LUND UNIVERSITY

Användning av risk- och sårbarhetsanalyser i samhällets krishantering - delar av en bakgrundsstudie

Abrahamsson, Marcus; Magnusson, Sven Erik

2004

Link to publication

Citation for published version (APA):
Abrahamsson, M., & Magnusson, S. E. (2004). *Användning av risk- och sårbarhetsanalyser i samhällets krishantering - delar av en bakgrundsstudie*. (LUCRAM; Vol. 1007). LUCRAM, Lund University.

Total number of authors:
2

General rights
Unless other specific re-use rights are stated the following general rights apply:
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Read more about Creative commons licenses: https://creativecommons.org/licenses/

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

LUND UNIVERSITY

PO Box 117
221 00 Lund
+46 46-222 00 00

Download date: 09. Feb. 2026

Lund 2004
Rapport 1007

Användning av risk- och sårbarhetsanalyser i samhällets krishantering

– delar av en bakgrundsstudie

Marcus Abrahamsson
Sven Erik Magnusson

Projekt finansierat av
Krisberedskapsmyndigheten

INNEHÅLLSFÖRTECKNING

DEL I – BAKGRUNDSMATERIAL **7**

1 BAKGRUND **9**

2 PROJEKTETS MÅLSÄTTNING, FÖRUTSÄTTNINGAR OCH BEGRÄNSNINGAR **11**

3 GENOMFÖRANDE **13**

3.1 PROJEKTETS GENOMFÖRANDE OCH TILLGÄNGLIG KOMPETENSBAS 13
3.2 DISPOSITION AV RAPPORT 13

4 BEGREPPEN SVÅR PÅFRESTNING OCH KRISHANTERING **16**

4.1 BEGREPPET SVÅR PÅFRESTNING 16
4.2 BEGREPPET KRISHANTERING 16
4.2.1 FEMA ramverk för krishantering *17*
4.2.2 CCMD ramverk för krishantering *18*
4.2.3 Krishantering och den nya hotbilden *20*

5 BEGREPPEN RISKANALYS OCH SÅRBARHETSANALYS **21**

5.1 INLEDNING 21
5.2 RISK, RISKANALYS OCH RISKHANTERING 21
5.2.1 Risk och riskperspektiv *21*
5.2.2 Riskanalys och riskhantering *23*
5.2.3 Riskanalyser och allmänna kvalitetskrav *25*
5.3 KORT SAMMANFATTNING AV DEN VETENSKAPLIGA BAKGRUNDEN FÖR ATT KLASSIFICERA RISKTYPER, RISKEVALUERINGSMETODER OCH RISKHANTERINGSSTRATEGIER 28
5.4 OLIKA ASPEKTER PÅ SÅRBARHETSBEGREPPET 29
5.5 RELATIONEN SÅRBARHET, HOT OCH RISK 32

6 MYNDIGHETSROLLER SAMT EN MODELL AV KRISHANTERINGENS UPPBYGGNAD **33**

6.1 MYNDIGHETERS OLIKA ROLLER 33
6.2 EN MODELL AV MYNDIGHETERS KRISHANTERINGSVERKSAMHET 34

7 MYNDIGHETSFÖRESKRIFTER PÅ SÄKERHETSOMRÅDET: NÅGOT OM STRUKTUR OCH UTVECKLING **36**

7.1 INLEDNING 36
7.2 NÅGOT OM OLIKA TYPER AV FÖRESKRIFTER OCH KONTROLLVERKSAMHET 36
7.2.1 Olika typer av föreskrifter *36*
7.2.2 Ett ramverk för bestämmelseskrivande, regelverk och kontroll *37*
7.3 RISK- OCH SÅRBARHETSANALYSER OCH DE TRE OLIKA FÖRESKRIFTSREGIMERNA 39

8 OLIKA TYPER AV GRUNDORSAKER TILL SVÅRA PÅFRESTNINGAR **40**

8.1 GRUNDLÄGGANDE ORSAKER TILL SVÅRA PÅFRESTNINGAR ENLIGT TYP 1 40
8.1.1 Olyckor av typ 1. En förklaringsmodell *41*
8.1.2 Interdependens i tekniska infrastruktursystem; speciellt el- och vattenförsörjning *43*
8.2 GRUNDLÄGGANDE ORSAKER TILL SVÅRA PÅFRESTNINGAR ENLIGT TYP 2: NATURKATASTROFER 43
8.3 GRUNDLÄGGANDE ORSAKER TILL SVÅRA PÅFRESTNINGAR ENLIGT TYP 3: TERRORISM OCH ANDRA TYPER AV AVSIKTLIG PÅVERKAN ELLER SKADA 44
8.4 FENOMENET EXTREMA HÄNDELSER 44
8.5 NÅGRA TEORIER OM KRISERS ORSAKER OCH UPPKOMST: SAMBANDET RISKHANTERING – KRISHANTERING 45
8.6 NÅGRA SLUTSATSER VAD GÄLLER RISK- OCH SÅRBARHETSANALYS ENLIGT FÖRORDNING 2002:472 47

9 STANDARDS SAMT RAMVERK FÖR RISKHANTERING ... 48

9.1 VAD ÄR ETT RAMVERK FÖR RISKHANTERING? ... 49
9.2 RISKHANTERINGENS TRE NIVÅER, SPECIELLT BEHANDLING AV STRATEGISKA RISKER ... 51
9.3 NÅGRA KOMMENTARER TILL DEN GENERELLA RISKHANTERINGSPROCESSEN ... 51
9.4 EXEMPEL PÅ STRATEGISKT RAMVERK: BEGREPPET SÄKERHETSLEDNINGSSYSTEM ... 54
9.4.1 Seveso II direktivet ... 55
9.4.2 Säkerhetsledningssystem enligt Seveso II ... 57
9.4.3 Begreppet säkerhetsrapport enligt Seveso II ... 58
9.5 SAMMANFATTNING AV KAPITLEN 1-9 ... 59

DEL II – METODER ATT GENOMFÖRA RISK- OCH SÅRBARHETSANALYSER ... 61

10 IDENTIFIERING OCH EVALUERING AV STRATEGISKA RISKER ... 63

11 RISKER PÅ PROGRAM- OCH PROJEKTNIVÅ ... 66

12 FÖRSLAG PÅ STRUKTUR FÖR RISK- OCH SÅRBARHETSANALYSER AV EXEMPELVIS SKYDDSVÄRDA KAPACITETER ... 67

13 ATT ANALYSERA STEGET FRÅN ALLVARLIG HÄNDELSE TILL SVÅR PÅFRESTNING ... 70

13.1 ALLMÄN ANALYSSTRUKTUR ... 70
13.2 STEG 1: IDENTIFIERING AV ALLVARLIGA HÄNDELSER ... 71
13.3 STEG 2: FRÅN ALLVARLIG HÄNDELSE TILL SVÅR PÅFRESTNING: SCENARIOBESKRIVNING VIA HÄNDELSETRÄD ... 72

14 IDENTIFIERING AV SVÅR PÅFRESTNING MED GROVANALYTISK METOD ... 73

15 EXTERNA HOT OCH SÅRBARHETSANALYS AV KRITISKA FÖRSÖRJNINGSSYSTEM OCH INFRASTRUKTURER ... 76

15.1 ALLMÄNT ... 76
15.2 STRUKTUR PÅ ANALYSEN: TILLGÄNGLIGA MANUALER ... 76
15.3 INTERDEPENDENS, SPECIELLT EL – TELE - IT ... 77

16 FÖRSLAG TILL MÖJLIGT INNEHÅLL I RISK- OCH SÅRBARHETSANALYSERNA ENLIGT FÖRORDNING 2002:472 ... 78

16.1 MÖJLIGT INNEHÅLL I RISK- OCH SÅRBARHETSANALYSERNA ... 78
16.1.1 A: Utvärdering av myndighetens funktion och roll ... 78
16.1.2 B: Upprättande av register över analyserade händelser och situationer (svåra påfrestningar) ... 79
16.2 CHECKLISTA FÖR DEN ÖVERGRIPANDE RISKHANTERINGS- OCH KRISHANTERINGSPROCESSEN ... 79

DEL III – SAMMANSTÄLLNING AV INTERVJUSTUDIEN 80

17 INTERVJUSTUDIEN 81

INTERVJUSTUDIENS SYFTE OCH UPPLÄGG 81
Urval av myndigheter för intervju 81
Presentation av resultaten från studien 81
ÖVERGRIPANDE SLUTSATSER FRÅN INTERVJUSTUDIEN 82
BANVERKET 85
LIVSMEDELSVERKET 88
POST- OCH TELESTYRELSEN 91
RÄDDNINGSVERKET 94
LUFTFARTSVERKET 97
STATENS VETERINÄRMEDICINSKA ANSTALT 101
SOCIALSTYRELSEN 104
RIKSFÖRSÄKRINGSVERKET 108
SVENSKA KRAFTNÄT 111

REFERENSER 114

BILAGA 1 CHECKLISTOR FÖR UTVÄRDERING AV RISKHANTERINGS- OCH KRISHANTERINGSPROCESSEN 119

CHECKLISTA FÖR UTVÄRDERING AV RISKHANTERINGSPROCESSEN 119
CHECKLISTA FÖR UTVÄRDERING AV KRISHANTERINGSPROCESSEN 122

BILAGA 2 KORT SAMMANFATTNING AV DEN VETENSKAPLIGA BAKGRUNDEN FÖR ATT KLASSIFICERA RISKTYPER, RISKEVALUERINGSMETODER OCH RIKSHANTERINGSSTRATEGIER 123

