VÄGLEDNING FÖR RISK- OCH SÅRBARHETSANALYSER I ELSEKTORN

SVENSKA KRAFTNÄT

ENERGI FÖRETAGEN

Omslagsfoto: Tomas Ärlemo

Org.nr 202100-4284

Svenska kraftnät
Box 1200
172 24 Sundbyberg
Sturegatan 1

Tel: 010-475 80 00
E-mail: registrator@svk.se
www.svk.se

FÖRORD

En fungerande elförsörjning är en förutsättning för att samhället ska fungera. Elsystemet genomgår stora förändringar. En ökad elektrifiering, t.ex. i transportsektorn, digitalisering och en allt större andel distribuerad och väderberoende elproduktion gör att systemet ställs inför nya utmaningar.

I takt med samhällsutvecklingen blir beroendet av en trygg och säker elförsörjning allt större. Men en konsekvens av ökat elberoende är också en ökad sårbarhet i samhället. Alla aktörer inom elförsörjningen behöver därför ha en robust och störningstålig verksamhet. Risk- och sårbarhetsanalyser är ett systematiskt arbetssätt för att analysera risker och sårbarheter i den egna verksamheten. Utifrån detta underlag kan åtgärder sedan identifieras och prioriteras. På så sätt skapas underlag för information till den egna verksamheten och till berörda intressenter.

Slutmålet är att öka den egna verksamhetens förmåga att förebygga, motstå och hantera störningar och därmed göra Sveriges elförsörjning mer robust.

För att ge stöd till elnätsföretags, elproduktionsföretags och elhandelsföretags arbete med risk- och sårbarhetsanalysen har Energiföretagen Sverige och Svenska kraftnät gemensamt utarbetat den här vägledningen. Den bygger på tidigare versioner utgivna 2010 och 2014 men vid revideringen har också synpunkter inhämtade via enkäter till branschföreträdare vid Kraftsamling 2014 och intervjuer genomförda i mars/april 2017 gett värdefulla bidrag till utvecklingen av innehållet.

Vägledningen utgår från kraven i såväl ellagen som elberedskapslagen. Vägledningen är inte styrande eller reglerande, utan ska ses som ett stöd i arbetet med att upprätta risk- och sårbarhetsanalyser.

Vi hoppas att den ska vara ett bra stöd för aktörerna i elsektorn i arbetet med risk- och sårbarhetsanalyser och verka väl i det gemensamma ansvaret för en trygg och säker elförsörjning.

Sundbyberg, juli 2017
Svenska kraftnät

Ulla Sandborgh
Generaldirektör

Sundbyberg, juli 2017
Energiföretagen Sverige

Pernilla Winnhed
Verkställande direktör

INNEHÅLL

INNEHÅLL

1. INLEDNING

En välfungerande och robust elförsörjning är en nödvändig förutsättning för ett fungerande samhälle. Energi- och elförsörjningen är samhällsviktiga verksamheter i fred och en del av det civila försvaret under höjd beredskap och därmed en del av Sveriges totalförsvarsförmåga. För att bedriva verksamhet med så få och så lindriga störningar som möjligt krävs en god uppfattning om vilka hot, risker och sårbarheter verksamheten står inför samt ett aktivt arbete för att bedöma och skapa förmåga att hantera dessa. Risk- och sårbarhetsanalysen är ett centralt verktyg i en verksamhets säkerhetsarbete och ger såväl systematik som möjlighet till uppföljning av åtgärder.

Elproduktionsföretag, elnätsföretag och elhandelsföretag ska samtliga upprätta risk- och sårbarhetsanalyser enligt elberedskapslagen (1997:288). Elnätsföretagen ska även upprätta risk- och sårbarhetsanalys enligt ellagen (1997:857). Myndigheten för samhällsskydd och beredskap (MSB) föreskriver att såväl statliga myndigheter som kommuner och landsting är skyldiga att upprätta risk- och sårbarhetsanalyser och dessa kan beröra aktörer inom elsektorn. Den internationella standarden ISO 31000 om riskhanteringsprocessen är frivillig att följa och kan beröra delar av risk- och sårbarhetsanalyserna.

De risk- och sårbarhetsanalyser som aktörerna i elsektorn upprättar förutsätts inkludera hela den egna verksamheten, med fokus på de delar som anses mest kritiska för att verksamheten ska kunna upprätthållas. Risk- och sårbarhetsanalyser ökar medvetenheten och kunskapen hos beslutsfattare och verksamhetsansvariga om hot, risker och sårbarheter inom den egna verksamheten och skapar därmed ett underlag för planering och beslut. Risk- och sårbarhetsanalyser kan också användas som underlag för information till allmänheten och kunder om risker och sårbarheter och behovet av att på individnivå också ha beredskap för avbrott och störningar.

På en nationell nivå är risk- och sårbarhetsanalyserna ett viktigt verktyg för att bedöma elförsörjningens beredskap på samhällsnivå och behov av åtgärder för att stärka samhällets elförsörjning, både i fredstid och under höjd beredskap. Inom elsektorn ska risk- och sårbarhetsanalyserna kunna utgöra underlag till Energimarknadsinspektionens risk- och sårbarhetsanalyser avseende leveranssäkerheten i elnäten. Risk- och sårbarhetsanalysen är också ett underlag för uppgiftslämnande till Svenska kraftnät, som använder uppgifterna för en nationell risk- och sårbarhetsanalys för elsektorn, vilken sedan utgör underlag för inriktning av elberedskapsåtgärder. Lagkrav och vägledningar används som utgångspunkt för elaktörernas risk- och sårbarhetsanalyser.

Risk- och sårbarhetsanalyser i elsektorn har alltså tre huvudsakliga syften:

> Skapa egennytta för den egna verksamheten, t.ex. i form av underlag för planering och beslut samt underlag till myndigheters risk- och sårbarhetsanalyser
> Främja/skapa robustare elförsörjning genom färre och lindrigare störningar
> Ge en samlad riskbild för elsektorn som helhet (se avsnitt 2.2)

Syftet med den här vägledningen är att ge stöd till aktörer i elsektorn vid upprättandet av sina risk- och sårbarhetsanalyser med tillhörande åtgärdsplaner. Vägledningen vänder sig i första hand till ansvariga för risk- och sårbarhetsanalyser i elproduktionsföretag, elnätsföretag och elhandelsföretag. Fokus i vägledningen är att beskriva en arbetsprocess för risk- och sårbarhetsanalyser indelad i förberedelsefas, analysfas och rapporteringsfas.

Vägledningen är utarbetad gemensamt av Energiföretagen Sverige och Svenska kraftnät och bygger på tidigare versioner utgivna 2010 och 2014. Vid revideringen har synpunkter inhämtade via enkäter till branschföreträdare vid Kraftsamling 2014 och genom intervjuer genomförda i mars/april 2017, gett värdefulla bidrag till utvecklingen av vägledningen.

2. HELHETSSYN I SÄKERHETSARBETET

2.1 Risk- och sårbarhetsanalyser på olika samhällsnivåer

Det övergripande syftet med risk- och sårbarhetsanalyser är att minska sårbarheten i samhället och att öka förmågan att hantera kriser. Detta är viktigt på alla samhällsnivåer och därför är såväl statliga myndigheter som kommuner och landsting genom lag och förordning ålagda att genomföra risk- och sårbarhetsanalyser.

Enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska samtliga statliga myndigheter, såväl nationella som regionala, årligen ta fram risk- och sårbarhetsanalyser. Enligt samma förordning ska de myndigheter som har ett särskilt ansvar för krisberedskapen (vilka framgår i en bilaga till förordningen) och de myndigheter som MSB beslutar, vartannat år lämna en redovisning baserad på analysen till Regeringskansliet och MSB. För Svenska kraftnäts del innebär detta att verket ska ta fram en nationell risk- och sårbarhetsanalys för elsektorn som även omfattar den egna myndigheten. Länsstyrelserna ska upprätta regionala risk- och sårbarhetsanalyser och de stödjer andra aktörer som också är ansvariga för krisberedskapen i länet, i deras risk- och sårbarhetsanalyser. Kommuner och landsting genomför risk- och sårbarhetsanalyser enligt lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

MSB har publicerat föreskrifter om redovisning av risk- och sårbarhetsanalysarbetet. Statliga myndigheter lämnar en redovisning till regeringen (enligt MSBFS 2016:7). Kommuner och landsting rapporterar till länsstyrelsen respektive Socialstyrelsen (enligt MSBFS 2015:4 och 2015:5). Kommunen ska till exempel redovisa identifierade kritiska beroenden i kommunens samhällsviktiga verksamhet. Redovisningen bör utgå från kritiska beroenden som rör den samhällsviktiga verksamhet som kommunen själv förvaltar, bedriver eller äger, till exempel elnät, inklusive bolag, förbund eller andra samarbetsformer. Alla dessa aktörer redovisar också arbetet till MSB.

Genom rapporteringen kan bland andra kommuners och landstings risk- och sårbarhetsarbete utgöra ett av underlagen i en regional risk- och sårbarhetsanalys. På motsvarande sätt kan till exempel länsstyrelsernas och de centrala myndigheternas redovisningar bidra till en övergripande nationell riskbild för Sverige. MSB använder rapporteringen som underlag i t.ex. den nationella risk- och sårbarhetsanalysen.

TÄNK PÅ!

Att både kommuner och länsstyrelser kan ha behov av att samverka med elsektorn vid utarbetande av kommunala respektive regionala risk- och sårbarhetsanalyser. Företag inom elsektorn kan också ha nytta av denna samverkan i sitt arbete, till exempel genom att få information om vilka risker kommunen respektive länsstyrelsen har identifierat inom respektive geografiskt område.

2.2 Svenska kraftsnäts nationella risk- och sårbarhetsanalys för elsektorn

Svenska kraftnäts arbete med nationell risk- och sårbarhetsanalys för elsektorn utgår från elberedskapslagen (1997:288) och syftar till att stärka samhällets förmåga att förebygga och hantera allvarliga störningar inom elförsörjningen. Det omfattar även att kunna återställa efter en inträffad händelse. Samverkan med andra aktörer i att förebygga, hantera och återställa är en viktig aspekt i analysen. Risk- och sårbarhetsanalys omfattar därför alla typer av risker på hela hotskalan, upp till höjd beredskap/krig.

Underlaget till den nationella risk- och sårbarhetsanalysen för elsektorn baseras på uppgifter som Svenska kraftnät begär in (enligt SvKFS 2013:2) från elaktörerna (se avsnitt 4.1.3 och 4.1.4), men även andra underlag som t.ex. analyser av specifika scenarier som rör elförsörjningen. Resultatet av den nationella risk- och sårbarhetsanalysen ger ett underlag för planering av beredskapsåtgärder inom elsektorn och därför är det viktigt att berörda aktörer inom elförsörjningen är involverade i arbetet. Ett exempel på samverkan mellan aktörerna och Svenska kraftnät är det årliga mötet Kraftsamling.

2.3 Risk- och sårbarhetsanalysen är en del av det systematiska säkerhetsarbetet

Elproduktionsföretag, elnätsföretag, och elhandelsföretag ska förhålla sig till olika författningar med krav på riskanalyser och annan typ av säkerhetsarbete, däribland ellagen och elberedskapslagen, men också säkerhetsskyddslagen, lagen om skydd mot olyckor, miljöbalken med flera.

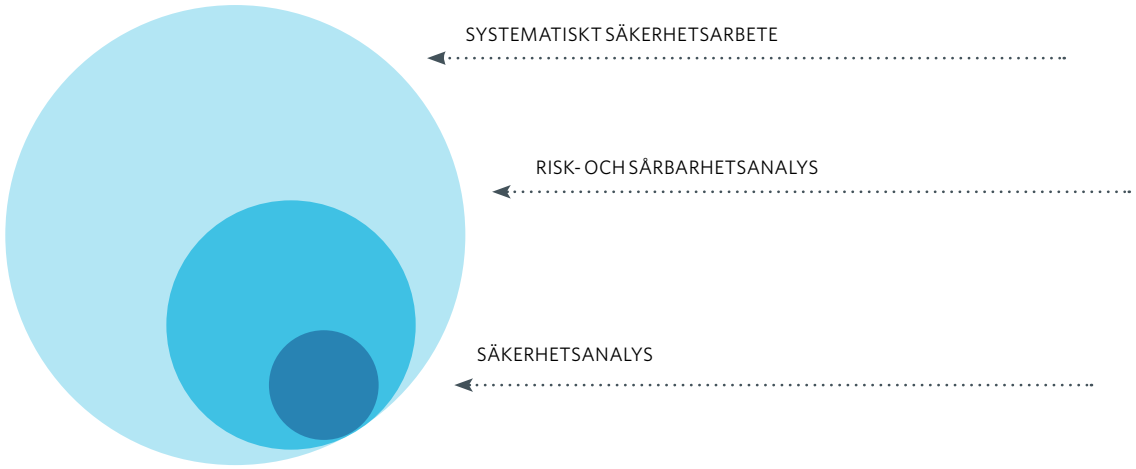
TÄNK PÅ!

