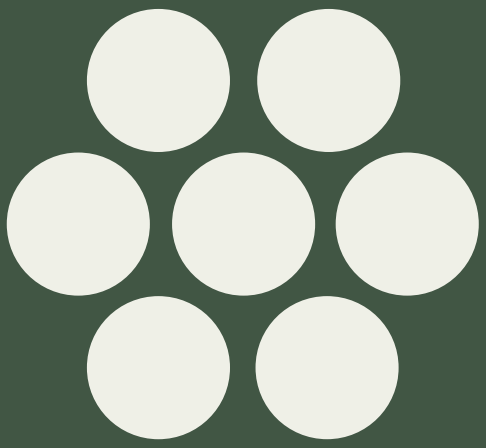
Instruktion för RSA inom Bashot Telekom

Version 2.0



Hotkatalog
Risk- och sårbarhetsanalys

Innehåll

1. Inledning

1.1 Allmänt

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

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

1.2 Revisionshistorik

Utgåva	Datum	Handläggare	Beskrivning
1.0	2021-12-21	L. Björkman	Lansering
1.1	2022-02-03	L. Björkman	Justering av avsnitthandledning
2.0	2024-02-26	K. Bergman L. Björkman J. Persson	Ersättning av risk- och sårbarhetsanalyser

Tabell 1 Revisionshistorik

1.3 Bakgrund

En tillhandahållare av kommunikationsnät eller kommunikationstjänster har en skyldighet att upprätta risk-och sårbarhetsanalyser i enlighet med *PTS föreskrift PTSFS 2022:11*. Föreskriften innehåller bland annat nedanstående bestämmelse:

– tekniska och organisatoriska åtgärder som enligt 8 kap. 1 § lagen (2022:482) om elektronisk kommunikation ska vidtas för att hantera risker som hotar säkerheten i nät och tjänster.

En av dessa åtgärder anges i 5 kap. Riskanalys och lyder enligt följande:
I en riskanalys ska tillhandahållaren analysera risken för att tillgångar, informationsbehandlingstillgångar eller förbindelser orsakar eller drabbas av säkerhets- eller integritetsincidenter. Riskanalyser ska göras för varje tillgång, informationsbehandlingstillgång och förbindelse.

Som allmänt råd i kapitlet anges:
Vid genomförandet av riskanalyser bör tillhandahållaren åtminstone analysera organisatoriska, logiska och fysiska hot.

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

1.4 Analysobjekt

Analysobjekten omfattar:

Tillgångar
funktion som utgörs av en avgränsad del av ett kommunikationsnät eller en kommunikationstjänst och som är nödvändig för att tillhandahålla ett sådant nät eller en sådan tjänst, samt som används för att sända, motta, bearbeta eller lagra information,

Informationsbehandlingstillgångar
system, databaser och fysiska resurser som används för informationsbehandling,

Förbindelser
del av kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett kommunikationsnät,

Verksamhet

del av nätägarens organisation med ansvar för säkerhet, förvaltning och drift av nät och tjänster.