BILAGA 3 KORTFATTAD BESKRIVNING AV EN GENERELL METOD ATT IDENTIFIERA RISKSCENARIER. 129

BILAGA 4 TEKNISK SÅRBARHETSANALYS 131

DEL I – BAKGRUNDSMATERIAL

1 Bakgrund

I regeringens proposition 2001/02:158 *”Samhällets säkerhet och beredskap”* (s 38) föreslås att

> *”Varje statlig myndighet bör för att stärka sin krishanteringsförmåga ha till uppgift att genomföra en analys av den sårbarhet eller de risker som kan finnas inom myndighetens ansvarsområde och som mycket allvarligt kan nedsätta förmågan hos verksamheten inom området (sårbarhetsanalys). Den bör årligen uppdateras och redovisas till Regeringskansliet. Sårbarhetsanalysen skall avse sådana tillstånd som kan uppstå när en eller flera händelser utvecklar sig eller trappas upp till att omfatta flera delar av samhället. Tillståndet skall vara av en sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner och kräver att insatser från flera olika myndigheter och organ samordnas för att kunna hantera situationen och därmed begränsa konsekvenserna.”*

Propositionen resulterade så småningom i *förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap* vars 3 § och 4 § innebar en viss konkretisering av ordalagen i propositionen. Enligt nämnda förordning skall statliga myndigheter årligen analysera om det finns sådan sårbarhet och sådana risker inom myndigheternas respektive ansvarsområden som synnerligen allvarligt kan försämra förmågan till verksamhet inom området, se citat **3 §** nedan:

> *”<u>Risk- och sårbarhetsanalys</u>*
> ***3 §*** *Varje myndighet skall i syfte att stärka sin krishanteringsförmåga årligen analysera om det finns sådan sårbarhet och sådana risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Vid denna analys skall myndigheten särskilt beakta*
>
> *1. situationer som uppstår hastigt, oväntat och utan förvarning,*
> *2. situationer som kräver brådskande beslut och samverkan med andra samhällsorgan,*
> *3. situationer som allvarligt påverkar samhällets funktionsförmåga eller tillgång på nödvändiga resurser, och*
> *4. förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde.*
>
> *Myndigheten skall värdera och sammanställa resultatet av arbetet i en risk- och sårbarhetsanalys. Analysen skall lämnas till Regeringskansliet vid samma tidpunkt som gäller för inlämnande av årsredovisningen.”*

Utöver detta har ett antal myndigheter utpekats med särskilt ansvar för fredstida krishantering och ålagts att planera och vidta förberedelser för att förebygga, motverka och begränsa identifierade sårbarheter inom sex angivna samverkansområden. Dessa myndigheter har ett särskilt ansvar för att samverka med varandra samt med länsstyrelserna, övriga statliga myndigheter, kommuner, landsting, sammanslutningar och näringsidkare som är berörda, se citat **4 §** nedan:

> *”Särskilt ansvar för fredstida krishantering*
> ***4 §*** *Myndigheterna som anges i bilagan till denna förordning skall planera och vidta förberedelser för att förebygga, motverka och begränsa identifierad sårbarhet och risker inom de samverkansområden som anges i bilagan. Myndigheterna skall därvid särskilt*
> *1. samverka med länsstyrelserna i deras roll som områdesansvarig myndighet,*
> *2. samverka med övriga statliga myndigheter, kommuner, landsting, sammanslutningar och näringsidkare som är berörda,*
> *3. beakta behovet av forsknings- och utvecklingsinsatser och annan kunskapsinhämtning, och*
> *4. beakta säkerhetskraven för de tekniska system som är nödvändiga för att de skall kunna utföra sitt arbete.”*

Enligt författarnas synsätt kan formuleringen *”planera och vidta förberedelser för att förebygga, motverka och begränsa identifierad sårbarhet och risker”* ovan anses vara en beskrivning av begreppet riskhantering, d.v.s. författarna anser att de aktuella myndigheterna, för att kunna uppfylla intentionen i förordningen, måste ha en väl utvecklad organisation för riskhantering avseende risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. För ett klargörande av skillnaden mellan krishantering och generell riskhantering, se kommentaren till figur 4.2. Vad detta kan innebära utvecklas vidare i senare delar av denna rapport.

2 Projektets målsättning, förutsättningar och begränsningar

Projektets målsättning har varit att ge KBM underlag för att utarbeta instruktion till myndigheter berörda av *förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap* för produktion av risk- och sårbarhetsanalyser, samt i görligaste mån förtydliga/konkretisera vissa begrepp, förutsättningar och frågeställningar avseende dessa risk- och sårbarhetsanalyser. Det har funnits två primära målsättningar:

1. Att beskriva rådande kunskapsläge avseende risk- och sårbarhetsanalyser samt det underlag och den metodik som tillämpas nationellt och internationellt för att producera sådana analyser.

2. Att ange en möjlig och praktiskt användbar metodik för att uppfylla kraven i förordningen 2002:472.

Det stod från början klart att målsättningen bara kunde uppfyllas i begränsad omfattning. Vad gäller den första målsättningen är den existerande kunskapsmassan av kolossalformat, ostrukturerad och under stark utveckling. Inte minst livlig är debatten angående vilken roll risk- och sårbarhetsanalyser generellt kan spela inom den totala krishanteringsprocessens ram och inför utvecklingen av de delvis nya hot och risker som det moderna samhället har att bemästra.

Inom varje tekniksektor existerar ett antal vägledningar och manualer med skiftande struktur och innehåll, utgivna av bl.a. nationella och internationella myndigheter och organisationer. Möjligheten att ge en användbar och lättöverskådlig översikt minskas av att strategier för risk- och sårbarhetshantering varierar från sektor till sektor. Det är alltså orealistiskt att försöka generellt definiera en ”state-of-art” som skall kunna omsättas i entydiga rekommendationer.

Ett annat problem har varit att försöka klargöra sambanden mellan myndigheternas generella riskhantering och organisationen av krishanteringen. Självklart innebär inte förordningen 2002:472 ens implicit något krav på myndigheternas generella riskhantering. Samtidigt anser vi att kraven i förordningens 4 § svårligen kan uppfyllas utan att myndigheter organiserar sin krishantering i en struktur med stora likheter med ett formellt ledningssystem, d.v.s. med policy, rutiner och instruktioner (se närmare definition av begreppet ledningssystem i avsnitt 9.4). Myndighetens totala riskhantering täcker avseende målsättningar, riskkategorier och allmän organisatorisk omfattning ett område avsevärt större än krishanteringen. Dock är krishanteringen en viktig och integrerad delmängd av riskhanteringen. Mot bakgrund av detta är det svårt att beskriva risk- och sårbarhetsanalysens roll i krishanteringen utan att ta hänsyn till myndighetens riskhantering generellt. Vi har därför valt att i någon utsträckning redovisa utvecklingen internationellt avseende kraven på myndigheters totala riskhantering, samt mycket översiktligt beskriva huvuddragen i några standards och vägledningar som producerats. Orsaken är givetvis att struktur på och innehåll i risk- och sårbarhetsanalyser för krishantering uppvisar mycket stora likheter med motsvarande analyser för den allmänna riskhanteringen. Även om författarna anser att det vore till klar fördel om myndigheterna utformade sin riskhantering som ett bland andra strategiska ledningssystem förutsätter resten av detta dokument inte på något sätt existensen av ett generellt sådant system för riskhanteringen.

Vi har valt att, avseende myndigheters riskhantering, i stor utsträckning använda källor från regeringskansliet i Storbritannien. Vi har bl.a. adopterat synsättet (något modifierat) att definiera tre generiska risknivåer: strategisk nivå, program/projektnivå samt operativ/anläggningsnivå. Ramverk för risk- och krishantering beskrivs och betydelsen av fungerande ledningssystem för dessa aktiviteter betonas.

Referenser eller webbadresser ges till ett antal vägledningar och manualer, speciellt avseende sårbarhetsanalyser av infrastruktursystem utsatta för externa hot. Dessa referenser innehåller ett antal checklistor för specifika system och hotbilder. Generella checklistor för utvärdering av risk- och krishanteringsprocessen listas i appendix.

Metoder att genomföra risk- och sårbarhetsanalyser diskuteras, bl.a. redovisas en allmängiltig metodik att generera riskmatriser/riskprofiler, byggd på den s.k. grovanalysmetoden (preliminary hazard analysis). Ett förslag på innehållet i en risk- och sårbarhetsanalys enligt förordning 2002:472 redovisas. Författarna står för innehållet i förslaget och det kan möjligen ses som ett komplement till den struktur som ges i vägledningen (KBM, 2003a).

3 Genomförande

3.1 Projektets genomförande och tillgänglig kompetensbas

Rapporten utgör i huvuddrag en syntes och sammanfattning av en studie som genomförts vid Lunds Universitets Centrum för Riskanalys och Riskhantering, LUCRAM, under perioden april-oktober 2003. Studien bestod av två tätt sammanlänkade delar, dels en allmän områdesöversikt och sammanställning av en kunskapsbakgrund utifrån litteraturstudier etc., dels en intervjustudie involverande nio centrala myndigheter där syftet var att föra inledande samtal kring, samt genomföra en översiktlig genomgång av, metodik, metoder och procedurer använda av myndigheterna i deras risk- och krishanteringsarbete.