Att även om olika författningar har olika utgångspunkter består den riskanalysprocess som krävs ofta av samma delmoment. Arbetet med att identifiera, analysera, värdera och behandla riskerna kan därför i stort sett genomföras i en och samma process och med hjälp av samma metoder. Resultatet av analyserna ger därefter ingångsvärden till åtgärder inom olika delar av ett systematiskt säkerhetsarbete.

Arbetet med risk- och sårbarhetsanalys och säkerhetsanalys enligt § 5 säkerhetsskyddsförordningen (1996:633) är ett exempel där utgångspunkterna skiljer sig åt, men där metod och process för analys kan vara densamma. För mer information om säkerhetsanalys hänvisas till Svenska kraftnäts Vägledning för säkerhetsanalys (Svenska kraftnät 2005) och Vägledning IS/IT-säkerhet samt säkerhetsskydd (Version 1.0, Dnr: 2012:331).

Risk- och sårbarhetsanalys kan ses som en del av företagets systematiska säkerhetsarbete och säkerhetsanalysen kan ses som en fördjupning av de delar av risk- och sårbarhetsanalysen som rör hot mot rikets säkerhet eller skydd mot terrorism. Vid arbete med risk- och sårbarhetsanalys kan arbetet inledas med att identifiera verksamheter/funktioner som alltid måste fungera för att en störning inte ska uppstå. Därefter identifieras och analyseras de riskkällor som kan påverka dessa funktioner/verksamheter. När en säkerhetsanalys ska genomföras inleds arbetet istället med att identifiera verksamheter som är skyddsvärda med hänsyn till rikets säkerhet och eller skydd mot terrorism, och vid den efterföljande riskinventeringen tittar man huvudsakligen på aktörsstyrda hot som till exempel terrorism och sabotage.

Fördelarna med att utföra säkerhetsanalys och riskanalys i så enade arbetsprocesser som möjligt är många. Dubbelarbete undviks och resurser utnyttjas på ett effektivt sätt samtidigt som synergier skapas vilket leder till att organisationens beslutsunderlag förbättras. En av de största effektivitetsvinsterna finns framför allt i riskidentifieringsfasen. Vidare riskerar inte viktiga områden inom säkerhetsarbetet att falla bort eller tyngdpunkten i säkerhetsarbetet att bli felaktig. Denna vägledning visar på metoder och processer för risk- och sårbarhetsanalyser som med fördel kan integreras med övrigt systematiskt säkerhetsarbete.



Figur 1. Förhållande mellan risk- och sårbarhetsnalys och övrigt säkerhetsarbete

3. FORMELLA KRAV PÅ RISK- OCH SÅRBARHETSANALYSER

Arbete med risk- och sårbarhetsanalyser inom elsektorn är reglerat genom ellagen (1997:857), elberedskapslagen (1997:288) samt tillhörande förordningar och föreskrifter. I det här kapitlet presenteras ett urval av de viktigaste författningarna.

Ibland har olika lagstiftning likartade krav och i tabell 1 visas en jämförelse mellan kraven från Energimarknadsinspektionen och Svenska kraftnät.

3.1 Ellagen

Enligt ellagen (1997:857) ska de elnätsföretag som bedriver nätverksamhet med stöd av nätkoncession för linje med en spänning som understiger 220 kilovolt eller nätkoncession för område upprätta en risk- och sårbarhetsanalys avseende leveranssäkerheten i det egna elnätet. En åtgärdsplan som visar på hur leveranssäkerheten ska förbättras ska upprättas med utgångspunkt i analysens resultat. En redovisning baserad på risk- och sårbarhetsanalysen och åtgärdsplanen ska årligen lämnas till Energimarknadsinspektionen.

3.2 Energimarknadsinspektionens föreskrifter

Med bakgrund i ellagen (1997:857) har Energimarknadsinspektionens utarbetat föreskrifter och allmänna råd (EIFS 2013:3) om risk- och sårbarhetsanalyser och åtgärdsplaner avseende leveranssäkerheten i elnäten för innehavare av nätkoncession för linje med en spänning som understiger 220 kilovolt och innehavare av nätkoncession för området. Enligt föreskrifterna ska dessa aktörer upprätta risk- och sårbarhetsanalyser som innehåller följande information:

> Kartläggning av nuläget
> Identifiering av riskkällor
> Uppskattning av risker och sårbarhet
> Identifiering och prioritering av åtgärder som leder till minskad risk och sårbarhet

Endast riskkällor som är av exceptionell karaktär och som inte omfattas av nätkoncessionsinnehavarens kontrollansvar får undantas från analysen. Upprättade risk- och sårbarhetsanalyser ska dokumenteras och rapporteras till Energimarknadsinspektionen. Redovisningen beskrivs närmare i 4.4.3.

TABELL 1. RELATION MELLAN KRAVEN FRÅN ENERGIMARKNADSINSPEKTIONEN OCH SVENSKA KRAFTNÄTS ALLMÄNNA RÅD, MED HÄNVISNING TILL KAPITEL I VÄGLEDNINGEN.

ENERGIMARKNADSINSPEKTIONENS FÖRESKRIFTER	SVENSKA KRAFTNÄTS ALLMÄNA RÅD	AVSNITT I KAPITEL 3
Kartläggning av nuläget	> Identifiering av funktioner/ verksamheter som alltid måste fungera för att en störning inte ska uppstå	4.2 Förberedelsefas
Identifiering av riskkällor Uppskattning av risker och sårbarhet Identifiering och prioritering av åtgärder som leder till minskad risk och sårbarhet	> Identifiering av riskkällor som kan påverka/hota dessa funktioner/ verksamheter > Riskanalys för att bedöma sannolikhet och konsekvens > Riskutvärdering för att bedöma vilka av de identifierade riskkällorna som ska behandlas vidare, vilka åtgärder som ska vidtas för identifierade risker osv. > Bedömning av förmåga att motstå och hantera identifierade riskkällor, inklusive identifiering av kritiska beroenden > Riskbehandling genom identifiering och prioritering av åtgärder med anledning av analysens resultat	4.3 Analysfas
Rapportering till Energimarknadsinspektionen	> Uppgiftslämnande till Svenska kraftnät	4.4 Rapporteringsfas

TABELL 2. ENERGIMARKNADSINSPEKTIONENS FÖRESKRIFTER OCH ALLMÄNNA RÅD (EIFS 2013:1) OM KRAV SOM SKA VARA UPPFYLLDA FÖR ATT ÖVERFÖRINGEN AV EL SKA VARA AV GOD KVALITET.

LASTINTERVALL (MEGAWATT)	AVBROTTSTID VID NORMALA ÅTERSTÄLLNINGSFÖRHÅLLANDEN (TIMMAR)	AVBROTTSTID VID ONORMALA ÅTERSTÄLLNINGSFÖRHÅLLANDEN (TIMMAR)
>2≤5	12	24
>5≤20	8	24
>20≤50	2	24
>50	2	12

3.3 Elberedskapslagen

Ett av kraven i elberedskapslagen (1997:288) är att aktörer som bedriver produktion av el, handel med el eller överföring av el ska upprätta risk- och sårbarhetsanalyser avseende säkerheten i den egna verksamheten. Kravet innebär också att aktörerna ska lämna de uppgifter till elberedskapsmyndigheten, Svenska kraftnät, som myndigheten behöver för att kunna upprätta en nationell risk- och sårbarhetsanalys för elsektorn (se avsnitt 2.2).

3.4 Svenska Kraftnäts föreskrifter

Svenska kraftnäts föreskrifter och allmänna råd (SvKFS 2013:2) om elberedskap innehåller bland annat bestämmelser om risk- och sårbarhetsanalys samt uppgiftslämnande till Svenska kraftnät för den som bedriver produktion av el, handel med el eller sådan överföring av el som sker med stöd av nätkoncession.

Arbetet med risk- och sårbarhetsanalyser ska enligt föreskrifterna genomföras årligen och omfatta att systematiskt identifiera, analysera och dokumentera riskkällor som kan påverka säkerheten i den egna verksamheten. I arbetet ingår också att bedöma hur sårbar verksamheten är mot dessa riskkällor samt att föreslå åtgärder med anledning av resultatet av analysen. Riskkällor som är av mycket ovanlig eller exceptionell karaktär ska också ingå. Den egna verksamhetens beroenden av andra verksamheter ska beaktas i analysen. I Svenska kraftnäts föreskrift anges som allmänt råd att risk- och sårbarhetsanalysen kan omfatta följande moment:

- Identifiering av funktioner/verksamheter som alltid måste fungera för att en störning inte ska uppstå.
- Identifiering av riskkällor som kan påverka eller hota dessa funktioner/verksamheter.
- Riskanalys för att bedöma sannolikhet och konsekvens.
- Riskutvärdering för att bedöma vilka av de identifierade riskkällorna som ska behandlas vidare, vilka åtgärder som ska vidtas för identifierade risker och så vidare.
- Bedömning av förmåga att motstå och hantera identifierade riskkällor, inklusive identifiering av kritiska beroenden.
- Riskbehandling genom identifiering och prioritering av åtgärder med anledning av analysens resultat

På begäran ska aktörerna lämna uppgifter till Svenska kraftnät som underlag för den nationella risk- och sårbarhetsanalysen för elsektorn (se också 3.4).

FOTO: TOMAS ÅRLEMO

KRAV OCH EXEMPEL

ELNÄTSFÖRETAG

För elnätsföretag kan exempel på delar av verksamheten som ständigt måste fungera vara transformatorstationer, styr- och reglersystem och driftoperatörer. Också lagkrav eller andra regleringar kan fungera som utgångspunkt för vad som bör ingå i analysen. Exempelvis gäller enligt ellagen att ett avbrott inte får överstiga 24 timmar (funktionskravet). I vissa delar av elnätet, med högre lastnivåer, ska den maximala avbrottstiden vara betydligt lägre, se tabell 2. Händelser som riskerar att medföra att dessa tidskrav överskrids bör därmed inkluderas i analysen.
Enligt EIFS 2013:3 ska koncessionshavaren identifiera de uttagspunkter i nätet där funktionskravet, eller strängare krav på leveranssäkerhet som följer av andra föreskrifter (exempelvis tabell 1), inte bedöms vara uppfyllt. För dessa uttagspunkter ska det anges vilka åtgärder som kommer att vidtas för att kraven ska uppfyllas, samt när dessa åtgärder ska vara genomförda.

ELPRODUKTIONSFÖRETAG

För elproduktionsföretag kan exempel på delar av verksamheten som ständigt måste fungera viktiga produktionsanläggningar, fysiska tillgångar eller beroenden till kritiska leverantörer. Andra parametrar att utgå ifrån kan till exempel vara avtal med kunder, leverantörer eller intressenter avseende produktionskapacitet.

ELHANDELSFÖRETAG

För elhandelsföretag kan exempel på delar av verksamheten som ständigt måste fungera vara viktiga elhandelssystem. Kritiska delar av verksamheten för ett elhandelsföretag är ofta kopplade till den finansiella aspekten av verksamheten, till exempel analys av avtalsbestämmelser gentemot kunder eller elleverantörer.