1.5 Syfte

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

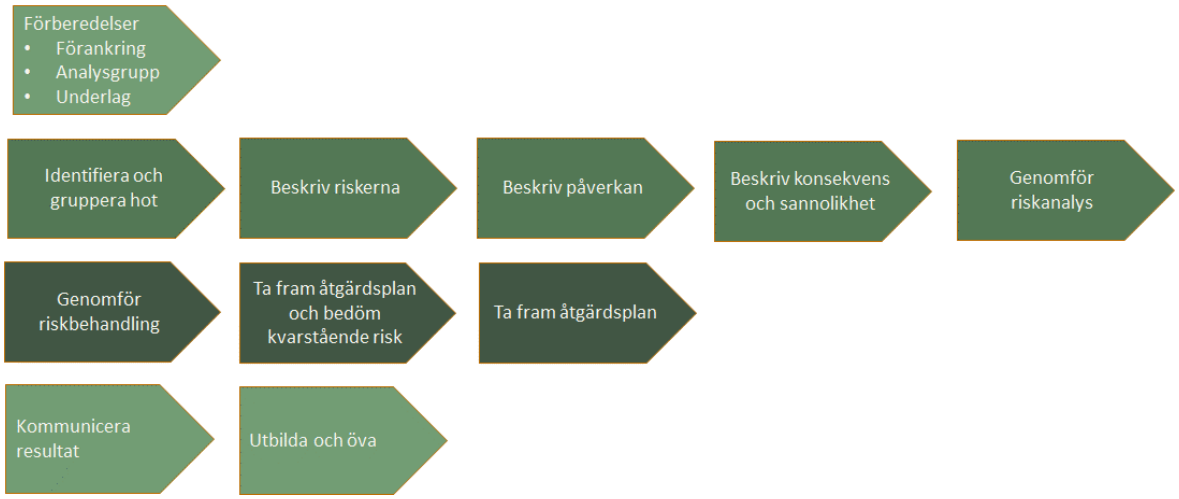
1.6 Avgränsningar

Risk- och sårbarhetsanalyserna i detta dokument avser inte:

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

1.7 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 MSB (Myndigheten för Samhällsskydd och Beredskap).
RSA-metoden omfattar nedanstående steg:



Figur 1 RSA-metoden

1.8 Återkommande RSA

Minst en gång per år ska det göras en översyn och en bedömning av och om förändringar i omvärlden, 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.

1.9 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.

1.10. Revidering och ansvar

Risk- och sårbarhetsanalysen revideras en gång per år eller då väsentliga förändringar gjorts avseende organisation eller i system för informationsbehandling och system för administration och drift av nät och tjänster. Systemägarna ansvarar för att detta görs.

1.11. 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 medan ifyllda riskanalyser ska klassificeras som TLP: Amber + Strict eftersom de kan innehålla känslig information.

TLP är en förkortning av Traffic Light Protocol och är en internationell standard för märkning av säkerhetsklassning av 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

- **Hot/Hotkategori** - Hot eller hotkategori avser potentiella faror eller risker som kan påverka en organisation eller dess tillgångar. Hoten kan kategoriseras baserat på liknande egenskaper eller metoder, vilket möjliggör en mer systematisk och strategisk hantering av säkerhetsrisker.
- **Risk** - sannolikheten för att en oönskad händelse inträffar och de potentiella konsekvenserna av denna händelse.
- **Konsekvens** - skada eller påverkan som kan uppstå om en riskhändelse inträffar.
- **Sårbarhet** - brist eller svaghet i system, processer eller resurser som ökar risken för oönskade händelser.
- **Riskanalys** - process för att förstå riskens natur och för att avgöra risknivån.
- **Resulterande sårbarhet** - Sårbarheter som återstår efter införande av skyddsåtgärder.
- **Sannolikheten** anger hur troligt det är att hotet kommer att inträffa.

3. Förberedelser

3.1 Förberedelser

För att säkerställa att resultaten av risk- och sårbarhetsanalyser är effektiva och leder till välgrundade förebyggande och förbättrande åtgärder, är det nödvändigt med noggranna förberedelser. Detta innefattar att avsätta adekvata resurser inklusive tekniska verktyg, arbetstid och kvalificerad personal, samt att följa en strukturerad och genomtänkt process för genomförandet av analyserna.

3.2 Förankring

Företagsledningens 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 företagsledningen en stark kultur för riskmedvetenhet och ansvarstagande på alla nivåer inom organisationen.

3.3 Analysgrupp och underlag

En analysledare ska utses som 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

Analysgruppen bör inte vara för stor och innefatta ansvariga för förvaltning och drift av analysobjekten samt, beroende av analysobjekt, experter inom nätplanering, teknik, säkerhetssamordning, ekonomi och juridik.

En dokumentationsansvarig bör utses och är den som håller i pennan. Den dokumentansvarige 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 ta reda på alla nödvändiga fakta och att se till att medlemmarna i analysgruppen har tagit del av dessa.