Följande projektdeltagare har haft en aktiv roll i genomförandet av projektet:

Prof. em. Sven Erik Magnusson (projektledare)
Tekn. Lic. Marcus Abrahamsson (utredningsman)
Prof. Roland Akselsson (människa, teknik, organisation, säkerhetskultur)
Adj. prof. Lars Fredholm (krishantering)
Adj. lektor Anders Jacobsson (riskhantering)
Prof. Gustaf Olsson (infrastrukturer, interdependens)
Adj. prof. Kurt Petersen (riskanalys, riskhantering)
Doc. Per Runeson (telekommunikationssystem)

Sven Erik Magnusson och Marcus Abrahamsson svarar för huvuddelen av textmassan i del I & II och Marcus Abrahamsson för huvuddelen av intervjustudien i del III. Samtliga övriga projektdeltagare har medverkat med författande av delavsnitt.

3.2 Disposition av rapport

Rapporten är uppbyggd av tre huvudsakliga delar. Del I omfattar kapitel 1 ─ 9 och utgör väsentligen en bakgrundsbeskrivning till del II, som behandlar det praktiska genomförandet av risk- och sårbarhetsanalyser. I del III redovisas ovan nämnda intervjustudie.

Del I

Kapitel 4 är avsett att diskutera några grundläggande begrepp och definitioner. Betydelse och utformning av risk- och sårbarhetsanalyser kan bara utvärderas inom den totala krishanteringens ram. I avsnitt 4.2 ges därför ett par kompletterande definitioner av krishanteringens faser. Slutligen berörs de omständigheter som främst efter 11 september 2001 ändrat vår syn på den totala hotbilden och på krishanteringens roll och funktion.

I kapitel 5 diskuteras vidare några mer operativa definitioner. Terminologi och allmänna förfaringssätt avseende riskanalys och riskhantering berörs, liksom allmänna kvalitetskrav avseende riskanalyser. Olika aspekter på begreppet sårbarhet belyses och slutligen diskuteras relationen mellan begreppen sårbarhet, hot och risk.

Vi har bedömt det som viktigt att i viss utsträckning redovisa olika myndighetsroller med avseende på skydd av allmänheten, samt skissera hur en krishanteringsfunktion kan vara en integrerad del av myndighetens verksamhet. En summarisk beskrivning ges i kapitel 6. I kapitel 7 presenteras en översikt av olika typer av myndighetsföreskrifter på säkerhetsområdet samt redovisas mycket kortfattat ett ramverk för bestämmelseskrivande, regelverk och kontroll/tillsyn.

I kapitel 8 ges en beskrivning av tre huvudsakliga kategorier eller typer av grundorsaker/riskkällor till svåra påfrestningar som vi anser måste beaktas i risk- och sårbarhetsanalyserna. Typ 1 kan betecknas ”organisatoriska” olyckor (se avsnitt 8.1 för en redogörelse av vad som kan innefattas i begreppet ”organisatoriska” olyckor), typ 2 utgörs i huvudsak av naturkatastrofer av olika slag och typ 3 slutligen utgörs av terroristangrepp och annan påverkan med avsikt att skada ett system. I avsnittet 8.5 berörs kortfattat några teorier om olyckors och katastrofers uppkomst och hur dessa teorier kan leda till att olika delar av krishanteringen bör prioriteras för att effekten av denna hantering skall bli optimal.

Kapitel 9 utgår från vår bedömning att även om en myndighets riskhantering primärt är en allmän förvaltningsuppgift kan den inte särskiljas från beredskaps- eller krishanteringsuppgiften. Kapitlet ger därför en allmän översikt över organisationers riskhantering, samt betydelsen av att riskhantering ses som en ledningsuppgift bland andra och sköts via ett specifikt ledningssystem. En diskussion hålls om riskhantering på tre olika nivåer, strategisk nivå, program/projektnivå samt operativ/anläggningsnivå. Från Storbritannien har vi hämtat en beskrivning av innehållet i handlingsprogram (strategiskt ramverk) för myndigheters riskhantering. Kapitlet avslutas med en sammanfattning av huvuddragen kapitel 1 ─ 9.

Del II

I denna del av dokumentet diskuteras översiktligt praktiska metoder att genomföra risk- och sårbarhetsanalyser. Vi följer den riskhierarki som tidigare skisserats med en uppdelning i strategiska risker, program-/projektrisker, risker på operativ nivå och på nivån tekniska system. Att skyddsvärda kapaciteter skall analyseras avseende risker på den lägsta nivån är mer eller mindre självklart. Det är oklart i vilken utsträckning förordningen 2002:472 över huvud har som mål att 3 § skall omfatta de två övre risknivåerna, d.v.s. strategisk nivå och program-/projektnivå. Författarna har valt att tolka 3 § som att samtliga risker som synnerligen allvarligt kan försämra förmågan till verksamhet skall beaktas i analysen, d.v.s. även risker på de två övre nivåerna.

Kapitel 10 diskuterar metodik att behandla strategiska risker generellt, kapitel 11 risker på program- och projektnivå som kan leda till en svår påfrestning. Kapitel 12-14 redovisar metoder att analysera risker inom de skyddsvärda kapaciteterna och riktar sig primärt till myndigheter berörda av förordningens 4 §. Kapitel 15 redovisar hur risk- och sårbarhetsanalysens struktur kan förändras när huvudmålet är att beakta avsiktliga hot och attacker samt ger webbadresser till ett antal manualer och vägledningar. Slutligen presenteras i kapitel 16 ett förslag på möjligt innehåll i risk- och sårbarhetsanalyserna enligt förordning 2002:472 samt ges hänvisningar till checklistor för utvärdering av den övergripande riskhanterings- och krishanteringsprocessen.

Del III

Del III, intervjustudien, beskrivs i kapitel 17 genom att de olika myndigheterna får beskriva sina funktioner/aktiviteter under en rad gemensamma rubriker. Kapitlet inleds med en relativt fyllig sammanfattning av den totala studien.

4 Begreppen svår påfrestning och krishantering

I den fortsatta behandlingen behöver ett antal termer preciseras. Det är värt att nämna att begreppsförvirringen inom området ibland kan vara svår och att entydiga och allmänt accepterade definitioner ofta saknas. En förklaring till denna situation kan vara att det i stor utsträckning rör sig om företeelser och händelser som till sin art kan vara mycket olika men ändå rymmas inom samma begrepp.

4.1 Begreppet svår påfrestning

Begreppet svår påfrestning har i detta dokument använts för att beskriva den typ av tillstånd som krisberedskapen är avsedd att förhindra/motverka. Begreppet beskrivs i KBM-dokumentet *”Planeringsinriktning för samhällets krisberedskap 2005”* (KBM 2003b) enligt följande:

> *”En svår påfrestning på samhället i fred utgör inte någon enskild händelse i sig, exempelvis en olycka eller ett sabotage, utan är ett tillstånd som kan sägas uppstå när en eller flera händelser gemensamt eskalerar och konsekvenserna av dessa händelser omfattar stora delar av samhället. /…/ Tillståndet är av sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner eller hotar grundläggande värden av olika slag i samhället. För att hantera situationen och därmed begränsa konsekvenserna krävs samordning av insatserna från flera olika myndigheter och organ.”*

Ett primärt syfte med denna rapport är att redovisa metoder och angreppssätt att analysera eskaleringsförloppet från situationerna i 3 § i förordning 2002:472 till tillståndet ”svår påfrestning”.

4.2 Begreppet krishantering

Krishantering är ett centralt begrepp för denna rapport och en mängd olika definitioner och tolkningar av begreppet existerar i litteraturen på området. Sundelius m.fl. (1997) beskriver innebörden av begreppet ”nationell kris” enligt följande:

”*Nationell kris innebär för oss att de centrala aktörerna uppfattar situationen som att:*

1. *betydande värden står på spel (hotas),*
2. *begränsad tid står till förfogande,*
3. *omständigheterna präglas av betydande osäkerhet.*”

Vi har valt att definiera begreppet ”krishantering” genom att återge en modifierad form av FEMA-definitionen (FEMA = US Federal Emergency Management Agency), samt en kompletterande beskrivning av krishanteringens olika faser som de beskrivs i dokumentet ”*Crisis and Emergency Management: A Guide for Managers of the Public Service of Canada”* (CCMD, 2003).

Vi gör dessutom ett försök att antyda något om de utmaningar som den nationella krishanteringen möter inför den nya och utökade hotbild som framträtt eller fått en ökad betydelse under den senaste femårsperioden. Den sistnämnda redovisningen är högst fragmentarisk, för en mer fullständig översikt refereras exempelvis till en rad artiklar i tidskriften *"Journal of Contingencies and Crisis Management"* under senare år samt till referenserna i Boin (2003).

4.2.1 FEMA ramverk för krishantering

I figur 4.1 nedan ges en standardiserad definition av krishanteringens olika delar enligt FEMA. De olika faserna överensstämmer väl med den indelning som ges i dokumentet "Strategi för forskning för samhällets beredskap" (KBM, 2003c), s. 13.