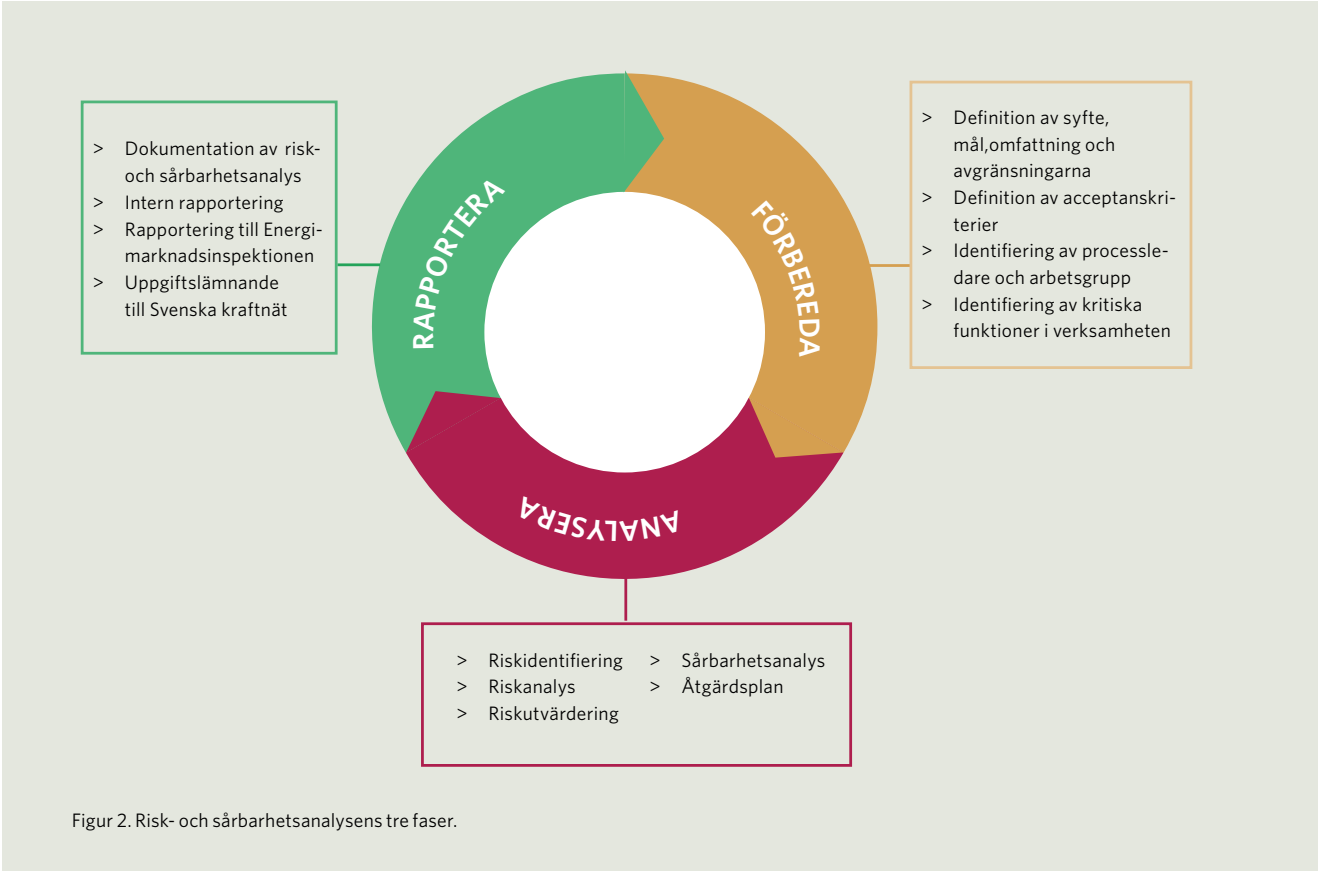
EXEMPEL PÅ LAGAR, FÖRORDNINGAR OCH FÖRESKRIFTER SOM BERÖR ELAKTÖRERNAS RISK- OCH SÅRBARHETSANALYSER

- Ellag (1997:857)
- Elberedskapslag (1997:288)
- Offentlighets- och sekretesslag (2009:400)
- Säkerhetsskyddslag (1996:627)
- Lag (2003:778) om skydd mot olyckor
- Miljöbalken (1998:808)
- Säkerhetsskyddsförordning (1996:633)
- Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
- Affärsverket svenska kraftnäts föreskrifter och allmänna råd (SvKFS 2013:2) om elberedskap
- Energimarknadsinspektionens föreskrifter och allmänna råd (EIFS 2013:3) om risk- och sårbarhetsanalyser och åtgärdsplaner avseende leveranssäkerhet i elnäten
- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:7) om statliga myndigheters risk- och sårbarhetsanalyser

4. PROCESS FÖR RISK- OCH SÅRBARHETSANALYS

4.1 Översikt över processen

I detta kapitel beskrivs hur arbetet med att upprätta risk- och sårbarhetsanalyser kan genomföras i en samlad process. Arbetet kan delas in i tre faser vilket illustreras i figuren nedan.



Figur 2. Risk- och sårbarhetsanalysens tre faser.

TÄNK PÅ!

Att för större företag med flera olika verksamhetsområden är det lämpligt att genomföra verksamhetsspecifika risk- och sårbarhetsanalyser. Inom dessa organisationer bör därför ovanstående process utföras parallellt på flera olika delar av verksamheten (exempelvis handel och distribution).

Processbeskrivningen utgår ifrån att det är första gången en risk- och sårbarhetsanalys upprättas. I de fall en risk- och sårbarhetsanalys redan genomförts handlar de årliga revideringarna om att granska utarbetat material, uppdatera analysen med nytillkomna och bortfallna risker samt att bedöma om åtgärderna har haft önskad effekt på förmågan att förebygga, motstå och hantera störningar. Som ett resultat av denna analys ska även åtgärdsplanen uppdateras. Mer omfattande revideringar bör genomföras på regelbunden basis för att mer djupgående analysera och komplettera befintlig risk- och sårbarhetsanalys.

4.2 Förberedelsefas

I förberedelsefasen läggs grunderna för det fortsatta arbetet med risk- och sårbarhetsanalysen, bland annat genom:

> Formulering av syfte, mål, omfattning och avgränsningar
> Definition och beslut kring riskkriterier
> Beslut kring nominering av processledare och arbetsgrupp
> Identifiering av funktioner/verksamheter som alltid måste fungera

4.2.1 Syfte, mål, omfattning och avgränsningar

Ledningen bör utarbeta och dokumentera ett formellt beslut om arbetsinriktning. I detta beslut bör information om verksamhetens förutsättningar, avgränsningar och tidplan anges. Syfte och tydliga mål med arbetet som utgår från lagstiftningen bör formuleras i detta skede. Ledningens engagemang och aktiva stöd i processen är en förutsättning för ett lyckat resultat.

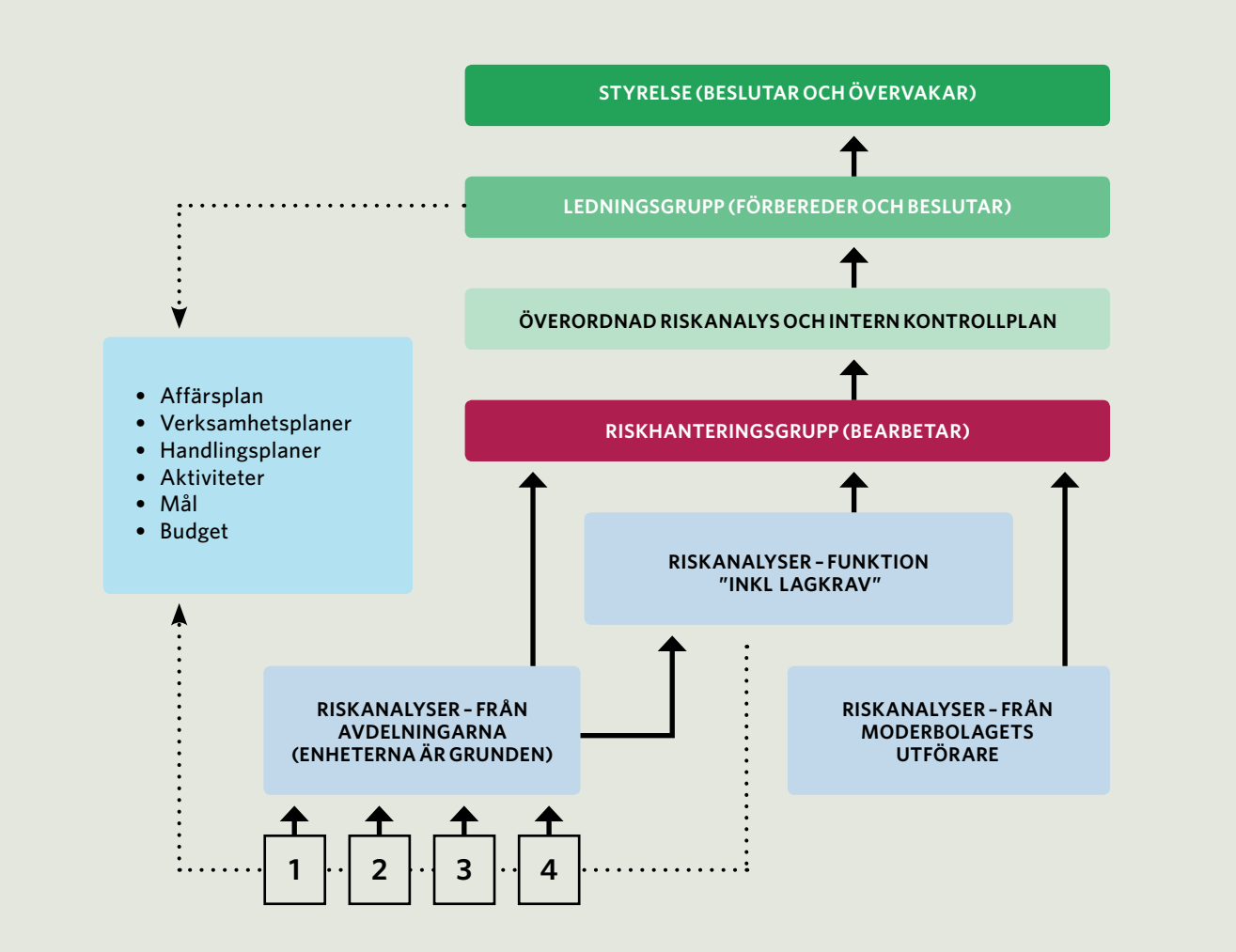
För elnätsföretag är tidpunkten för rapportering till Energimarknadsinspektionen given (senast under juli månad), men analysarbetet kan i övrigt genomföras enligt önskad tidplan. Till exempel kan det finnas andra processer/arbeten i organisationen med vilka arbetet med risk- och sårbarhetsanalys kan samordnas.

Det kan också vara bra att utarbeta en kommunikationsplan för hur resultatet ska kommuniceras internt och externt (se vidare 4.4.2).

4.2.2 Processledare och arbetsgrupp

Processledaren ska ha företagsledningens mandat att leda och bedriva arbetet med risk- och sårbarhetsanalysen. Som stöd till processledaren utses en grupp med tillräcklig och bred kunskap om verksamheten. I arbetsgruppen bör personer med kunskap om både de operativa och strategiska delarna av verksamheten ingå. Detta för att så många olika typer av risker som möjligt ska kunna identifieras och analyseras.

Personer med beslutsmandat bör också ingå i analysgruppen för att kunna prioritera och besluta om åtgärder. Arbetsgruppen behöver få en gemensam plattform och tid att utföra arbetet.



Figur 3. Exempel på hur arbetet med risk- och sårbarhetsanalys kan vara organiserat i ett företag i elsektorn.

FOTO: TOMAS ÅRLEMO

En referensperson/referensgrupp bör få ta del av risk- och sårbarhetsanalysen för att bidra med nya infallsvinklar och därmed utgöra en typ av kvalitetskontroll för att säkerställa att alla typer av risker är inkluderade i analysen. Resultatet bör förankras i och godkännas av ledningen.

4.2.3 Riskkriterier

Ett viktigt ingångsvärde för arbetet med risk- och sårbarhetsanalyser är att ha en tydlig definition av riskkriterier, det vill säga vilka konsekvenser organisationen kan tolerera till följd av en viss risk. Riskkriterierna bör beslutas på ledningsnivå. För att arbeta med enhetlig definition av riskkriterier kan man använda en så kallad kriteriemodell, se exempel i tabell 3, 4 och 5.

TABELL 3. EXEMPEL PÅ KRITERIEMODELL FÖR ELNÄTSFÖRETAG.

NIVÅ TYP AV KONSEKVENS	KLASS 1 "OBETYDLIGA"	KLASS 2 "LINDRIGA"	KLASS 3 "ALLVARLIGA"	KLASS 4 "OACCEPTABLA"
Ekonomi	> Mindre kostnader för reparation/ återställning > (<100 kkr)	> Måttliga kostnader för reparation/ återställning etc. > (100 kkr – 3 Mkr)	> Höga kostnader för reparation/återställning/avbrottsersättning etc. > (3 Mkr – 30 Mkr)	> Extremt höga kostnader för reparation/återställning/ avbrottsersättning etc. > (<300 Mkr)
Förtroende	> Enstaka klagomål	> Fåtal klagomål > Enstaka notis i lokalmedia > Mindre allvarligt kontraktsbrott mot en eller ett fåtal kunder	> Många klagomål > Högt tryck på information från allmänhet och media > Allvarligt kontraktsbrott mot en eller ett fåtal kunder	> Ohanterbart antal klagomål > Extremt högt tryck på information från allmänhet och media > Nationell (negativ) uppmärksamhet i media > Flertal allvarliga kontraktsbrott mot kunder
Liv och hälsa	> Tillbud	> Allvarligt tillbud	> Lindrig personskada som kräver vård	> Allvarlig personskada som kräver vård > Dödsfall
Leveranssäkerhet	> Obetydligt antal kunder drabbade av avbrott (<100)	> Fåtal kunder drabbade av avbrott (100–2 000)	> Större antal kunder drabbade av avbrott (2 000–20 000)	> Mycket stort antal kunder drabbade av avbrott (>20 000)
Avbrottstid	> <2 MW: 2 timmar > 2–5 MW: 1 timme > 5–20 MW: 1/4 timme > >20 MW: 1/6 timme	> <2 MW: 4 timmar > 2–5 MW: 2 timmar > 5–20 MW: 1/2 timme > >20 MW: 1/4 timme	> <2 MW: 12 timmar > 2–5 MW: 6 timmar > 5–20 MW: 2 timmar > >20 MW: 1 timme	> <2 MW: 24 timmar > 2–5 MW: 12 timmar > 5–20 MW: 8 timmar > >20 MW: 2 timmar
Samhällets elförsöjning/ påverkan på samhället	> Mindre påverkan på samhällets elförsörjning > Mindre påverkan på samhället	> Måttlig påverkan på samhällets elförsörjning > Måttlig påverkan på samhället	> Allvarlig påverkan på samhällets elförsörjning > Allvarlig påverkan på samhället	> Mycket allvarlig påverkan på samhällets elförsörjning > Mycket allvarlig påverkan på samhället