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

- beskrivning av analysobjektet(n). Aktuella objekt utgörs av de definierade tillgångar och förbindelser som har dokumenterats i enlighet med kraven i PTSFS 2022:11.
- författningskrav, föreskrifter och andra styrande dokument som direkt kan påverka riskanalysen
- statistik som underlättar analysgruppens bedömning
- incident- och problemrapporter
- liknande riskanalyser som kan vara av stort värde för arbetet
- allmänna hotbilder som kan vara till stöd och hjälp för att identifiera hot

3.4 Lokal och utrustning

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

3.5 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.

3.6 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.

3.7 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. Kommunicera resultat och åtgärdsförslag till berörda funktioner.

3.8 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 MSB: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. Verktyget finns för följande tillämpningar:

- Verksamhet nätdrift
- Site och nod
- Passiv och säker förbindelse
- Robusta radionät
- Robust och säker IoT
- Fastighetsnät
- Informationsbehandlingstillgångar,

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 (ssnf.org)

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, i enlighet med PTSFS 2022:11.

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.

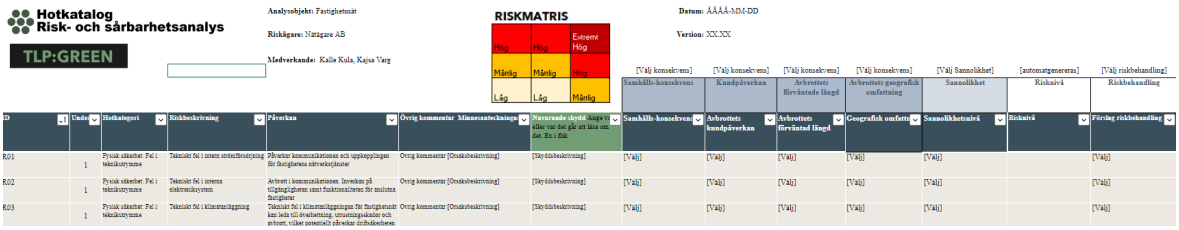
Riskanalys

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:

- hotkatalog
- riskanalys
- 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

[Skriv åtgärdförslag]	[Välj risknivå]	[Skriv åtgärdsresonemang]	[Ange ansvarig]	[Ange datum]	[Ange status]	[Ange datum]
Åtgärdshantering vid förslag Reduceras och Eliminieras						
Åtgärdförslag	**Kvarstående risk - risknivå efter att åtgärden är införd**	**Beskrivning av resonemang kring risknivå efter införd åtgärd**	**Åtgärdsansvarig**	**Datum när åtgärden ska vara införd**	**Status genomförande**	**Uppföljnings-datum**
[åtgärd]	[Välj]	[text]	[namn]	[datum]	[Välj]	[datum]

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 1.11 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	Naturliga händelser: Väder	Storm - Fällskador (träd, stam och rotvältor).
R02	1	Naturliga händelser: Väder	Storm - Erodering (strand)

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 hot, 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** innehåller prefabricerade hot. 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 vald hotkategori. 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.

[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 omfattningen (lokalt, regionalt, nationellt).

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

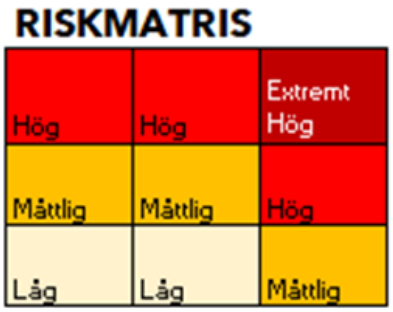
4.3.4 Genomför en riskanalys

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.

[automatgenereras]
Risknivå
Risknivå
Låg

Figur 8 Risknivå

I kolumn **Risknivå** presenteras den beräknade risknivån (beräkning sker automatiskt). Definitionen av risk inom ramen för riskhantering 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 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.

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 ett företag 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 företaget uppdatera sin konitnuitetsplan med åtgärder som kan vidtas om dessa risker skulle inträffa.