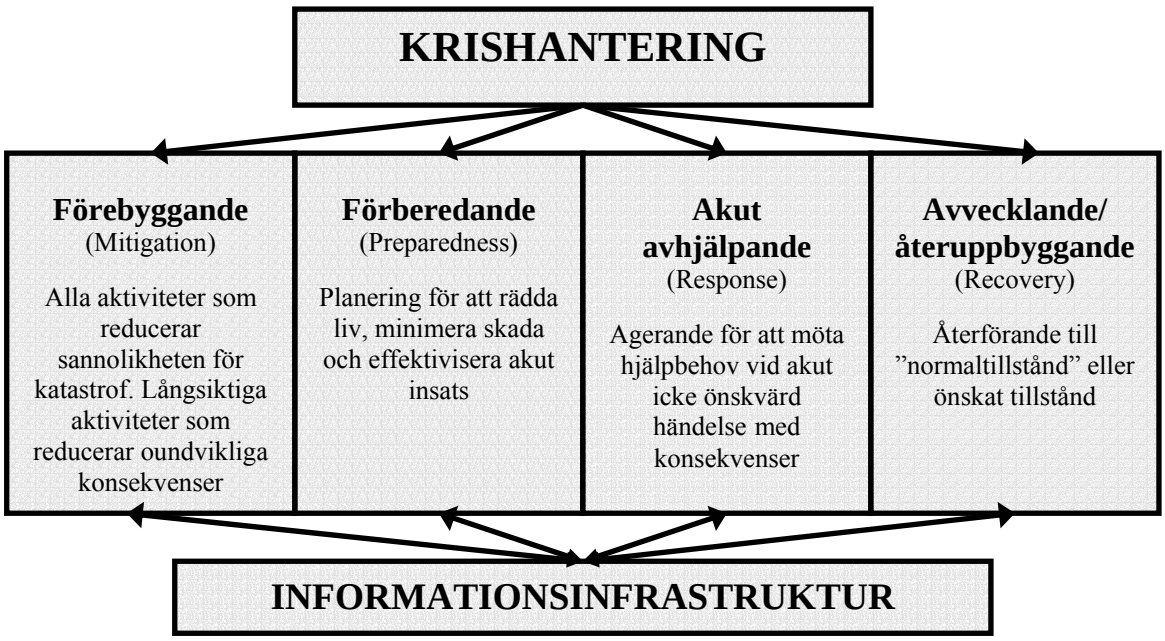


Fig. 4.1 Krishanteringens olika delar enligt FEMA (US Federal Emergency Management Agency)

För att illustrera begreppen ovan ges några exempel.

Förebyggande: Det kontinuerliga arbetet att reducera katastrofers effekt på människor och egendom. Exempel på åtgärder kan vara att förhindra att byggnader uppförs nära vattnet i översvämningshotade områden, förse lasarett med reservkraft, regelbundna inspektioner för att förhindra dammbrott, beräkning av rökfyllnadstiden vid brand i byggnad med stort antal människor. Riskanalyser, riskbedömningar och åtgärder för riskreduktion (baserade på genomförda riskanalyser) utgör en väsentlig komponent av denna del av krishanteringen.

Förberedande: Planering täcker en rad aktiviteter som genomförs innan en kris inträffat. Exempel utgör övning och utbildning av personal inom krisberedskapen, utveckling av insatsplaner, utveckling av datorprogramvara för beslutsstöd i en insatssituation.

Akut avhjälpande: Innebär en omedelbar insats för att skydda liv och egendom. Kräver definitionsmässigt ett skyndsamt agerande och en koordinerad användning av tillgängliga resurser i en omfattning som överskrider den rutinmässiga. Fasen kan innehålla ageranden innan händelsen inträffat som en reaktion på varningssignaler.

Avvecklande/återuppbyggande: Inkluderar aktiviteter både för att på kort sikt återskapa funktionen hos livsviktiga försörjningssystem och mer långsiktiga aktiviteter för att återställa infrastruktursystem till läget före katastrofen.

Informationsinfrastruktur: Begreppet skall ses i vid bemärkelse och utgör en viktig del av krishanteringsplanen. Viktiga komponenter är system för detektion av vad som skulle kunna leda till oönskade händelser, s.k. ”early warning system”, samt procedurer för kommunikation och återkoppling mellan de olika delarna av krishanteringsprocessen, exempelvis hur insikter från risk- och sårbarhetsanalyser (förebyggande) kan användas i de övriga delarna (som underlag för övningar etc.).

4.2.2 CCMD ramverk för krishantering

Som nämnts tidigare finns ingen entydig allmängiltig definition av begreppet krishantering och i figur 4.2 nedan visas ett alternativt sätt att beskriva krishanteringsprocessen som används av Canadian Centre for Management Development (CCMD, 2003). Framställningen har många beröringspunkter med FEMA-definitionen och kan ses som ett komplement till denna med exempel på något annorlunda infallsvinklar på problemställningen.

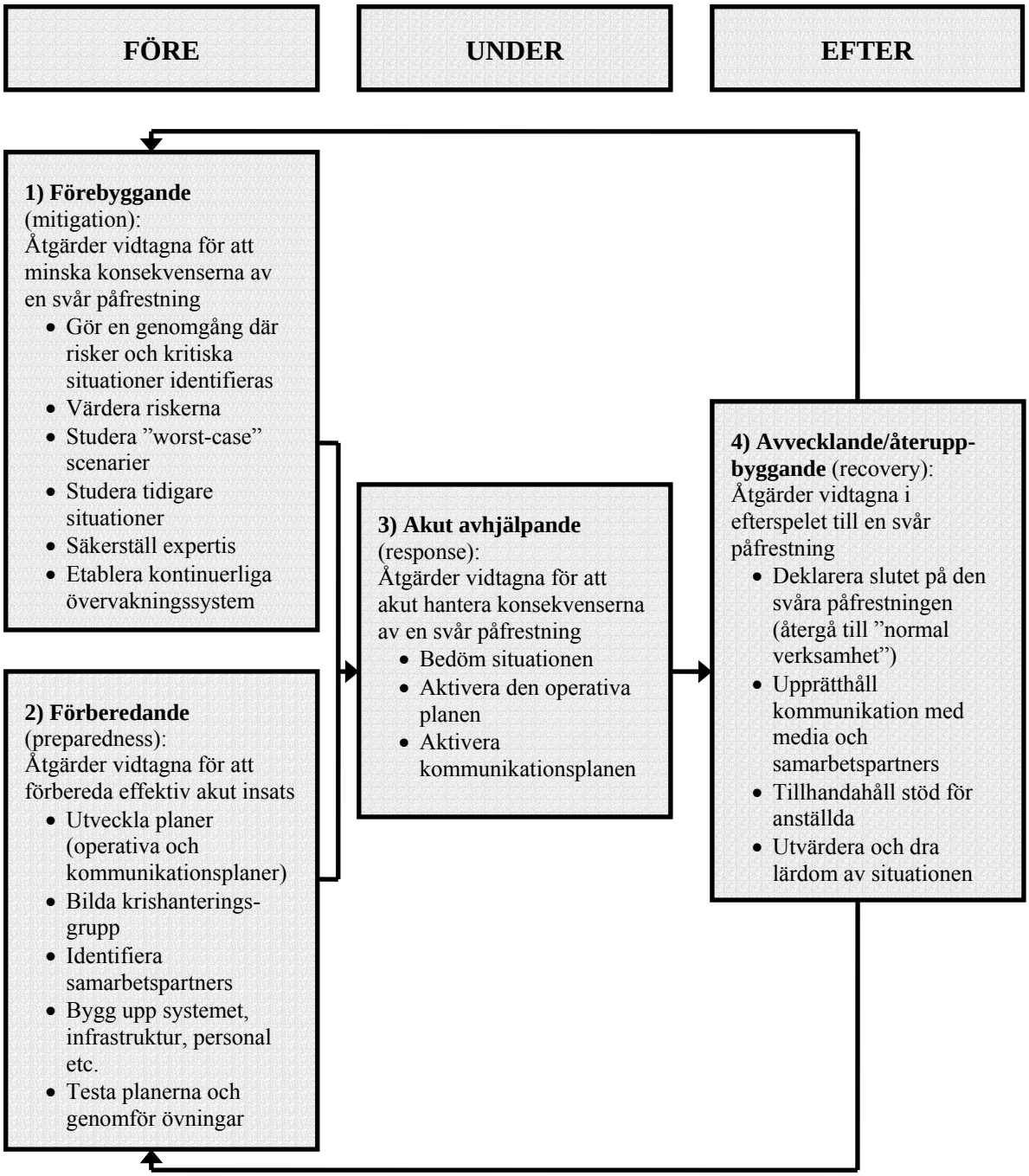


Fig. 4.2 Krishanteringsprocessen enligt CCMD (Canadian Centre for Management Development)

Åtgärderna i boxen ”Förebyggande” ingår i organisationens generella riskhantering. De risker som avses i detta sammanhang är dock endast en delmängd av den totala riskexponeringen, närmare bestämt risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. En annan skillnad är att den generella riskhanteringen traditionellt sett i hög utsträckning fokuserar på att minska sannolikheten för uppkomst av svår påfrestning medan krishanteringen traditionellt haft sin tyngdpunkt på konsekvensreducerande åtgärder; se vidare avsnitt 8.5 för en inledande diskussion kring dessa frågor.

4.2.3 Krishantering och den nya hotbilden

Synen på krishantering har genomgått en radikal förändring de senaste åren. Tag SARS-epidemin som exempel. ”Epidemin” illustrerar problemet att med rimlig säkerhet bedöma hotets omfattning och möjlig spridning, möjligheten att skapa en tillförlitlig överblick av hur allvarligt problemet är, samt den traditionella riskhanteringens och nationalstatens ifrågasatta förmåga till effektiva insatser. SARS-epidemin innebar en relativt begränsad hälsorisk men övergick trots detta till att bli en ekonomisk störningskälla med enorm förstöringspotential. SARS medförde bl.a. mycket kraftiga störningar i den globala lufttrafiken och turismen samt isolering av världsstäder. Ingen vet om den i skrivande stund kan betraktas som nedkämpad.