TABELL 4. EXEMPEL PÅ KRITERIEMODELL FÖR ELPRODUKTIONSFÖRETAG

NIVÅ / TYP AV KONSEKVENS	KLASS 1 "OBETYDLIGA"	KLASS 2 "LINDRIGA"	KLASS 3 "ALLVARLIGA"	KLASS 4 "OACCEPTABLA"
Ekonomi	> Mindre kostnader för reparation/återställning	> Måttliga kostnader för reparation/återställning	> Höga kostnader för reparation/återställning	> Extremt höga kostnader för reparation/ återställning
Förtroende	> Enstaka klagomål	> Fåtal klagomål > Enstaka notis i lokal media	> Många klagomål > Högt tryck på information från allmänhet och media	> Ohanterbart antal klagomål > Extremt högt tryck på information från allmänhet och media > Nationell (negativ) uppmärksamhet i media
Liv och hälsa	> Tillbud	> Allvarligt tillbud	> Lindrig personskada som kräver vård	> Allvarlig personskada som kräver vård > Dödsfall
Produktionskapacitet	> > Kapacitet minskad > med <1%	> > Kapacitet minskad > med <5%	> Kapacitet minskad > med <25%	> Kapacitet minskad > med >25%
Samhällets elförsörjning/påverkan på samhället	> Mindre påverkan på samhällets elförsörjning > Mindre påverkan på samhället	> Måttlig påverkan på samhällets elförsörjning > Måttlig påverkan på samhället	> Allvarlig påverkan på samhällets elförsörjning > Allvarlig påverkan på samhället	> Mycket allvarlig påverkan på samhällets elförsörjning > Mycket allvarlig påverkan på samhället

TABELL 5. EXEMPEL PÅ KRITERIEMODELL FÖR ELHANDELSFÖRETAG

NIVÅ / TYP AV KONSEKVENS	KLASS 1 "OBETYDLIGA"	KLASS 2 "LINDRIGA"	KLASS 3 "ALLVARLIGA"	KLASS 4 "OACCEPTABLA"
Ekonomi	> Mindre, negativa avvikelser i relation till budget	> Måttliga, negativa avvikelser i relation till budget	> Stora, negativa avvikelser i relation till budget > Behov av omprioriteringar på lite längre sikt (verkan inom 6 mån)	> Extremt stora, negativa avvikelser i relation till budget > Omprioriteringar bör ske omgående (verkan inom 3 mån)
Förtroende	> Enstaka klagomål	> Fåtal klagomål > Enstaka notis i lokal media	> Många klagomål > Högt tryck på information från allmänhet och media	> Ohanterbart antal klagomål > Extremt högt tryck på information från allmänhet och media > Nationell (negativ) uppmärksamhet i media
Information vid prissättning	> Mindre osäkerhet i information vid prissättning	> Osäkerhet i information vid prissättning	> Stor osäkerhet i information vid prissättning	> Ingen information att tillgå vid prissättning
Samhällets elförsörjning/påverkan på samhället	> Mindre påverkan på samhällets elförsörjning > Mindre påverkan på samhället	> Måttlig påverkan på samhällets elförsörjning > Måttlig påverkan på samhället	> Allvarlig påverkan på samhällets elförsörjning > Allvarlig påverkan på samhället	> Mycket allvarlig påverkan på samhällets elförsörjning > Mycket allvarlig påverkan på samhället

En kriteriemodell formaliserar riskkriterierna utifrån verksamhetens mål, strategier, ekonomiska förutsättningar, lagkrav och andra regler etc. Kriteriemodellen visar på en övergripande nivå vilka typer av konsekvenser som är oönskade och vilka som inte tole-reras. Modellen utgör en gemensam måttstock och säkerställer att analyser och bedömningar görs utifrån samma övergripande bild om vad företaget eftersträvar att motverka. Kriterier och kriteriemodellen underlättar riskutvärderingen som är ett senare steg i analysen (se 4.3.3).

På samma sätt som konsekvenserna kan definieras i en kriteriemodell, kan också definitioner för sannolikhet beslutas och dokumenteras. Ett exempel visas i tabell 6.

TABELL 6. EXEMPEL PÅ TABELL FÖR BEDÖMNING AV SANNOLIKHET.

SANNOLIKHET	FREKVENS
Mycket låg	<1 gång/100 år
Låg	<1 gång/25 år >1 gång/100 år
Måttlig	<1 gång/år >1 gång/25 år
Hög	>1 gång/år

Ovanstående verktyg kan användas för att tydligt definiera och kommunicera konsekvens- och sannolikhetsnivåer som utgör ett stöd i det fortsatta arbetet med risk- och sårbarhetsanalyser.

TABELL 7. EXEMPEL PÅ TABELL FÖR HÄNDELSEKLASSNING.

HÄNDELSEKLASS	FREKVENS (PER ÅR)
1. Årlig händelse	>1
2. Förväntad händelse	0,1–1
3. Sannolik händelse	0,01–0,1
4. Ej förväntad händelse	0,001–0,01
5. Osannolik händelse	<0,001

FOTO: TOMAS ÄRLEMO

4.2.4 Identifiering av processer som alltid måste fungera

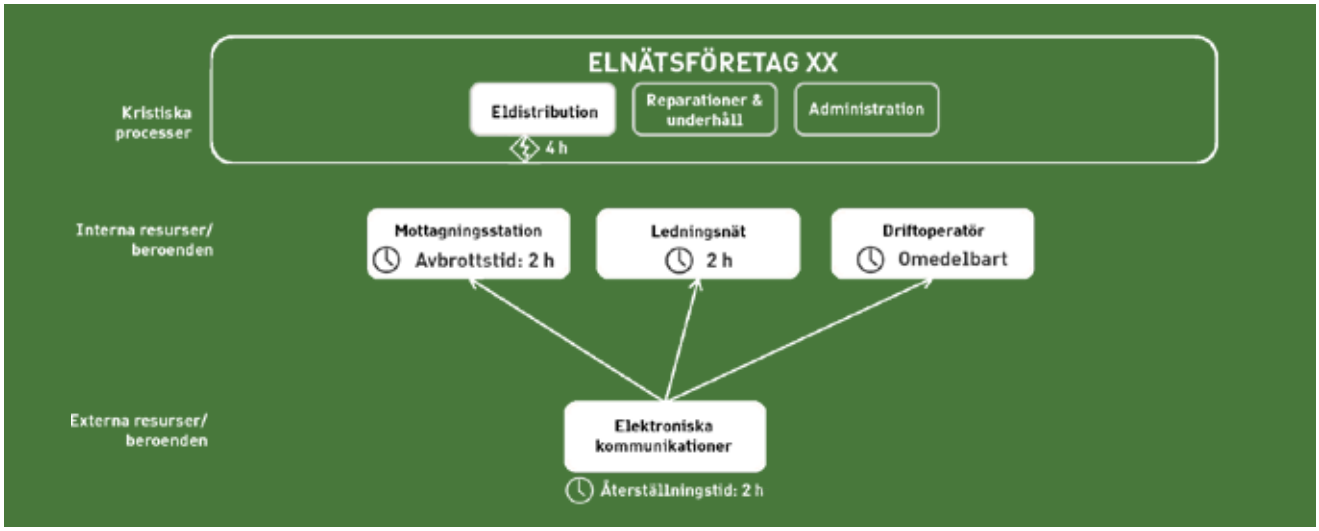
En av de viktigaste utgångspunkterna för analysen är kunskapen om vilka verksamhetens kritiska processer är, det vill säga, vilka funktioner/anläggningar/system och liknande som alltid måste fungera. En genomgång av verksamheten och dess processer skapar också förståelse för kritiska beroenden. Som stöd för detta arbete kan redan framtagna process- och verksamhetsbeskrivningar användas.

För en visualisering av verksamhetens kritiska processer och beroenden kan en konsekvensanalys (business impact analysis) genomföras. Enligt denna metod identifieras de kritiska processernas funktioner/anläggningar/system och de interna och externa resurser som krävs för att de identifierade processerna ska kunna genomföras som planerat. För var och en av de kritiska processerna identifieras maximalt tolerabla avbrottstider. Dessa tider anger hur länge den kritiska processen kan vara otillgänglig innan organisationen drabbas av intolerabla konsekvenser.

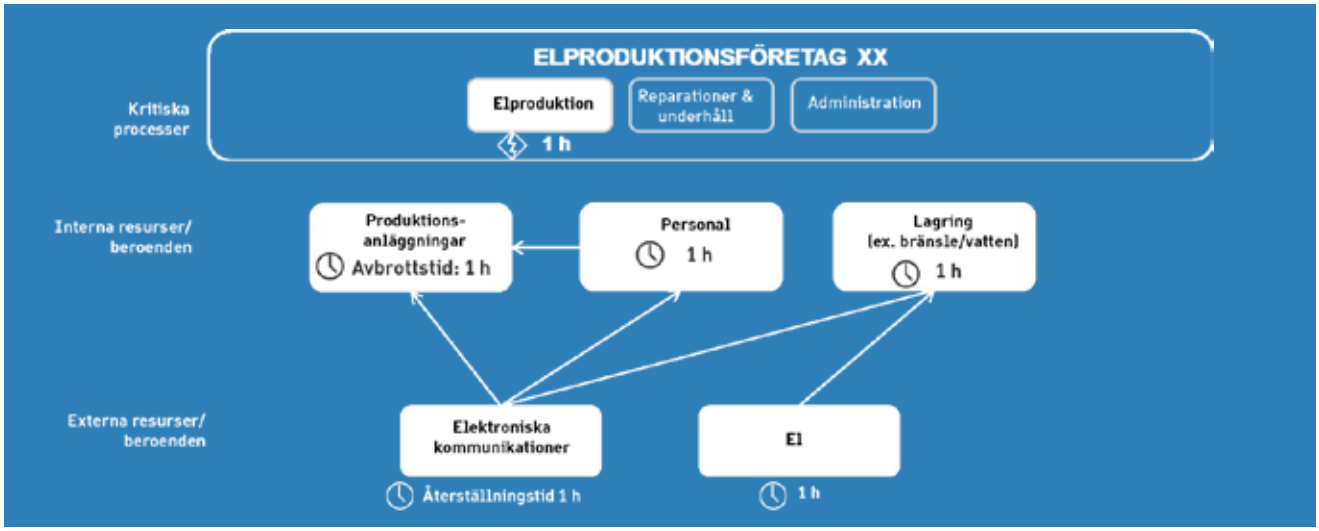
De maximalt tolerabla avbrottstiderna ställer krav på återställningstid för de stödjande resurserna. Detta tidskrav innebär att respektive resurs måste fungera igen inom en viss tid efter en störning så att överliggande process kan fungera inom uppsatta tidskrav. De processer och underliggande resurser med kortast tolerabla avbrottstiderna blir därmed de mest kritiska delarna av verksamheten och de delar som bör prioriteras i risk- och sårbarhetsanalysen och den efterföljande åtgärdsplanen.

I det förenklade exemplet i figur 4,5 och 6 beskrivs Organisationerna XX:s kritiska processer och underliggande processer och resurser. För var och en av processerna identifieras sedan de interna och externa resurser som krävs för att upprätthålla processen. Hur många nivåer av verksamheten man väljer att kartlägga i konsekvensanalysen kan anpassas beroende på hur djupt analysen behöver gå eller hur komplex verksamheten är. I ovanstående exempel skulle de övergripande processerna kunna vara indelade i ett antal underprocesser, som i sin tur är beroende av olika resurser.

