort, medel, lång).

I kolumn **Avbrottets geografiska omfattning** görs en bedömning av avbrottets geografiska omfattning (lokalt, regionalt, nationellt).

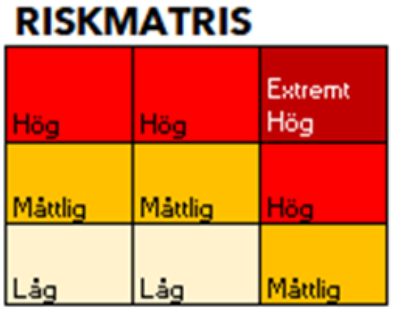
I kolumn **Sannolikhet** görs en bedömning av sannolikheten för att hotet inträffar (låg, medelhög, hög, mycket hög).

4.3.4 Bedöm risknivå

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. Risknivån beräknas automatiskt med hjälp av verktyget och presenteras med färg i tabellen och med motsvarande färg i riskmatrisen, se bild 10 nedan.

Figur 8 Risknivå

I kolumn **Risknivå** presenteras den beräknade risknivån (beräkning sker automatiskt). Definitionen av risk inom ramen för riskbedömning är: Risk=Konsekvens*Sannolikhet



Figur 9 Riskmatris

4.3.5 Förslag på riskbehandling

I detta steg görs en bedömning av hur ska analyserad risknivå ska behandlas.

Figur 10 Riskbehandling

I kolumn **Riskbehandling** anges hur den beräknade risknivån ska behandlas

Generell kan man utgå från att risknivåerna måttlig, hög och extremt hög risk alltid kräver åtgärder.

Här är några aspekter på de val som kan väljas under kolumnen:

- **Acceptera:** Om risken bedöms som acceptabel och dess konsekvenser inte anses alltför allvarliga, kan det vara lämpligt att acceptera risken utan ytterligare åtgärder. Detta kan vara fallet om kostnaderna för att behandla risken överstiger dess potentiella påverkan.
- **Reducera:** Om risken är för hög och dess konsekvenser är oacceptabla, kan behandlingsstrategin vara att reducera risken. Detta kan innebära att implementera förebyggande åtgärder eller kontroller för att minska sannolikheten eller konsekvenserna av risken.
- **Eliminera:** Om risken anses oacceptabel och inte kan tolereras, kan eliminering vara den föreslagna behandlingsåtgärden. Detta innebär att identifiera och eliminera grundorsaken till risken för att förhindra dess uppkomst.
- **Överföra:** Ibland kan det vara strategiskt att överföra risken till en tredje part, till exempel genom försäkring eller kontraktsavtal. Detta minskar organisationens direktansvar för risken.

4.3.6 Risk-och åtgärdshantering

Åtgärdsförslag

I detta steg identifierar man lämpliga åtgärder för att hantera angivet val från riskbehandlingen samt för att göra en bedömning av eventuellt kvarstående risker efter genomförda åtgärder.

Åtgärdförslag	Kvarstående risk - risknivå efter att åtgärden är införd	Beskrivning av resonemang kring risknivå efter införd åtgärd
[åtgärd]	[Välj]	[text]

Figur 11 Åtgärdsförslag

Kolumnen **Åtgärdsförslag** används för att ange de åtgärder som är lämpliga utifrån förslaget på riskbehandling. Använd riskanalysen för att utvärdera åtgärdsförslagen.

Kolumnen **Kvarstående risknivå** används för att göra en analys av den kvarstående risknivån efter ett införande av föreslagna åtgärder. Analysen baseras på fyra fördefinierade risknivåer enligt nedan:

- **Låg risknivå** - Åtgärderna skulle minska risken till en nivå där den anses vara försumbar eller mycket låg.

- **Måttlig risknivå** - Åtgärderna skulle ge en viss effekt och minska risken till en acceptabel nivå, men det finns fortfarande en märkbar osäkerhet. *En översyn av åtgärdsförslagen bör göras.*
- **Hög risknivå** - Åtgärderna skulle endast ha en begränsad effekt, och risken skulle kvarstå på en betydande nivå och kräva ytterligare insatser. *Risknivån kräver en översyn av åtgärdsförslagen.*
- **Extremt hög risknivå** - Åtgärderna skulle ha en minimal eller ingen påverkan på risken, och den skulle kvarstå på en kritisk nivå och kräva omedelbara och omfattande åtgärder. *Risknivån kräver en översyn av åtgärdsförslagen.*

Kolumn **Beskrivning av resonemang kring risknivå efter införd åtgärd** används för att beskriva argumenten för den valda risknivån. Om det behövs mer utrymme för anteckningar, finns det möjlighet att placera anteckningar i en separat ruta "Minnesanteckningar" till höger från tabellen.

4.3.7 Åtgärdsplan

En åtgärdsplan för beslutade åtgärder fastställs och integreras i Verksamhetsutövarens verksamhetsplan.

Åtgärdsansvarig	Datum när åtgärden ska vara införd	Status genomförande	Uppföljningsdatum
[namn]	[datum]	[Välj]	[datum]

Figur 12 Åtgärdsplanering

Kolumn **Åtgärdsansvarig** ange vem som är ansvarig för åtgärden.

Kolumn **Datum när åtgärden ska vara införd** används för att ange vilket datum åtgärden ska vara införd.

Kolumnen **Status genomförande** används för att följa hur det går att införa åtgärder.

Kolumnen **Uppföljningsdatum** används för att ange datum för uppföljning av beslutade åtgärder

5. Kontinuitetsplanering och Riskhantering

5.1 Allmänt

Kontinuitetsplanering är en strategisk process som syftar till att säkerställa att en organisation kan fortsätta sin verksamhet även när den utsätts för störningar eller hot. Det handlar om att planera för att upprätthålla verksamheten på en tolerabel nivå, oavsett vilken typ av störning som inträffar. Exempel på sådana störningar kan vara allt från cyberattacker och naturkatastrofer till personalbrist eller strömavbrott.

5.2 Riskhantering

När en Verksamhetsutövare har genomfört Risk- och sårbarhetsanalys (RSA) och vidtagit åtgärder, kan det ändå finnas kvarstående risker som av olika anledningar inte kan hanteras inom rimlig tid eller till acceptabla kostnader. För att hantera dessa ska Verksamhetsutövaren uppdatera sin kontinuitetsplan med åtgärder som kan vidtas om dessa risker skulle inträffa.