Den moderna krisen diskuteras bl.a. i Boin (2003) från vilken publikation vi återger följande synpunkter. Utgångspunkten är att ett antal nya kriskategorier avtecknar sig vid horisonten: cyberterrorism, andra typer av terrorism med biologiska och/eller kemiska vapen, transnationella kollapser av tekniska försörjningssystem, genmodifierade livsmedel och kris relaterad till allmänhetens tilltro till livsmedelsindustri och tillsynsmyndigheter, globala klimatförändringar etc. Den moderna krisens komplexitet motstår ofta vår förmåga att identifiera orsaker, att förstå eskaleringsmekanismer och att genomföra effektiva motåtgärder. Den kan ofta inte beskrivas på ett traditionellt vis med hjälp av parametrar som anger början och slut, intensitet och geografisk utbredning. Det är en i samhället inbyggd sårbarhet som bryter fram, tycks försvinna men återkommer, ibland i muterad form. Konsekvenserna av den moderna krisen anges inte främst i antalet dödade eller sårade; det som angrips är statens själva legitimitet och dess förmåga att ge det skydd som åtminstone i fredstid har betraktats som självklart. Frågan uppstår om vi har analytiska verktyg att förstå orsaker, mönster, händelseutvecklingar och slutliga skadeeffekter vad gäller dessa nya hot och faror. En diskussion kring några utvecklingslinjer avseende riskanalytiska metoder generellt ges i kommande avsnitt.

5 Begreppen riskanalys och sårbarhetsanalys

5.1 Inledning

En rapport med målsättningen att diskutera utgångspunkter för KBM:s fortsatta arbete inom området risk- och sårbarhetsanalyser har att redovisa en diskussion om terminologi för nyckelbegrepp som hot, risk, sårbarhet, riskanalys och sårbarhetsanalys, samt föreslå definitioner som underlättar det praktiska arbetet med kraven i förordningen 2002:472. Detta är viktigt inte minst från synpunkten att de utförda analyserna bör ha samma begreppsapparat om det totala materialet skall kunna sammanställas, analyseras och syntetiseras med rimlig arbetsinsats.

5.2 Risk, riskanalys och riskhantering

Anm. Hela avsnitt 5.2 är en bearbetning av utdrag ur Nilsson (2003).

5.2.1 Risk och riskperspektiv

Definitionen av risk har i modern tid sitt ursprung i ett *tekniskt "objektivistiskt"* förhållningssätt där man intagit ett strikt naturvetenskapligt förhållningssätt till riskproblematiken. Risk kan rent tekniskt förstås som en sammanvägning av sannolikheten för att en händelse skall inträffa samt de (negativa) konsekvenser händelsen i fråga kan anses leda till. Kaplan (1997) menar att risk rent tekniskt kan definieras som svaret på tre frågor:

- Vad kan hända (vilka scenarion, S, kan uppstå)?
- Hur troligt är det att det händer (sannolikhet, L)?
- Vilka är konsekvenserna, X, av händelsen?

Svaren på frågorna kan uttryckas som en trippel: (*S, L, X*). Genom att formulera trippeln som ett uttryck, d v s $R = \{<S_i, L_i, X_i>\}_c$ erhålles en uppsättning svar på de tre frågorna[1]. Risk är därmed lika med summan av alla scenarier, sannolikheten för att de skall inträffa samt den konsekvens som då uppstår. Risker skall inte förväxlas med riskkällor, d v s det fenomen som ger upphov till den oönskade händelsen. En industrianläggning är en typisk riskkälla som kan orsaka en oönskad händelse, t ex att en explosion inträffar som leder till att flera människor dör eller skadas eller att ett utsläpp av en kemikalie sker vilket ger effekter på den omgivande miljön. Sannolikheten för att explosionen skall inträffa samt hur stora konsekvenserna blir bestämmer riskens storlek.

I det tekniska perspektivet är fokus oftast på en eller ett par aspekter (t ex dödsfall och personskada). Ingen skillnad görs i hur olika personer ser på konsekvenserna av en händelse och hur de värderar dessa. Analytikerna skall genomföra en analys som är fri från sådana subjektiva värderingar.

[1] $_i$ står för ett specifikt scenario. $_C$ står för complete och innebär att alla scenarier är intressanta för att besvara frågan om vad risk är.

Denna tekniska definition av risk ger dock en förhållandevis okomplicerad bild av riskproblematiken. Den svarar inte på frågor varför vissa händelser kan anses oönskade. Den svarar inte heller på varför individer har olika uppfattning om vad som är en risk och betydelsen av denna risk. Forskning som fokuserar på frågor av denna art brukar ofta sägas utgå från ett *socialkonstruktivistiskt perspektiv*. Renn (1998) menar att det finns flera brister med det tekniska synsättet:

- Det utelämnar den mångfald av negativa sidor som folk i allmänhet förknippar med risk.
- Samspelet mellan mänskliga aktiviteter och konsekvenser är mer komplext och unikt än vad som ryms i det sannolikhetsbegrepp som används i de tekniska analyserna.
- Den tekniska riskanalysen kan inte ses som en värdefri vetenskaplig aktivitet. Värderingar reflekteras i hur risker karakteriseras, mäts och tolkas.
- Den numeriska kombinationen av konsekvens och sannolikhet förutsätter ofta likvärdig betydelse för de båda komponenterna. Detta förhållande har emellertid visat sig vara mer komplicerat i verkligheten då allmänheten i högre grad undviker risker med låg sannolikhet men med stora konsekvenser än risker med stor sannolikhet och måttlig konsekvens.
- Att generellt sammanställa data som berör stora populationer över lång tid utelämnar ofta viktiga individuella skillnader och preferenser.

Vilken typ av kunskaper är det som den socialkonstruktivistiska disciplinen rent konkret bidragit med? Som ett tidigt exempel kan nämnas Otway & von Winterfeldts forskning (1982) vilken visat på några kvalitativa aspekter som påverkar människors acceptans negativt av teknologiska risker:

- Ofrivillig utsatthet.
- Brist på personlig kontroll.
- Osäkerhet om sannolikheten eller konsekvensen av en olycka.
- Brist på erfarenhet av risken.
- Tidsfördröjda effekter av exponeringen.
- Genetiska effekter.
- Olyckor som sker sällan men när de inträffar så är effekten av katastrofal karaktär (Low Probability – High Consequence).
- Fördelar som inte är påtagliga.
- Fördelar som gynnar andra.
- Olyckor som förorsakas av mänskliga faktorn (jämfört med t ex naturrelaterade).

Sambandet och betydelsen av riskens kvalitativa egenskaper och riskperceptionen har bl.a. undersökts inom den psykometriska traditionen[2]. Man har fokuserat på två frågor: Formar de olika kvalitativa egenskaperna ett värderingsmönster? Är det möjligt att modellera hur individer ""konstruerar" risker och på det sättet vinna insikt?

En del företrädare för den socialkonstruktivistiska disciplinen menar att risk heltigenom är en social konstruktion, således också det tekniska synsättet. De mått som oftast används för konsekvenser inom det tekniska synsättet (dödsfall, skador och ekonomiska förluster, etc) är inget som kan anses ha ett objektivt värde, utan bygger på samhällets värderingar.

[2] Man har emellertid fokuserat på den subjektiva bedömningen av enskilda riskkällor och inte närmare belyst hur risker uppfattas i förhållande till andra sammanhang som livsmål etc.

5.2.2 Riskanalys och riskhantering

I figur 5.1 nedan ges en generisk beskrivning av riskhanteringsprocessen enligt IEC (International Electrotechnical Commission, 1995).

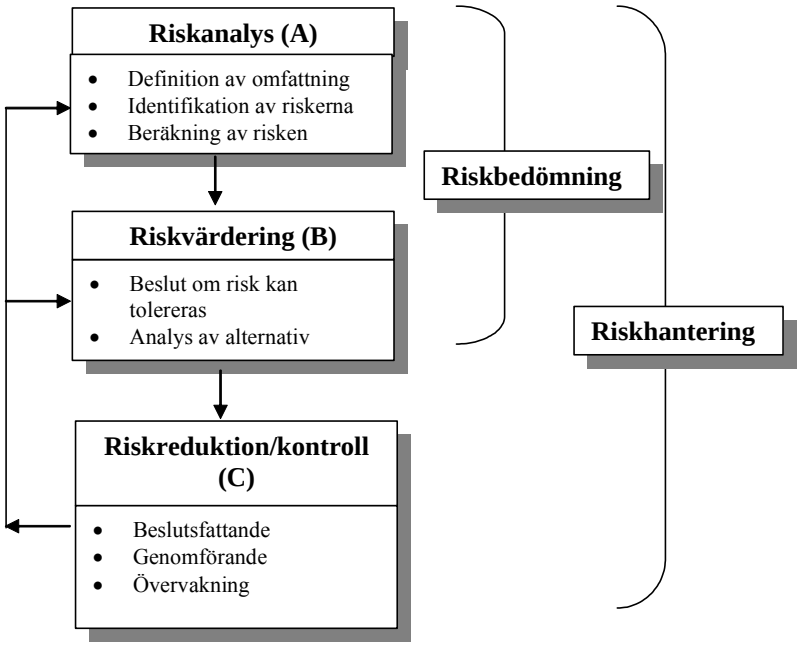


Fig.5.1. Riskhanteringsprocessen. Källa: International Electrotechnical Commission, IEC 1995.