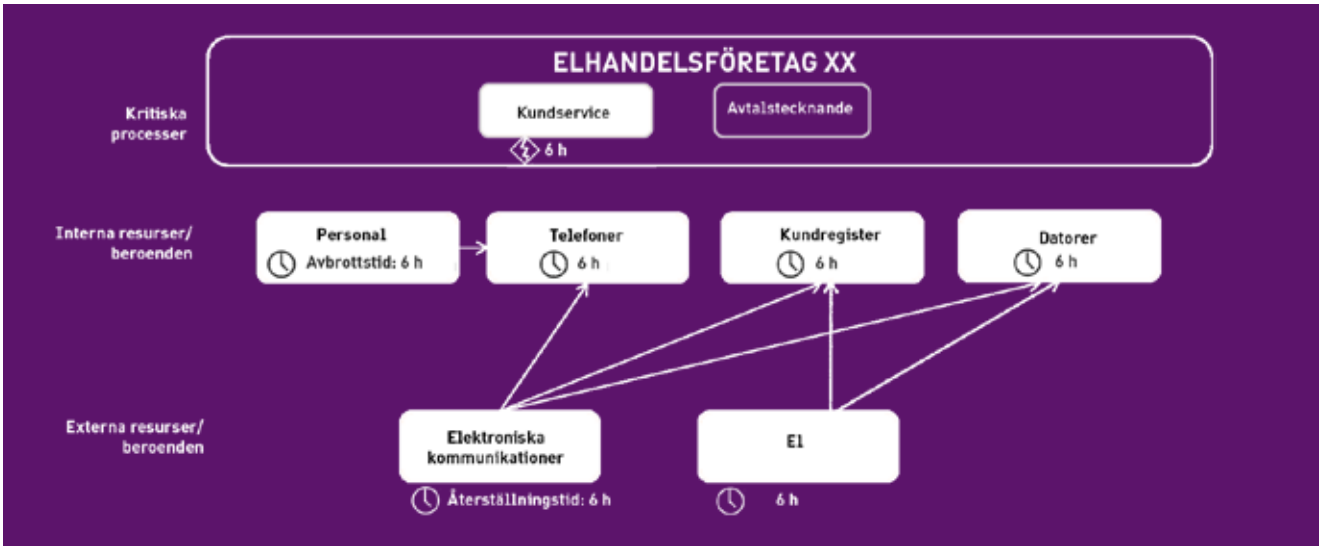
FOTO: TOMAS ÅRLEMO



Figur 4. Exempel på konsekvensanalys för elnätsföretag.



Figur 5. Exempel på konsekvensanalys för elproduktionsföretag.



Figur 6. Exempel på konsekvensanalys för elhandelsföretag.

KRAV OCH EXEMPEL

ELNÄTSFÖRETAG

För elnätsföretag gäller att dokumentationen av analysen ska inkludera en sortering av identifierade risker enligt nedanstående fem huvudgrupper. För respektive riskkategori ges också exempel på risker som kan ingå.

De fem huvudgrupperna, ej exemplen på risker, anges i Energimarknadsinspektionens föreskrifter. Ytterligare kategorier kan läggas till i de fall det anses relevant, men ovanstående fem grupper måste alltid finnas med i analysen.

1. Anläggningsteknik
a) Risker kopplade till ex. oisolerad luftledning, PEX-kablar från 1970-talet eller läckande oljekablar.
b) Samförläggning av ledningar i tunnlar där exempelvis en ledningsbrand kan slå ut flera förband, kanske även reservmatningen, eller styr- och övervakningskablar.
c) Huvudmatning och reservmatning in till stationer i gemensam ledningssträckning.
d) Tillgång till eller möjlighet att ansluta reservkraft.
e) Terrorism drabbar viktiga anläggningar.

Särskilda krav på regionnät:
f) Trädsäkrade luftledningar.
g) Redundans.
h) Kapacitet.

2. Enstaka anläggningsobjekt
a) Teknik och ålder – låg tillgänglighet på reservmaterial och brist på personal med relevant kompetens.
b) Risk för brand i t ex kabelkällare eller transformatorcell.
c) Utgående ledningars fördelning mellan olika skenor – ledningar som utgör redundans för varandra bör inte vara anslutna till samma skena. Även ledningarnas förläggning/placering inom stationen, kabelkällare och stationsområdet är avgörande för riskerna att få fel även i reserven.
d) Enskilda känsliga komponenter av mindre god kvalitet.
e) Dolda fel i kontrollanläggning, reläskydd och ej inkopplade redundanta anläggningsdela.

3. Nätstruktur
a) Enskilda noder där enstaka fel orsakar stora konsekvenser.

4. Organisation och arbetsprocesser
a) Bortfall av nyckelpersoner.
b) Strejk.
c) Ej tillgång till tillräckligt många entreprenörer.
d) Brister i informationssäkerhet.

5. Övrigt
a) Arbetsplatsolycka i samband med reparation drabbar anställd.
b) Arbetsplatsolycka i samband med reparation drabbar tredje part.
c) Leverantör av kritiska resurser kan ej leverera.

ELPRODUKTIONSFÖRETAG

Nedan listas exempel på hur risker kan grupperas för elproduktionsföretag. För respektive kategori anges också exempel på specifika risker.

1. Produktionsanläggningar
a) Väderhändelse förstör delar av anläggningen vilket medför produktionsbortfall.
b) Sabotage mot viktiga anläggningar.
c) Terrorism drabbar viktiga anläggningar.

2. Kritiska system
a) Elavbrott gör att organisationen inte kan komma åt de kritiska systemen.
b) Systemfel medför att de kritiska systemen är otillgängliga.
c) Sabotage, exempelvis cyberattack eller skadlig kod riktas mot ett eller flera kritiska system.

3. Organisation och arbetsprocesser
a) Bortfall av nyckelperson.
b) Pandemi medför stort personalbortfall.
c) Brister i informationssäkerhet.
d) Kritisk leverantör går i konkurs.
e) Leverans av kritiska resurser ej möjlig, exempelvis på grund av väderlek eller strejk.

4. Övrigt
a) Arbetsplatsolycka som medför dödsfall.
b) Arbetsplatsolycka som medför skada på anställd.
c) Arbetsplatsolycka som medför skada på tredje part.

ELHANDELSFÖRETAG

Nedan listas exempel på hur risker kan grupperas för elhandelsföretag. För respektive kategori anges också exempel på specifika risker.

1. IT-system

a) Elavbrott gör att kritiska IT-system blir otillgängliga.

b) Sabotage, exempelvis cyberattack eller skadlig kod riktas mot ett eller flera kritiska system.

c) Ej tillgång till kundregister, exempelvis på grund av tekniskt fel.

2. Organisation och arbetsprocesser

a) Kundtjänst kan ej hålla öppen, exempelvis på grund av personalbrist eller tekniskt fel.

b) Bortfall av nyckelperson.

c) Brister i informationssäkerhet.

d) Kritisk leverantör går i konkurs.

e) Ej tillgång till kritiska resurser.

3. Lokaler och fysiska tillgångar

a) Ej tillgång till organisationens lokaler, exempelvis på grund av brand eller översvämning.

b) Stöld av datorer.

4. Övrigt

a) Kundmissnöje.

b) Prisförändringar.

4.3 Analysfas

En risk är sammanvägningen av sannolikheten för att en händelse (en riskkälla) ska inträffa och de (negativa) konsekvenser händelsen i fråga kan leda till. En riskanalys är ett systematiskt sätt bedöma sannolikheten för de identifierade riskkällorna och deras omedelbara konsekvenser. En sårbarhetsanalys kan på motsvarande sätt beskrivas som ett systematiskt sätt att organisera och analysera kunskap och information om de konsekvenser i form av olika följdhändelser som en specifik risk medför.

Svenska kraftnät föreskriver inte att en specifik analysmetod ska användas, endast att arbetet ska ske systematiskt. Energimarknadsinspektionens föreskrifter anger att en etablerad analysmetod ska användas vid identifiering av riskkällor och uppskattning av risker, och i ett allmänt råd ges exempel på etablerade metoder. Dessa är grov-analys, felträdsanalys och händelseträdsanalys, så som de beskrivs i standard ISO 31 0101. I bilaga 1 finns en utförligare beskrivning av några metoder. Oavsett vilken metod som används är det alltid samma grundläggande delar som bör finnas med i sammanställningen av risk- och sårbarhetsanalysen. Vilken metod som väljs baseras på organisationens behov och förutsättningar såsom storlek på verksamheten, antalet involverade individer, samordning med andra processer i organisationen etc.

I denna vägledning genomförs analysfasen enligt nedanstående steg:

> Riskidentifiering
> Riskanalys
> Riskutvärdering
> Sårbarhetsanalys
> Åtgärdsplan

Beskrivningen av stegen avser att ge vägledning för att uppfylla lagstiftningens krav på risk- och sårbarhetsanalyser och baseras delvis på MSB: s vägledning för risk- och sårbarhetsanalyser för kommuner, landsting och statliga myndigheter (MSB245, 2011) men även på ISO 31000.

4.3.1 Riskidentifiering

Riskidentifieringen är en process för att upptäcka, kartlägga och beskriva riskkällor. Målet med riskidentifieringen är att skapa en lista över de typer av händelser som kan inträffa och som kan få stor påverkan på organisationens förmåga att leverera de tjänster den är tänkt att leverera.

TÄNK PÅ!

Utgångspunkten bör vara att samtliga riskkällor som anses vara av betydelse för den egna verksamheten och för elförsörjningen i stort inkluderas i riskidentifieringen.

Utgångspunkten för arbetet med riskidentifiering och urval bör vara att samtliga riskkällor som anses vara av betydelse för den egna verksamheten och för elförsörjningen i stort inkluderas i analysen. Även om en riskkälla kan tyckas osannolik kan konsekvenserna för samhället bli så omfattande att den anses oacceptabel och därför behöver den beaktas i analysen. Detta innebär att man bör beakta hela hotskalan, från olyckor och kriser till riskkällor av mycket ovanlig karaktär, för att få en uppfattning om den egna verksamhetens förmåga att hantera även sådana händelser som inträffar mer sällan men som kan innebära stora konsekvenser på samhällets elförsörjning. Denna typ av händelser benämns i elberedskapslagen som störningar som kan medföra svåra påfrestningar på samhället. Det ges inte någon exakt definition av vad som avses med sådana störningar, men vad som är kännetecknande kan sammanfattas på följande sätt:

> Händelser som är svåra att förutse och inträffar sällan.
> Händelser som trappas upp eller sprider sig mellan regioner och eller
viktiga samhällssektorer där det finns kritiska beroenden av/till elförsörjningen (såsom bränsleförsörjning, telekommunikationer, transporter osv.) och leder till allvarliga störningar i viktiga samhällsfunktioner.
> Händelser som kräver att olika aktörer i samhället (såväl myndigheter som privata aktörer) behöver samarbeta för att hantera situationen och begränsa konsekvenserna.

Både antagonistiska och icke-antagonistiska riskkällor kan leda till svåra påfrestningar på samhället, liksom riskkällor kopplade till höjd beredskap/krig. Riskidentifieringen bör också täcka in riskkällor som uppstår som följdeffekter av att en annan risk inträffar. För att underlätta identifieringen kan riskkällorna delas in i olika grupperingar. Se exempel på detta för respektive typ av aktör i exemplen på sidan 31–32.

Det finns flera olika metoder för hur riskidentifiering kan gå till. Vanliga metoder är Grovanalys, HAZOP (Hazard and operability analysis) Bow-tie och What if-analys. Exempel på riskkällor mot organisationer i elsektorn ges i Hotkatalog för elbranschen (Svenska Kraftnät Dnr: 2012/331, version 1.0). Fler riskkällor kan också identifieras genom att använda sig av erfarenheter och historisk data. Gemensamt för de olika metoderna är att de ofta utgår ifrån en beskrivning av systemet/verksamheten, antingen strukturellt eller funktionellt. Strukturella metoder beskriver en struktur, exempelvis verksamhets olika organisatoriska delar. De funktionella metoderna beskriver mer funktioner i verksamheten. De olika metoderna kan användas var för sig eller i kombination. En beskrivning av de vanligaste metoderna återfinns i bilaga 1.

I risk- och sårbarhetsanalysen är det viktigt att beskriva hur riskidentifieringen gått till och vilka avgränsningar som gjorts. Detta för att möjliggöra för enkel uppdatering av materialet, även om ansvariga personer byts ut. Vid redovisning av risk- och sårbarhetsanalyser till Svenska kraftnät och Energimarknadsinspektionen ingår att redovisa analysmetoder som använts för bland annat riskidentifieringen.

Sammanställningen av de identifierade riskkällorna vidareutvecklas sedan i nästa steg: riskanalysen.

FOTO: TOMAS ÅRLEMO

ATT ARBETA MED RISKER I HELA HOTSKALAN

Nedan listas några exempel på olika typer av händelsescenarier, som genom att orsaka sådana störningar i elförsörjningen och i andra viktiga samhällssektorer, kan medföra svåra påfrestningar på samhället. Scenarierna syftar till att ge stöd i metod och tankesätt, men bör inte användas som direkta ingångsvärden i arbetet. (Läs mer i Hotkatalog för elbranschen, Svenska kraftnät Dnr: 2012/331, version 1.0.)

Svåra naturhändelser som till exempel isstormar kan orsaka så omfattande skador på elnät och transformatorer att störningar i elförsörjningen även påverkar andra samhällsviktiga sektorer som är beroende av en fungerande elförsörjning, såsom telekommunikationssektorn och transporter.

Ett haveri i en stor kraftverksdamm belägen högt upp i en älv kan innebära omfattande översvämningar och skadeverkningar längs en stor del av vattendraget. De direkta konsekvenserna kan innefatta allvarliga skador på dammar och vattenkraftstationer, nätstationer och kraftledningar men även på annan infrastruktur som vägar, broar, telenät och bebyggelse i området. Samverkan mellan olika aktörer i området krävs för att hantera konsekvenserna av händelsen.