I praktiken är det naturligtvis så att olika teknologigrenar och olika verksamhetsgrenar allmänt sett har sina egna standardiserade processer för såväl riskanalys och riskhantering i stort. Här ges endast en övergripande bild av de huvudsakliga elementen. Det skall nämnas att processen i figur 5.1 avser riskanalys av tekniska system. Motsvarande generiska modeller existerar givetvis även för analys av andra typer av verksamheter och system. Nedan ges en översiktlig beskrivning av en procedur för riskanalys av tekniska system.

1. Definition av systemet som skall analyseras samt omfattning av analysen

I det första steget skall: a) orsakerna till analysen beskrivas, b) det system som skall analyseras definieras och avgränsas liksom; c) de tekniska, miljömässiga organisatoriska och övriga aspekter som är relevanta för problemet; d) antaganden och begränsningar som styr analysen skall fastställas och; e) de beslut som behöver tas identifieras.

2. Identifikation av riskkällor och genomförande av en initial konsekvensvärdering

I det andra steget identifieras riskkällorna och det sätt på vilket de kan utgöra hot[3]. En initial värdering görs, baserat på en konsekvensanalys, för att analysera hur signifikanta riskkällorna är. Syftet är att besluta om a) åtgärder skall utföras på den här nivån för att eliminera eller reducera faran; b) om analysen skall avslutas p g a att riskkällorna är insignifikanta eller; c) om man skall fortsätta med riskuppskattning.

[3] Den engelska benämningen är Hazard analysis. En annan svensk benämning är faroanalys

De vanligaste metoderna för riskidentifikation i ett tekniskt system kan delas in i tre områden (Nicolet-Monnier 1996):

- Komparativa metoder (process/systemchecklistor, säkerhetsgranskning/översyn, indexmetoder för relativ rangordning och preliminära analyser av riskkällor).
- Fundamentala metoder (”Hazard and operability studies”, ”What if?–analyses”, ”Failure mode effect and criticality analyses” och ”Goal oriented failure analyses”).
- Logiska diagram metoder (felträdsanalys, händelseträdsanalys (under rubriken ”Exempel på redovisning av säkerhetsrisker” ges en utförligare beskrivning av händelse- och felträd), analys av mänsklig tillförlitlighet, och ”system success trees”).

3. *Riskuppskattning*

I en riskuppskattning bedöms de initierande händelserna, följden av dem, skadereducerande inslag och hur frekvent de skadliga konsekvenserna inträffar. Syftet är att kvantifiera riskuttrycket $R = \{<S_i, L_i, X_i>\}_c$ (kaplan 1997). Uppskattningen görs i tre steg.

I det *första* steget görs en frekvensanalys. Syftet med *frekvensanalysen* är att bestämma hur ofta de oönskade effekterna som tidigare identifierats inträffar. Tre grundläggande tillvägagångssätt föreligger:

- Se till historiska data.
- Förutse frekvensen genom att använda tekniker som felträdsanalys och händelseträdsanalys.
- Förlita sig på expertbedömningar vilket innebär att subjektiva element infogas i bedömningen.

I det *andra* steget analyseras konsekvenserna på människor, egendom, etc. mer i detalj. *Konsekvensanalysen* baseras på de oönskade händelser som bedömts som intressanta och syftar till att beskriva de effekter som kan härledas till dessa företeelser. Det är angeläget att överväga såväl direkta konsekvenser som sådana som kan uppstå på längre sikt. Slutligen bör man fundera på sekundära konsekvenser. Analysen kan göras kvantitativt eller kvalitativt. Ändamålet kan vara att t ex uppskatta det antal människor som är lokaliserade i olika miljöer, på olika avstånd från riskkällan och som dödas, skadas eller på annat sätt berörs negativt.

I riskuppskattningens *sista* steg undersöks sannolikheten för att riskkällan skall orsaka det oönskade händelseförloppet - scenariot. Risken kan därefter, som tidigare redogjorts för, uttryckas på flera sätt..

Viktigt i det här steget är att fastslå huruvida riskuppskattningen reflekterar hela risken eller endast en del av den. Osäkerheten är ofta stor i beräkningarna. En osäkerhetsanalys kan användas för att bestämma variationen eller graden av noggrannhet i resultatet från modellerna.

4. *Verifikation*

En formell utvärdering bör utföras av någon utanför projektet för att bekräfta analysens integritet. Man bör kontrollera att avgränsningen som gjorts är den rätta m h t målet och gå

igenom alla kritiska antaganden för att försäkra sig om att de är trovärdiga. Vidare bör bekräftas att analysen använder de för ändamålet rätta metoderna, modellerna och data och undersöka om utredningen går att utföra av andra än de som ursprungligen gjort den.

5. Dokumentation

Riskanalysprocessen bör dokumenteras. Styrkor och svagheter med olika riskmått skall förklaras och osäkerheterna kring riskuppskattningarna uttryckas på ett sätt så att den tilltänkte läsaren förstår vad som menas.

6. Uppdatering

Om riskhanteringsprocessen är kontinuerligt pågående bör analysen utformas på ett sådant sätt att den kan uppdateras under systemets, händelsens eller aktivitetens livscykel. Vilka metoder man beslutar sig för att använda beror t ex på vilken fas systemet befinner sig i, målet med studien, hur allvarlig risksituationen är etc.[4].

5.2.3 Riskanalyser och allmänna kvalitetskrav

Att utföra en riskanalys är ofta ett av de första stegen i en process som kommer att utmynna i att ett beslut skall fattas. Beslutet kan handla om huruvida den aktuella risken är acceptabel eller inte, samt vilka alternativ som skall väljas för att reducera eller kontrollera risken. För att kunna fatta ett så bra beslut som möjligt i en fråga krävs det att beslutsfattaren har tillgång till så fullständig och korrekt information som möjligt. Ett ganska självklart påpekande kan tyckas, men ändå viktigt att betona då beslutssituationer ofta kännetecknas av ett komplext och ofullständigt bakgrundsmaterial. Innebörden i detta är att beslut måste fattas under stor osäkerhet. Morgan & Henrion (1990) anser, med anledning av den ovan beskrivna situationen, att vissa krav bör ställas på en analys för att den skall leda till beslut som är så bra som möjligt med hänsyn tagen till den aktuella kunskapen, dess begränsningar och dess innebörd. De sammanfattar dessa kriterier som tio ”budord”.

1. Studera adekvat litteratur, konsultera experter och praktiker inom ämnet.

Hur ser kontexten ut? Om det finns en klient för vilken analysen utförs, vilka är dennes behov? Har han/hon formulerat problemet på ett sätt som återspeglar den verkliga situationen? Kanske är det nödvändigt att hjälpa klienten att omformulera problemet. Det gäller att använda den litteratur, de experter och praktiker som är rätt m h t problemet.

Det är nödvändigt att återkomma till dessa frågeställningar under processens gång. Oavsett om det finns en klient eller inte är det nödvändigt att grundläggande förstå kontexten och de aktörer som berörs.

[4] En genomgång av problemet med riskanalysens praktiska användning skedde i Magnusson m fl (1999). Rapporten som utgör ett förslag till samordnad nordisk riskforskning, analyserar svårigheterna sett från industrins, myndigheternas och allmänhetens synvinkel

2. Låt analysen vara probleminriktad.

Problemet skall styra vilka metoder och verktyg som används, inte vilka som man föredrar eller redan investerat i.

3. Gör analysen så enkel som möjligt men inte för enkel.

Om analysen är enkel är den också lätt att förstå och att beskriva. Transparensen ökar vilket ger ett ökat förtroende för de slutsatser som dras. Naturligtvis finns det också en stor fara i att analysen hålls för enkel. För att finna rätt detaljnivå krävs att analysen och problemformuleringen itereras.

4. Identifiera alla antaganden som kan anses signifikanta.

Signifikanta antaganden är de som kan antas påverka slutsatserna av analysen, t ex.

- Frågan som initierat analysen (är det hälsovådligt att exponeras för kemikalie X?).
- Värderingskriterier som använts för att t ex definiera olika alternativ (t ex kostnader för ny teknologi).
- Omfattning av analysen och hur olika gränsdragningar här kan påverka analysen.
- Mjuka frågor som kanske går förlorade i den kvantitativa analysen (t ex känslan av förlorad frihet vid tvång av bältesanvändning i bil)
- Avrundningar till följd av aggregeringar i analysen (t ex den rumsliga upplösningen i geografiska modeller).
- Värdeomdömen vad beträffar t ex riskattityd.
- Målfunktioner som använts vilket inkluderar metoder för att kombinera flera kriterier och värdera beslut.

5. Var tydlig beträffande beslutskriterier och policy.

Vikten av detta skall inte underskattas. De är signifikanta antaganden men tas för givna allt för ofta. Det är viktigt att komma ihåg att beslutskriterier och den policy som används inte är universalt gällande utan grundar sig på normativa val.

Exempel på några olika kategorier för beslutskriterier är:

- Nyttobaserade kriterier (*cost-benefit, cost-effectiveness*, *minimera möjligheten för värsta tänkbara utfall*, *etc.*).
- Rättighetsbaserade kriterier (*noll risk*, d v s oavsett riskens storlek eller fördelarna med aktiviteten som ger upphov till risken skall risken elimineras, *begränsad risk* – som noll risk men tillåt risken så länge den inte överstiger en viss nivå)
- Teknologibaserade kriterier (*Best Available Technology* – krav ställs på att använda så bra teknik som möjligt för att reducera risken).