Riktad IT-attack mot styr- och kontrollsystem i en produktionsanläggning kan medföra störningar i elproduktionen inom ett visst område. Sker sådana attacker samtidigt mot flera produktionsanläggningar trappas händelsen upp. På ett liknande sätt kan en serie IT-attacker mot tekniska system hos elhandelsföretag drabba flera företag samtidigt.

En svår vinterstorm som leder till nedfallna träd, snövallar och skador på infrastruktur faller normalt inom elföretagens ansvar att kunna hantera. Men i kombination med exempelvis en svår influensaepidemi som påverkar tillgängligheten till personella resurser kan konsekvenserna bli mycket svårare för enskilda aktörer att klara av.

TÄNK PÅ!

Både riskkällor som kan ha sitt ursprung i den egna organisationen (exempelvis tekniska fel/fel i infrastruktur, materialfel och –brist, kompetensbrist osv.) och utanför den egna organisationen (exempelvis extrema väderhändelser, olyckor med farligt gods, stora bränder, sabotage, dataintrång mot verksamhetens kritiska system, spionage/informationsinhämtning, epidemier/pandemier, elektromagnetiska hot som kan slå ut kritisk infrastruktur osv.) kan utvecklas till händelser som kan medföra svåra påfrestningar på samhället.

TÄNK PÅ!

Endast risker som inte är av exceptionell karaktär ska rapporteras till Energimarknadsinspektionen, medan en begäran från Svenska kraftnät kan beröra risker som täcker hela hotskalan. Det är viktigt att ha i åtanke att det i flera fall inte finns någon tydlig gräns för i vilken kategori en riskkälla ska placeras, och att en och samma riskkälla därför kan behöva redovisas både till Energimarknadsinspektionen och till Svenska kraftnät.

4.3.2 Riskanalys

Riskanalysens huvudsakliga syfte är att definiera en risknivå för de identifierade riskkällorna genom att för varje risk besvara frågorna ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?”. I viss mån kan dessa frågor ha besvarats redan under riskidentifieringen, men i detta steg handlar det om att kvantifiera och att inkludera faktorer som påverkar sannolikhet och konsekvens. Organisationens nuvarande förmåga att hantera riskerna ska inkluderas i analysen. Det är också viktigt att inkludera beroenden mellan olika risker och deras riskkällor.

Riskanalysen kan genomföras med varierande grad av noggrannhet beroende på risk, syftet med analysen och vilken information som finns tillgänglig. Riskanalysen kan inkludera kvalitativa, semikvantitativa och kvantitativa metoder, samt kombinationer av dessa. Kvalitativa metoder definierar sannolikhet och konsekvens i termer av exempelvis låg, medium och hög tillsammans med förklaringar till vad dessa termer innebär. Semikvantitativa metoder använder beräkningar för att bedöma sannolikhet och konsekvens och kombinerar dessa för att bestämma en risknivå. Kvantitativa metoder sätter specifika värden på sannolikhet och konsekvens. Detta ger exakta risknivåer för de analyserade riskerna. En fullständig kvantitativ analys är inte alltid möjlig på grund av brist på information eller på grund av att analysen tar för mycket resurser i anspråk i relation till nyttan av en exakt värdering. Ofta är en kvalitativ eller semikvantitativ metod tillräcklig om de bedömningar som gjorts baserats på trovärdiga antaganden och av personer med rätt kompetens och erfarenhet.

Det finns flera sätt att svara på frågan hur sannolik en händelse är. Ett relativt enkelt, och ofta tillräckligt, sätt är att ange sannolikheten i intervall för att på så sätt minska behovet av en detaljerad bedömning. Med en mindre detaljerad bedömning är det dock viktigt att redogöra för de antaganden som görs i olika delar av bedömningen.

Beskrivningen av konsekvenser kan göras på olika sätt. Har man upprättat en kriteriemodell och fastställt definitioner för sannolikhet bör dessa utgöra centrala utgångspunkter i analysen. Bedöms inte risken ge en faktisk påverkan på något av de målområden som sattes upp i modellen, som till exempel liv och hälsa, ekonomi eller samhällets elförsörjning, behöver den inte inkluderas i den fortsatta analysen.

Nedanstående frågor kan ställas för att stötta i bedömningen av konsekvenser och deras omfattning:

> Vilka delar av verksamheten drabbas?
> Vilka följdhändelser kan inträffa?
> Hur stor är den geografiska omfattningen?
> Hur långvarig är störningen?
> Hur påverkas elförsörjningen i stort?
> Hur påverkas samhället över tiden?

FOTO: TOMAS ÅRLEMO

> Hur klarar vi händelsen ledningsmässigt?
> Hur klarar vi händelsen resursmässigt?
> Hur klarar vi informationshantering?

Oavsett vilken typ av konsekvensbedömning som används bör den information som ligger till grund för bedömningen redovisas. Vid bedömning av konsekvenser på samhällsnivå förväntas aktörerna i elsektorn inte bedöma dessa på en detaljerad nivå, utan endast i termer av relativ omfattning, exempelvis ”inga konsekvenser på samhället”, ”mindre konsekvenser för samhället”, ”måttliga konsekvenser för samhället” eller ”allvarliga konsekvenser för samhället”.

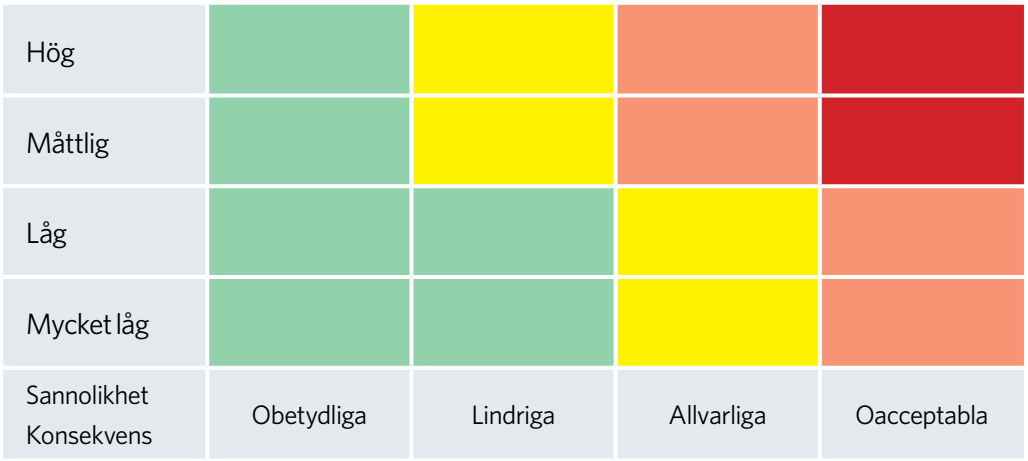
4.3.3 Riskutvärdering

Syftet med riskutvärderingen är att underlätta beslut kring vilka risker som kräver en djupare analys och därmed analyseras vidare i sårbarhetsanalysen. Riskutvärderingen resulterar också i beslutsunderlag för vilka risker som ska åtgärdas och hur dessa åtgärder ska prioriteras.

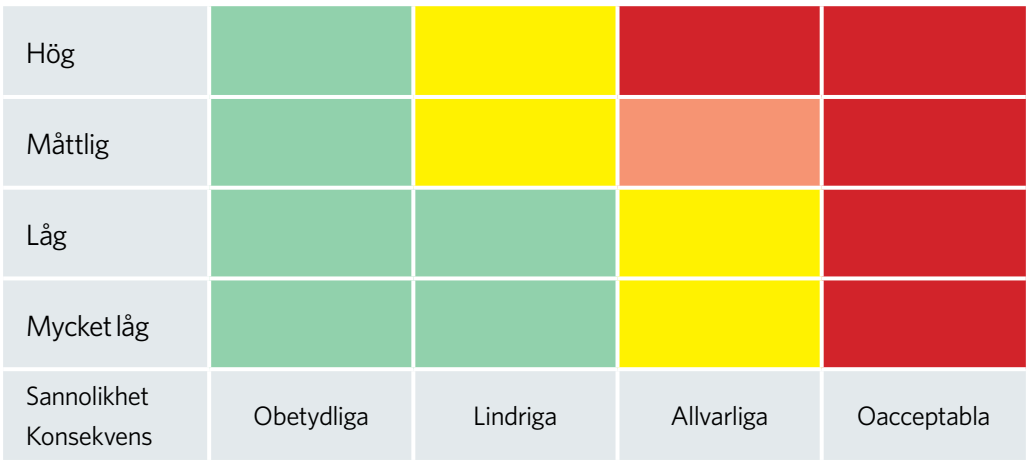
I riskutvärderingen jämförs risknivån (enligt riskanalysen ovan) för riskerna med de riskkriterier som satts upp i kriteriemodellen. Med hjälp av den kriteriemodell som togs fram i förberedelsefasen blir det enklare att föra över riskerna i en riskmatris och att vara konsekvent i bedömningarna (se exempel i figur 7). På detta sätt görs en bedömning av om en risknivå är tolerabel eller inte. Värderingen kring om en risk ska behandlas eller inte förbättras om den också inkluderar en kostnad-nyttoanalys. Utvärderingen används därefter som underlag för planering och genomförande av åtgärder.

En värdering som baseras på kvalitativa och semikvantitativa mått innehåller osäkerheter. Plottningen i riskmatrisen är främst för att visa hur risker förhåller sig till varandra, snarare än hur sannolikhet och konsekvens faktiskt förhåller sig. Riskvärderingen och matrisen kan fortfarande utgöra ett underlag vid prioritering av åtgärder.

En bedömning behöver göras av vilken vikt sannolikhetsaspekten ska ges i förhållande till konsekvensaspekten i riskutvärderingen. Sannolikheten är endast en uppskattning och enligt Svenska kraftnäts föreskrifter ska även händelser med låga sannolikheter ingå i analysen. Mot bakgrund av detta bör sannolikhetsaspekten inte väga lika tungt som konsekvensaspekten (se figur 8). Dock kan sannolikhetsbe-



Figur 7. Exempel på riskmatris.



Figur 8. Exempel på riskmatris där konsekvens ges högre vikt än sannolikhet.

dömningen ligga till grund för prioritering av åtgärder och investeringsbeslut kopplat till åtgärder som ryms inom kontrollansvaret och i detta avseende vara en relevant utgångspunkt.

Riskutvärderingen kan leda till ett beslut att ytterligare analys (sårbarhetsanalys) behövs. Det kan också leda till ett beslut om att risken inte ska behandlas, om det till exempel innebär höga kostnader för att behandla risken eller att åtgärden inte minskar risken tillräckligt mycket. Det är dock viktigt att fatta ett aktivt beslut om att inte behandla risken.

4.3.4 Sårbarhetsanalys

Baserat på riskutvärderingens resultat analyseras riskerna i de högsta risknivåerna, eller några av dem, vidare i en sårbarhetsanalys. Sårbarhetsanalysen är en fördjupad analys som syftar till att detaljerat analysera hur allvarligt och omfattande en specifik risk påverkar den egna organisationen samt att bedöma organisationens förmåga att förebygga, motstå och hantera risken. Med hjälp av analysen identifieras därmed organisationens sårbarheter, förmåga att hantera konsekvenserna och en identifiering av brister i denna förmåga.

Tyngdpunkten i en sårbarhetsanalys bör vara att analysera vilka konsekvenser en viss händelse för med sig och hur organisationen hanterar, motstår och återhämtar sig från dessa. De konsekvenser som den egna verksamheten inte kan förutse, motstå, hantera och återhämta sig ifrån indikerar hur sårbar organisationen är för en specifik händelse. Sårbarhetsanalysen utgår ifrån den egna verksamheten och de processer/system som måste fungera för att kunna upprätthålla verksamheten. Se avsnitt 4.2.4 om hur de mest kritiska delarna av verksamheten kan identifieras.

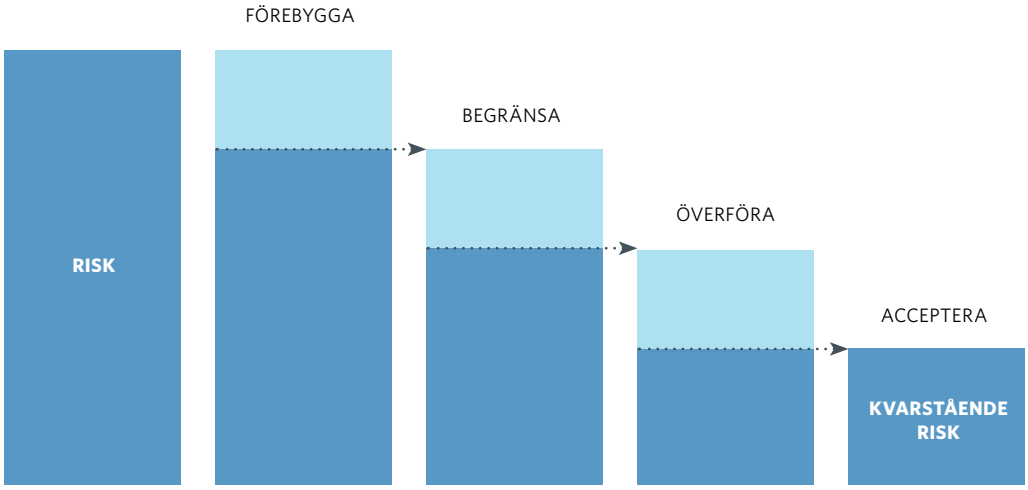
Förslagsvis väljs ett antal olika risker ut årligen för närmare analys av organisationens förmåga. Det kan vara fördelaktigt att beskriva dessa i form av scenarier. Scenarierna bör vara skilda i det avseendet att de leder till olika typer av konsekvenser. Ett sätt att analysera scenarierna kan vara genom övningar, där förmågan att förebygga, motstå, hantera och återställa testas. Övningarna kan antingen ge ingångsvärden till den fortsatta analysen, alternativt verifiera resultaten av analysen och de vidtagna åtgärderna. För mer information om hur scenarier kan användas i en sårbarhetsanalys, se t.ex. MSB:s ”Vägledning för risk- och sårbarhetsanalyser” (MSB245, 2011).

Sårbarhetsanalysen avslutas med en utvärdering av identifierade sårbarheter och organisationens uppskattade förmåga att hantera analyserade scenarier. Förmågan kan med fördel bedömas utifrån de två kriterierna ”Förmåga att förebygga, motstå och hantera händelse X” och”Bristande förmåga att förebygga, motstå och hantera händelse X.” Med utgångspunkt i denna utvärdering görs sen bedömning av vilka åtgärder som bör vidtas och de dokumenteras i en åtgärdsplan.

4.3.5 Åtgärdsplan

För att öka organisationens förmåga att förebygga, motstå och hantera störningar ska en åtgärdsplan utarbetas med utgångspunkt i risk- och sårbarhetsanalysen. Åtgärdsplanen ska innehålla prioriteringar om hur identifierade risker och sårbarheter ska behandlas (åtgärdas). Åtgärdsplanen bör användas löpande i verksamheten och uppdateras regelbundet då nya åtgärder tillkommer eller då åtgärder vidtagits. Åtgärdsplanen kan exempelvis ligga till grund för verksamhetsplanering och budgeteringsarbete. Hålls åtgärdsplanen kontinuerligt uppdaterad fungerar den också som underlag vid revidering av risk- och sårbarhetsanalysen.

Åtgärderna kan syfta till att förebygga sannolikheten för att risker inträffar, begränsa negativa konsekvenser av inträffade händelser eller en kombination av dessa (se figur



Figur 9. Olika typer av riskbehandlingar.

5). Exempel på att förebygga risker kan vara skalskydd och liknande. Ett annat alternativ att förebygga kan vara att helt eliminera risken genom att förändra de processer/rutiner som föranleder risken och arbeta på andra sätt. Dessa arbetssätt kan dock leda till andra risker.

Att begränsa en risk innebär att minska konsekvenserna av den (se figur 9). Det kan exempelvis handla om att att skapa rutiner för snabb och effektiv övergång till reservsystem vid ett avbrott i ordinarie system eller andra åtgärder för att öka förmågan att hantera en störning. Överföring av risk innebär oftast att en tredje part tar över risken, till exempel genom försäkringar där främst finansiella konsekvenser överförs. Det är dock viktigt att inse att ansvaret, och därmed de flesta risker, stannar kvar hos den egna organisationen. Överföring av risk innebär alltså att nya risker uppstår som bör identifieras och analyseras.

Olika riskbehandlingsmetoder kan kombineras och en kombination av olika metoder är ofta det bästa för att få ner kvarstående risk till en tolerabel nivå. Ett visst mått av risk kvarstår så gott som alltid, oavsett behandlingsmetod. Hur stor denna kvarstående risk blir beror bland annat på vilka risker och risknivåer organisationen är beredd att acceptera och en bedömning av kostnad jämfört med bedömd nytta (minskning av risken).

Att välja att acceptera identifierade och analyserade risker bör alltid vara ett aktivt beslut med en dokumenterad motivering. För de risker som inte ska åtgärdas, alternativt åtgärdas på längre sikt, bör en beredskapsplan tas fram så att organisationen kan agera för att minska konsekvenserna och eller upprätthålla kritiska processer om risken inträffar.

Åtgärdsplanen ska dokumenteras och alla identifierade åtgärdsbehov bör inkluderas i planen. För elnätsföretag finns krav i Energimarknadsinspektionens föreskrifter på vilken information åtgärdsplanen ska innehålla (se 4.4.3). För samtliga företag bör dock åtgärdsplanen beskriva vilka åtgärder som ska vidtas och vilka risker som tolereras. Åtgärderna bör vara tidssatta (se också 4.4.3), samt prioritetsordningen för dem och vilken risk de hör ihop bör vara tydligt. Åtgärdsplanen kan också inkludera motivering till de olika åtgärderna inklusive förväntad kvarstående risk, ansvariga för genomförande och beslut, resursbehov och kostnader, hur nyttan dvs minskning av risken kan mätas, rapporteringskrav och tidplan.

Åtgärdsplanen och dess åtgärder bör följas upp regelbundet. Hur risker och sårbarheter samt organisationens förmåga utvecklas blir ett viktigt underlag till nästa risk- och sårbarhetsanalys. För att följa upp analysen och åtgärdsplanen kan t.ex. övningar användas. Övningarna kan genomföras i mindre skala för att exempelvis testa enskilda system eller rutiner, eller i större skala för att testa verksamhetens övergripande förmåga att motstå och hantera en störning. Ett förslag är att öva de risker (scenarier) som analyseras i sårbarhetsanalysen. Verifieringen av genomförda åtgärder kan också ske genom testning av nya system eller genom bedömning av intern/extern part.

TABELL 8. EXEMPEL PÅ VAD EN ÅTGÄRDSLISTA BÖR INNEHÅLLA

ÅTGÄRD (IDENTITET)	ANSVARIG	TIDPLAN	BEDÖMD EKONOMISK OMFATTNING
Åtgärd 1 (X001)	Anna Andersson	Omgående	10 000-20 000 SEK
Åtgärd 2 (X002)	Bo Bengtsson	På kort sikt	>1 000 000 SEK
Åtgärd 3 (X003)	Calle Carlsson	Omgående	50 000-75 000 SEK
Åtgärd 4 (X004)	Dan Davidsson	På kort sikt	400 000-600 000 SEK

KRAV FÖR ELNÄTSFÖRETAG

Enligt Energimarknadsinspektionens föreskrifter ska åtgärdsplanen innehålla information baserad på risk- och sårbarhetsanalysen. Åtgärdsplanen ska vidare tydligt visa vilka risker som ska åtgärdas och vilka dessa åtgärder är. Varje åtgärd ska ges en unik identitet och sorteras in under samma grupper som vid riskidentifieringen.

4.4 Rapporteringsfas

4.4.1 Dokumentation

För att kunna genomföra en väl underbyggd rapportering och kommunikation av resultatet av risk- och sårbarhetsanalysen internt och externt (bland annat till myndigheter) krävs det att risk- och sårbarhetsanalysen dokumenteras. Till exempel anger Energimarknadsinspektionen i sina föreskrifter (2013:3) att åtgärdsplanen ska dateras och sparas i minst 10 år. De utgångspunkter som använts och de avgränsningar som gjorts bör framgå i dokumentationen, för att andra än de som upprättat risk- och sårbarhetsanalysen ska kunna se vilka antaganden som gjorts. Dokumentationen bör också beskriva val av metod, vilka författningar och regleringar som följts, vilken typ av risker och sårbarheter som inkluderats etc.

KRAV FÖR ELNÄTSFÖRETAG

För elnätsföretag gäller att arbetet ska dokumenteras på ett sådant sätt att det ger en komplett bild av det arbete som har lett fram till resultaten. Arbetsprocessen ska utan svårighet kunna rekonstrueras baserat på skriftligt material. Dokumentationen ska sparas i minst 10 år.

Av dokumentationen bör det dessutom framgå vilka som har utfört arbetet och vilken del av organisationen de arbetar i. Utgångspunkter, avgränsningar, valda antaganden, metoder, indata och resultat bör också framgå. Vidare bör alla viktiga ställningstaganden som har gjorts under analys- och värderingsarbetet beskrivas tydligt.

EXEMPELMALL FÖR RSA-RAPPORT

1. Sammanfattning

Kort sammanfattning av arbetet och resultaten.

2. Inledning

2.1.Syfte och mål

Förklara kort syfte och mål med analysen, kan till exempel baseras på verksamhetsmål eller liknande.

2.2 Deltagare i analysgruppen

Lista processledare och deltagare i arbetsgruppen. Ange namn och befattning/funktion.

2.3 Avgränsningar och utgångspunkt

Beskriv vilka avgränsningar som gjorts och de utgångspunkter som använts under analysarbetet.

2.4 Bakgrund

Kort om varför RSA-arbetet genomförts.

3. Om företaget

Presentera företaget och verksamheten – anläggningar, verksamhetsområden, särskilda förutsättningar, viktiga kunder med mera. Denna del kan med fördel innehålla en systembeskrivning med anläggningsdata, eventuella redundansplanering, störningsstatistik, med mera.

3.1 Kartläggning av nuläget

Beskriv organisationens verksamhet och den omvärld den verkar i.

3.2 Indentifiering av kritiska funktioner i verksamheten

Beskriv organisationens kritiska funktioner/processer och deras beroenden.

4. Metod

Beskriv övergripande vilken metod företaget valt att använda i risk- och sårbarhetsanalysarbetet.

4.1 Kriteriemodeller

Presentera organisationens acceptanskriterier.

5. Analys

5.1 Riskidentifiering

Förklara metod för identifiering av risker relevanta för verksamheten.

Lista identifierade risker samt dessas påverkan på företaget/verksamheten.

5.2 Riskanalys

Redovisning av resultaten av företagets riskanalys, det vill säga uppskattning av sannolikhet och konsekvens utifrån vald metod.

5.3 Riskutvärdering

Sammanställning av företagets risker i en riskmatris /ett heat chart och en redovisning av företagets bedömning av vilka risker för vilka åtgärder ska vidtas och/eller som kräver djupare analys.

Förslagsvis kan man dela upp visualiseringen i två matriser – dels en matris där samtliga risker placeras ut, dels en separat där företagets 10 största risker tydliggörs och placeras ut med unik identifikation (ex. R001, R002, R003 osv)

5.4 Sårbarhetsanalys

Redovisning av resultatet av företagets sårbarhetsanalys och förmågan att hantera/motstå identifierade risker.

5.5 Åtgärdsförslag

Lisa åtgärdsförslag för de, enligt ovan listade, största riskerna. Listan bör innehålla en förklaring av vad som ska göras, vem som ansvarar för detta, tid för genomförande av åtgärder samt förväntat resultat.

6. Referenser/Källor

Ange vilka eventuella föreskrifter, metoddokument, vägledningar eller liknande som väglett arbetet.

7. Bilagor

4.4.2 Intern kommunikation

För att på ett effektivt sätt tillvarata resultatet från risk- och sårbarhetsanalys i den egna organisationen krävs en strukturerad process för analysen samt en medvetenhet kring denna process i organisationen och nyttan av analysen (se Inledningen).

För att risk- och sårbarhetsanalysen ska öka organisationens förmåga att förebygga, motstå och hantera risker bör kommunikationen av den planeras genom till exempel en kommunikationsplan där mål, målgrupper och kanaler för kommunikationen anges.Den kan tas fram redan under förberedelsefasen, se 4.2.1. I planen är det också lämpligt att ange hur uppföljningen av kommunikationsinsatserna ska ske. De åtgärdsförslag som identifieras kan med fördel tilldelas ansvariga från alla delar av verksamheten och när åtgärder vidtas bör effekten utvärderas. En viktig framgångsfaktor för att resultatet av arbetet med risk- och sårbarhetsanalyser ska komma till nytta i hela organisationen är att ledningen inser och betonar vikten av att upprättandet av risk- och sårbarhetsanalyser.

4.4.3 Rapportering till Energimarknadsinspektionen

Rapporteringen till Energimarknadsinspektionen beskrivs i Energimarknadsinspektionens föreskrifter (2013:3), 13-18§§. Elnätsföretag ska årligen rapportera, baserat på sin risk- och sårbarhetsanalys och åtgärdsplan, till Energimarknadsinspektionen. Detta ska ske i elektronisk form senast under juli månad varje år och analysen får inte vara äldre än ett år.

Formuläret för rapportering finns på Energimarknadsinspektionens webbplats, www.ei.se. Notera att det ifyllda formuläret inte kommer att sekretessbeläggas vilket måste beaktas då fritextavsnitten eventuellt fylls i. På Energimarknadsinspektionens webbplats finns också en särskild handbok om rapporteringen.Redovisningen av risk- och sårbarhetsanalysen ska innehålla följande information:

> Använd analysmetod.
> Om en riskmatris använts för presentation av sannolikhet och konsekvens.
> Antal identifierade risker och antal risker som ska åtgärdas, fördelade på huvudgrupperna.
> Om redovisningsenheten klarar att uppfylla funktionskravet.