Ofta används hybrider av de tre kategorierna ovan. Samtidigt är det viktigt att komma ihåg att det finns flera inkonsistenta kombinationer. Ofta händer det dessutom att en analytiker, utan

att de inser det, använder olika kriterier och strategier i olika delar av samma analys. Det händer då lätt att resultatet blir en inkonsistent produkt.

6. Var tydlig om den osäkerhet som gäller.

Detta kan gälla:

- Osäkerhet om tekniska, vetenskapliga, ekonomiska eller politiska kvantiteter (t ex inflationstakten, dimensionering av beredskap för krishantering, etc.).
- Osäkerhet om korrekt funktionell form av tekniska, vetenskapliga, ekonomiska eller politiska modeller (t ex den funktionella formen av en dos-respons modell för cancer).
- Icke-överensstämmande åsikter mellan experter rörande värdet av kvantiteter eller den funktionella formen för modeller (t ex olika gränsvärdessättningar).

7. Utför en systematisk känslighets- och osäkerhetsanalys.

En mycket viktig fråga är vilka antaganden och vilken osäkerhet som har potential att signifikant påverka analysen. Den frågan kan man besvara genom att utföra en känslighets- och osäkerhetsanalys. Känslighetsanalys handlar om att beräkna vilken effekt förändringar i inputvärden eller antaganden har för outputen. En osäkerhetsanalys syftar till att beräkna den totala osäkerheten i resultatet som orsakas av kvantifierad osäkerhet i indata och av de modeller som används.

Om ingen systematisk osäkerhetsanalys och känslighetsanalys utförs innebär det att analytikern och användaren inte klart kan bedöma hur adekvat analysen och dess resultat är.

8. Se problemformulering och analys som en iterativ process.

Allteftersom analysprocessen fortgår klarnar förhoppningsvis vad som är värt att fästa vikt vid. Nya data och ny information kan då inhämtas upprepande för att förbättra analysen, t ex genom:

- Omsorgsfull genomarbetning av de aspekter som anses viktiga
- Förenkling av de aspekter som kan anses mindre viktiga/oviktiga.

Målet är att försöka hålla analysen enkel, klar, förståelig, konsistent med målen och de frågor som är av vikt. För detta, liksom i tidigare steg, gäller det att bedriva processen iterativt istället för linjärt, vilket är vanligt förekommande.

9. Gör en tydlig och fullständig dokumentation

Dokumentation syftar dels till att hjälpa analytikern själv att komma ihåg vad han/hon har gjort, dels till att hjälpa andra analytiker med att använda, modifiera eller evaluera analysen. Dokumentationen är en kontinuerlig integrativ process som måste initieras i ett tidigt skede. I dokumentationen ingår bl.a. att identifiera alla komponenter och antaganden, identifiera resultatet av känslighetsanalysen, rapportera om alternativa modellformuleringar, framställa

tillräcklig dokumentation av den slutgiltiga modellen så att alla modelleringar och beräkningar kan reproduceras från den.

10. Underkasta analysen för en peer-review

En peer-review är en kritisk granskning och värdering av manuskript från professionella kollegor. Det kan ses som den traditionella metodiken för kvalitetskontroll i vetenskapliga sammanhang.

Morgan & Henrion (1990) menar att det är särskilt viktigt att behandla osäkerheten i analyser explicit när:

- det är viktigt att ta hänsyn till allmänhetens riskattityd, t ex om den starkt tar ställning för eller emot en risk.
- det finns flera källor till osäkerhet och dessa kombineras. De kan då jämföras och viktas för att användas i en vidare analys.
- det är nödvändigt att fatta beslut om ytterligare information måste inhämtas för att klarlägga osäkerheten. Rent allmänt kan man säga att ju större osäkerhet desto större är det förväntade värdet av ytterligare information

För en diskussion kring kvalitetskrav avseende analyser av olycksrisker hänvisas till Räddningsverket (2003).

5.3 Kort sammanfattning av den vetenskapliga bakgrunden för att klassificera risktyper, riskevalueringsmetoder och riskhanteringsstrategier

Inom det extremt mångdisciplinära forskningsområdet riskhantering har under de senaste decennierna förts en livlig debatt kring lämpliga strategier för evaluering och hantering av risker inom olika områden. Kärnfrågorna i debatten har rört bl.a. användningen av kvantitativa riskanalyser som bas för riskhantering, relevansen av allmänhetens uppfattningar som kriterium för reglering av riskrelaterade verksamheter, hanteringen av osäkerheter i riskanalyser, legitimiteten hos ”riskbaserade” gentemot ”försiktighetsbaserade” hanteringsstrategier, samt hur integrationen av analytiska och överläggande/rådgivande processer bör ske.

Under senare delen av nittiotalet genomfördes inom EU en omfattande studie i syfte att belysa ovanstående frågeställningar (Stirling, 1999). Studien har bland annat resulterat i en metodik för evaluering och klassificering av risktyper som bas för att välja lämpligast procedur för att förbättra riskhanteringens kvalitet, acceptans och effektivitet (Klinke & Renn, 2002), vilken presenteras i bilaga 2.

Metodiken att klassificera risktyper och lämpliga hanteringsstrategier är avsedd att dels verka för vetenskaplig noggrannhet, dels kunna reflektera sociala olikheter och verka för politisk genomförbarhet. I metodiken är begreppet risk uppbyggt av såväl ”objektiva” fysiska attribut, såsom potentiell skada till följd av en oönskad händelse, som ”subjektiva” perceptionella och kulturella attribut, såsom rättvisefrågor och upplevd risk. Som en första del av en vägledning för att välja lämplig riskhanteringsstrategi presenteras nio kriterier för riskevaluering, vilka följaktligen inkluderar såväl fysiska som sociala indikatorer, se bilaga 2.

Baserat på dessa nio kriterier (samt i praktiken även ett stort antal subkriterier) härleds en indelning i sex generiska riskklasser, se bilaga 2. Dessa riskklasser skiljer sig åt sinsemellan avseende bl.a. potentialen att generera katastrofer, graden av osäkerhet, tidsförskjutning mellan påverkan och märkbara effekter, samt graden av irreversibilitet, och kommer således att kräva fundamentalt skilda hanteringsstrategier.

För att möta upp detta krav på diversifierade hanteringsstrategier ges ett förslag på indelning i tre generiska grupper av strategier:

- riskbaserade hanteringsstrategier,
- försiktighetsbaserade hanteringsstrategier, samt
- samtals-/förhandlingsbaserade hanteringsstrategier,

vilkas karakteristika kortfattat redogörs för i bilaga 2. Sammantaget kan sägas att angreppssättet som presenteras i Klinke & Renn (2002) ger oss grundpelarna i en struktur för att kategorisera risker, och med utgångspunkt därur finna lämpliga strategier för hantering.

5.4 Olika aspekter på sårbarhetsbegreppet

Sårbarhet är ett begrepp med många betydelser och många användningar. Vi skall här koncentrera oss till definitioner av begreppet som är användbara i krishanteringssammanhang. I vägledningen (KBM, 2003a) ges en definition av begreppet sårbarhet som är av mycket generell natur:

> ”*Sårbarhet betecknar hur mycket och hur allvarligt ett system påverkas av en händelse. Graden av sårbarhet bestäms av förmågan att förutse, hantera, motstå och återhämta sig från händelsen.”*

När vi försöker att något differentiera och exemplifiera denna definition väljer vi tre användningsområden: sårbarhet och naturkatastrofer, sårbarhet i tekniska system i allmänhet och som ett nyckelbegrepp för skydd av infrastruktursystem mot externa hot och attacker, samt slutligen för social sårbarhet och krishantering i allmänhet.

<u>Sårbarhet speciellt länkat till naturkatastrofer</u>

Weichselgartner (2001) har gjort en sammanställning av ett 25-tal definitioner, de flesta länkade till området sårbarhet och naturkatastrofer. Låt oss citera två exempel:

Timmerman (1981): ”Sårbarhet betecknar den omfattning med vilken ett system reagerar negativt på en exponering från en utlöst riskkälla. Omfattning och styrka av den negativa reaktionen bestäms av systemets motståndsförmåga (ett mått på systemets förmåga att absorbera och återhämta sig från påverkan efter händelsen).”

Watts & Bohle (1993): ”Sårbarhet definieras i termer av exponering, kapacitet och handlingsmöjligheter. Det följer att åtgärdsstrategin för att kontrollera sårbarhet är att reducera exponering, öka förmågan att hantera påfrestningen, förstärka återhämtningspotentialen och effektivisera skadekontrollen via offentliga och privata medel”

Sårbarhet enligt denna definition är alltså både en beskrivning av tillståndet hos ett skyddsvärt system (exempelvis elförsörjning) innan händelsen utlösts och en beskrivning av förmåga till akut avhjälpande insatser, social motståndskraft och robusthet när riskkällan aktiverats. Länken mellan sårbarhetsanalys och krishantering framgår således klart av definitionen från Watts & Bohle ovan.

Sårbarhetsanalys av tekniska system, planerade och oplanerade hot

Det kan vara ändamålsenligt att särskilja sårbarhet i tekniska system och sårbarhet länkat till krishantering i allmänhet. Exempelvis har Einarsson & Rausand (1998) utvecklat en scenariobaserad metodik för sårbarhetsanalys av komplexa industriella system. I artikeln används termen sårbarhet för att beskriva de egenskaper hos ett industriellt system som kan påverka systemets möjligheter att överleva och fullfölja sin uppgift under närvaro av hot. Analysen utförs i ett antal steg (Einarsson 1999, Einarsson & Rausand 1998) som bl.a. innefattar identifikation av riskkällor m h a checklistor, identifikation av olycksscenarier (bl.a. med hjälp av händelseträd), bortgallring av scenarier med låg sannolikhet, uppskattning av de kvarvarande scenariernas effekter på människor, egendom och affärsliv, identifikation och utvärdering av skadereducerande resurser samt identifikation och utvärdering av resurser för att återuppbygga och återskapa företaget. En kortfattad beskrivning av metodiken ovan återfinns i bilaga 4.