Redovisningen av åtgärdsplanen ska innehålla följande information:

> Antalet åtgärder.
> Om varje åtgärd märkts med en unik identitet.
> Tidplan för genomförande.
> Om tidplanen ändrats sedan senaste redovisning.

FOTO: TOMAS ÅRLEMO

Kraven i ellagen och i Energimarknadsinspektionens föreskrifter, vilka gäller för elnätsföretag, anger att riskkällor av exceptionell karaktär och som inte omfattas av nätkoncessionsinnehavarens kontrollansvar får undantas från risk och sårbarhetsanalysen. Krig och terrorhandling definieras som risker av exceptionell karaktär och kan därför undantas från rapporteringen.

De inrapporterade uppgifterna ligger till grund för granskning och tillsyn som sker i två steg:

1. Energimarknadsinspektionen kommer att granska alla inlämnade uppgifter avseende rimlighet.
2. Den kompletta risk- och sårbarhetsanalysen och åtgärdsplanen kan, genom stickprov eller annat urval, komma att granskas på plats hos företaget.

4.4.4 Uppgiftslämnande till Svenska kraftnät

Svenska kraftnät kan begära uppgifter ur företagens risk- och sårbarhetsanalyser som underlag till den nationella risk- och sårbarhetsanalysen för elsektorn (SvKFS 2013). Uppgifterna ska lämnas vid den tidpunkt som Svenska kraftnät anger i sin begäran.

Risk- och sårbarhetsanalysen behöver inte redovisas till myndigheten i sin helhet. Den information Svenska kraftnät begär in enligt §8 i föreskrifterna (SvKFS 2013:2) inkluderar följande:

> Identifierade riskkällor som kan orsaka sådana störningar i elförsörjningen vilka bedöms kunna medföra svåra påfrestningar på samhället.
> Identifierade kritiska beroenden kopplat till redovisade riskkällor.
> Identifierade brister och sårbarheter kopplat till redovisade riskkällor.
> Identifierade åtgärdsbehov som inte omfattas av uppgiftslämnarens ansvar.

Detta underlag är av en inventerande karaktär och Svenska kraftnät kan behöva fördjupad information kopplad till olika riskkällor. Därför kan Svenska kraftnät också begära in kompletterande information om konsekvenser, sårbarhet, förmåga att motstå och hantera störningar samt åtgärdsbehov kring riskkällor som identifierats i den nationella risk- och sårbarhetsanalysen. Det kan till exempel röra sig om uppgifter kopplade till riskkällor som företag redovisat vid den mer inventerande uppgiftslämningen eller riskkällor som Svenska kraftnät identifierat i sitt eget analysarbete. Det kan även handla om riskkällor som regeringen eller MSB begärt att Svenska kraftnät ska analysera. En faktisk inträffad händelse kan också föranleda ett behov av att begära in underlag för analys och inriktning av elberedskapsåtgärder.

Alla företag som omfattas av elberedskapslagen och därmed av skyldigheten att genomföra risk- och sårbarhetsanalys är dock inte skyldiga att på begäran lämna uppgifter till Svenska kraftnät. Följande är undantagna från skyldigheten att lämna uppgifter enligt 4 § första stycket 3 i elberedskapslagen:

> Den som bedriver produktion av el om produktionen enbart sker i anläggningar som inte omfattas av anmälningsskyldighet enligt 7§ elberedskapslagen.
> Den som bedriver överföring av el med stöd av nätkoncession om ingen del av verksamheten omfattar anläggning med anmälningsskyldighet enligt 7§ elberedskapslagen.
> Den som bedriver handel med el utan eget balansansvarsavtal med Svenska kraftnät

5. SEKRETESS

De uppgifter som finns i en färdigställd risk- och sårbarhetsanalys kan vara skyddsvärda, då de visar på befintliga och potentiella sårbarheter i verksamheten och andra resurser. Det är därför viktigt att ta hänsyn till behovet av att skydda vissa uppgifter så att de inte ska kunna användas för angrepp mot företaget eller elförsörjningen i stort. I den interna hanteringen kan det till exempel handla om att skapa en medvetenhet om vilken typ av information som bör skyddas, vikten av att hantera denna information enligt företagets rutiner och att klassificera information så att samtliga personer som hanterar uppgifterna är medvetna om uppgifternas karaktär.

När uppgifter lämnas till en myndighet, som till exempel Svenska kraftnät eller Energimarknadsinspektionen, omfattas handlingen av offentlighetsprincipen. Offentlighetsprincipen innebär att var och en kan vända sig till en myndighet och begära ut en allmän handling. Huvudregeln är att alla handlingar som kommer in till eller skickas ut från myndigheten i princip är allmänna och offentliga. Myndigheter har dock möjlighet att sekretessbelägga uppgifter i allmänna handlingar, till exempel med hänsyn till rikets säkerhet eller om det berör uppgifter om myndighetens risk- och sårbarhetsanalyser. I samband med att uppgifter ska lämnas till en myndighet bör företaget bidra till myndighetens sekretessbedömning genom att informera om företaget bedömer att uppgifterna är skyddsvärda eller inte. Om uppgifterna är skyddsvärda ska företaget ange skälen till detta.

Bedömer företaget att uppgifter som lämnas till Svenska kraftnät är skyddsvärda ska företaget klassificera handlingen. Är en handling klassificerad som skyddsvärd hanteras uppgifterna i enlighet med denna fram till dess att behov av att genomföra en sekretessprövning uppstår. Innan uppgifterna lämnas ut till Svenska kraftnät kan också företaget föra en dialog med myndigheten kring dessa frågor för att komma fram till hur uppgifter som bedöms vara skyddsvärda ska hanteras i det specifika fallet.

FOTO: TOMAS ÅRLEMO

6. LÄS MER

Handböcker och vägledningar

Vägledning för Risk- och sårbarhetsanalyser, MSB (MSB245, 2011).

Vägledning för samhällsviktig verksamhet: att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid, MSB (MSB260, 2014).

Handbok för redovisning av risk- och sårbarhetsanalys samt åtgärdsplan. Version 7.0. Energimarknadsinspektionen.

Risk- och sårbarhetsanalyser för elnät – vägledning för elnätsföretag, Svensk Energi (2010).

Vägledning säkerhetsanalys, Svenska kraftnät (2005).

Vägledning IS/IT-säkerhet samt säkerhetsskydd, Svenska kraftnät, Version 1.0 (2014).

Hotkatalog för Elbranschen – Hot mot IT-, informationshantering, processkontroll och automation, Version 1.0, Svenska kraftnät (2014).

Standarder

SS-ISO 31000:2009 Riskhantering – Principer och riktlinjer (ISO 31000:2009, IDT).

IEC/ISO 31010:2009 Risk management – Risk assessment techniques.

ISO 55000:2014 Ledningssystem för tillgångar – översikt, principer och terminologi.

7. TERMER OCH BEGREPP

Anläggning:

En fast byggnadskonstruktion på land eller vatten. I anläggning inkluderas bland annat infrastruktur för styrnings- och övervakningssystem och talkommunikationer.

Elnät:

En nätkoncessionsinnehavares sammankopplade elektriska anläggningar för överföring av el som innehas med nätkoncession för linje eller med nätkoncession för område.

Funktionskravet:

Det minimikrav på leveranssäkerhet som följer av 3 kap. 9a § ellagen och som innebär att leveransavbrott i överföringen av el till en elanvändare aldrig ska överstiga 24 timmar. Kravet gäller inom ramen för koncessionshavarens kontrollansvar.

Händelse:

Förekomst eller förändring av särskilda omständigheter.
ANM. 1: En händelse kan vara en eller flera förekomster och ha flera orsaker.
ANM. 2: En händelse kan utgöras av något som inte inträffar.
ANM. 3: En händelse kan ibland refereras till som en ”incident” eller ”olycka”.
ANM. 4: En händelse utan konsekvenser kan benämnas som ”nästan en miss”,
”incident”, ”nästan en träff” eller ”nära ögat”.

Konsekvens:

Utfall från en händelse.
ANM. 1: en händelse kan leda till ett flertal olika konsekvenser.
ANM. 2: en konsekvens kan vara säker eller osäker och kan ha positiva eller negativa effekter på målen.
ANM. 3: Konsekvenser kan uttryckas kvalitativt eller kvantitativt.
ANM. 4: Initiala konsekvenser kan eskalera genom dominoeffekter.

Kontinuitetshantering:

Att långsiktigt etablera och kontinuerligt vidmakthålla en förmåga att upprätthålla sin verksamhet oavsett vad som inträffar.

Kritiska beroenden:

Beroenden som är avgörande för att samhällsviktiga verksamheter ska kunna fungera. Sådana beroenden karaktäriseras av att ett bortfall eller en störning i levererande verksamheter relativt omgående leder till sådana funktionsnedsättningar som kan få till följd att en allvarlig kris inträffar. Den drabbade verksamheten kännetecknas av att den saknar uthållighet, redundans och möjlighet att ersätta eller fungera utan den resurs som fallit bort.

Kvarstående risk:

Risk som kvarstår efter riskbehandling.

Risk:

En sammanvägning av sannolikheten för att en händelse ska inträffa och de (negativa) konsekvenser händelsen i fråga kan leda till (EIFS 2013:3). Osäkerhetens effekt på mål.
ANM. 1: En effekt är en avvikelse från det förväntade – positiv och/eller negativ.
ANM. 2: Mål kan ha olika aspekter (såsom ekonomi, hälsa och säkerhet eller miljömål) och kan gälla på olika nivåer (såsom strategisk-, organisatorisk-, projekt-, produkt- eller processnivå).
ANM. 3: Risker karaktäriseras ofta genom hänvisning till potentiella händelser och konsekvenser, eller genom en kombination av dessa.
ANM. 4: Risker uttrycks ofta i termer av en kombination av en händelses konsekvenser och därtill relaterad sannolikhet för förekomst.
ANM. 5: Osäkerhet är det tillstånd, även partiellt, av bristande information som relaterar till förstående för eller kunskap om en händelse, dess konsekvenser eller sannolikhet.

Riskanalys:

Process för att förstå riskens natur och för att avgöra risknivån.
ANM. 1: Riskanalys utgör grunden för riskutvärdering och för beslut om riskbehandling.
ANM. 2: Riskanalys inkluderar riskuppskattning.

Riskattityd:

Organisationens inställning till att bedöma och därefter eftersträva, behålla, ta eller avstå ifrån risker.

Riskbedömning:

Övergripande process för riskidentifiering, riskanalys och riskutvärdering. Process för att förändra risker.

Riskbehandling:

ANM. 1: Riskbehandling kan omfatta att:
> Undvika risken genom beslut att inte inleda eller fortsätta med den aktivitet som ger upphov till risken
> Ta eller öka risken för att kunna tillvarata en möjlighet.
> Eliminera riskkällan.
> Förändra sannolikheten.
> Förändra konsekvenserna.
> Dela risktagandet med annan part eller parter (inklusive avtal och riskfinansiering).
> Behålla risker genom välgrundade beslut.

ANM. 2: Riskbehandling som behandlar negativa konsekvenser benämns ibland ”riskminimering”, ”riskeliminering”, ”riskförebyggande” och ”riskreducering”.
ANM. 3: Riskbehandling kan skapa nya risker eller förändra befintliga risker.

Riskhantering:

Samordnade aktiviteter för att styra och leda en organisation med avseende på risk.

Riskidentifiering:

Process för att upptäcka, kartlägga/känna igen och beskriva risker. Referensförhållanden mot vilka betydelsen av en risk utvärderas.

Riskkriteria:

ANM. 1: Riskkriterier baseras på organisationens mål samt dess externa och interna kontext.
ANM. 2: Riskkriterier kan härledas från standarder, lagar, policys och andra krav.

Riskkälla:

[EIFS 2010:3] En händelse eller ett tillstånd som kan leda till negativa konsekvenser i form av leveransavbrott.
[ISO 31000] Element som i sig självt eller i kombination har en inneboende potential att utgöra en risk.

Risknivå:

Storlek på en risk eller kombination av risker, uttryckt i termer av en kombination av konsekvenser och deras sannolikhet.

Riskutvärdering:

Process för att jämföra resultaten från riskanalysen med riskkriterierna för att avgöra om risken och/eller dess storlek är acceptabel eller godtagbar.

Samhällsviktig verksamhet:

En verksamhet som uppfyller minst ett av följande villkor:

> Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
> Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

Sannolikhet:

Chans att någonting inträffar.

Systematiskt säkerhetsarbete:

Ett samlingsbegrepp för en verksamhets organiserade arbete med all form av säkerhet.

Sårbarhet:

Oförmåga att motstå eller återhämta sig från en händelse eller ett tillstånd som utgör en riskkälla.

SVENSKA KRAFTNÄT