Vid planerade hot kan sårbarheten definieras som ”svagheter i (det tekniska) systemet som kan utnyttjas av en inkräktare för att få tillgång till en kritisk resurs. Sårbarheter kan omfatta, men är inte begränsade till, byggnaders egenskaper, egenskaper hos utrustning, närvaro av personal, operativa och organisatoriska rutiner/instruktioner” (CCPS, 2002).

Social sårbarhet

Anm. avsnittet om social sårbarhet är huvudsakligen författat av prof. Per-Olof Hallin, Institutionen för kulturgeografi och ekonomisk geografi, Lunds Universitet.

Om svåra påfrestningar inträffar, drabbas civilbefolkningen nästan utan undantag i någon form. Det kan omfatta allt från fysiska påfrestningar, men också gälla olika former av sociala och psykiska belastningar. I och med en ny och breddad risk- och sårbarhetssituation, samt svårigheterna att förutse och hantera den, har social sårbarhet blivit ett centralt begrepp inom krishantering. En viktig fråga gäller hur sårbarheten fördelas i tid och rum över berörd befolkning. Analysmetoder saknas för närvarande för att på ett systematiskt sätt bedöma social sårbarhet.

Social sårbarhet är ett nytt begrepp inom risk- och sårbarhetsanalys. Vissa definierar det som en persons bristande tillgångar på resurser, t.ex. ekonomiska, materiella, personliga, fysiska, sociala och politiska, vilka kan leda till svaga strukturer hos individer och hushåll. Begreppet kan också omfatta föreställningar och vanor, dvs. människors uppfattningar och handlingsmönster kan leda till att de är mer sårbara än andra (Blaikie et al 1994, Miletti 1999 enligt Cutter et al 2000, Morrow 1999). Personer som bedöms ha svaga resurser eller inte får möjligheter att använda dem, anses ha en låg förmåga att hantera svåra situationer (Blaikie et al 1994, Anderson och Woodrow enligt Dibben 1999). Ibland inkluderas institutionell sårbarhet vilket omfattar mer samhälleliga faktorer som brist på riktlinjer, planering och

ledning på den lokala nivån (de Freitas et al 2001, Morrow 1999). Vidare måste social sårbarhet eller social robusthet ses som långvariga processer där förhållanden i vardagslivet också påverkar hur väl en befolkning kan stå emot exceptionella påfrestningar. På samma sätt bör extraordinära händelser av social karaktär ses som resultat av långvariga processer som vid ett givet tillfälle blossar upp som akuta. En viktig forskningsfråga i detta sammanhang är därför om det går att utveckla tidiga varningssystem för att förhindra dem.

I detta avsnitt definieras social sårbarhet som: *En individs, grupps eller befolknings oförmåga att motstå och återhämta sig vid olika former av påfrestningar*. Vid en sådan definition görs en skillnad mellan individens, gruppens och befolkningens sårbarhet. Utifrån ett *individuellt* perspektiv kan social sårbarhet vara hur hon hanterar exceptionella händelser som kanske främst drabbar henne, men det kan också gälla hur hon vid krissituationer agerar för sin egen överlevnad. Vissa personer med särskilda hjälpbehov kan vara särskilt sårbara eftersom de inte själva kan hantera eller påverka situationen. En *grupps sårbarhet* inriktas mot hur den gemensamt kan hantera en svår situation. En mindre social gruppering kan ses som relativt homogen gällande värdesystem och vanor. Den har även ett uppbyggt nätverk som kan aktiveras vid olika situationer. Det gör att den ofta snabbt kan agera vid krissituationer. Undantag är grupper i samhället som delas in efter demografiska utgångspunkter. Barn och äldre är särskilt sårbara grupper. Med tanke på att andelen äldre kommer att öka i de flesta av Sveriges kommuner, och därmed behovet av vård och omsorg, kan detta vid krissituationer leda till stora svårigheter att ta hand om dem. En *befolknings sårbarhet* måste ses mot bakgrund av att den är sammansatt av en mängd olika sociala grupperingar med olika föreställningar och handlingsmönster. För att hantera påfrestningar som drabbar exempelvis en kommuns eller ett läns befolkning fordras väl utbyggda samhälleliga institutioner. Individer, grupper eller befolkningar som har begränsade resurser och förmågor, eller lever i en miljö där strukturella och institutionella faktorer hindrar dem från att utnyttja dem, eller inte ger dem tillräckligt stöd, är sannolikt mer sårbara vid extraordinära händelser än andra.

Vid en krissituation samverkar alla tre nivåerna. Individens agerande påverkar hur gruppen kan hantera situationen och gruppens agerande påverkar hela befolkningens hanteringsförmåga. Även individuella misstag kan få omfattande negativa konsekvenser för en grupp eller till och med en hel befolkning. Institutionellt stöd kan ha betydelse på alla nivåer. Det är även viktigt att lyfta fram tiden som en viktig faktor vid krishantering. Med undantag av akut och räddningstjänstinriktade insatser är individuella och sociala grupperingars initiativ och förmågor kanske störst vid själva inträffandet av händelsen medan institutioners betydelse ökar efter hand. Vid Göteborgsbranden spelade lokala sociala nätverk en viktig roll närmast efter händelsen medan mer professionella krafter måste ta över efter en tid (Nieminen Kristoffersson 2002).

Exemplifieringen av de tre användningsområdena ovan avser att demonstrera att det i risk- och sårbarhetsanalyser kan vara fördelaktigt att dela upp begreppet sårbarhet i två delar:

- En inre sårbarhet i ett (tekniskt) system som härstammar från interna brister och som medför att om en oförutsedd eller riskmedvetet accepterad händelse/hot realiseras så orsakas en allvarlig felfunktion eller sammanbrott. Sårbarheten kan vara av fysisk, teknisk eller operativ art.

- Yttre, social sårbarhet.

Begreppen kommer att återkomma i del II av rapporten.

5.5 Relationen sårbarhet, hot och risk

Relationen mellan begreppen sårbarhet, hot och risk diskuteras i regeringens proposition 2001/02:158 *”samhällets säkerhet och beredskap”* och där framhålls bl.a. att det inte är ändamålsenligt att diskutera ett systems eller samhällets allmänna sårbarhet enskilt i den meningen att denna sårbarhet i sig skulle utgöra ett hot eller en risk och därmed vara ett tillräckligt underlag för beslut om åtgärder etc.

I propositionen betonas att en diskussion av sådana frågor även måste beakta sannolikheten för att en potentiell riskkälla realiseras eller att någon har avsikt och förmåga att verkställa ett hot, samt konsekvenserna av den händelse som kan inträffa.

Som en direkt följd av detta konstateras vidare att man, för att kunna erhålla ett underlag som gör det meningsfullt att diskutera huruvida åtgärder måste vidtas, måste genomföra en samlad analys av samtliga dessa aspekter. Som exempel på olika typer av åtgärder framförs såväl förebyggande, där avsikten är att eliminera eller kraftigt reducera risken (vilket man definierar som riskhantering), som åtgärder som syftar till att bättre kunna hantera situationen om den ändå skulle inträffa (vilket man definierar som krishantering).

Den operativa användningen av de begrepp och definitioner som diskuterats i kapitlet kommer att redovisas i inledningen av del II av detta dokument. I nästa kapitel fortsätter bakgrundsbeskrivningen i form av en diskussion kring olika roller som myndighetssektorn kan sägas ha avseende skydd av allmänheten, följt av en beskrivning av en tänkbar modell myndigheters krishanteringsverksamhet.

6 Myndighetsroller samt en modell av krishanteringens uppbyggnad

Det nämndes i avsnitt 4.2.3 att den ändrade hotbilden gör att nationalstatens förmåga att skydda sina medborgare har kommit att ifrågasättas. Det förefaller lämpligt att översiktligt antyda hur detta skydd är strukturerat och organiserat. Betydelsen för denna rapport, och en mycket viktig sådan, är slutsatsen att myndigheternas risk- och sårbarhetsanalys enligt författarna bör omfatta det totala ansvarsområdet; d.v.s. dels den interna verksamheten, dels alla externa verksamheter som lyder under myndighetens föreskrifter och/eller tillsyn. Slutligen skisseras en möjlig modell för myndigheternas krishantering.

6.1 Myndigheters olika roller

Myndighetssektorn kan schematiskt sägas ha tre olika roller i relation till skydd av allmänheten (Strategy Unit, 2002).

- Föreskrivande och tillsynsutövande. Verktyg för myndighetsutövning inom denna roll inkluderar lagstiftning/föreskrifter, kontroll, inspektion, tillståndsgivning, råd och anvisningar, information, etc.
- som en bas eller källa för resurser (räddningstjänst, polis, sjukvård, etc.) att användas för skydd mot externa risker – naturkatastrofer, epidemier, stora olyckor i tekniska system, etc.
- som ansvariga för riskhanteringen av den egna verksamheten och för skydd av den egna resursbasen.

De olika rollerna, som är delvis överlappande, illustreras av figur 6.1 nedan. För en närmare diskussion hänvisas till publikationen (Strategy Unit, 2002).

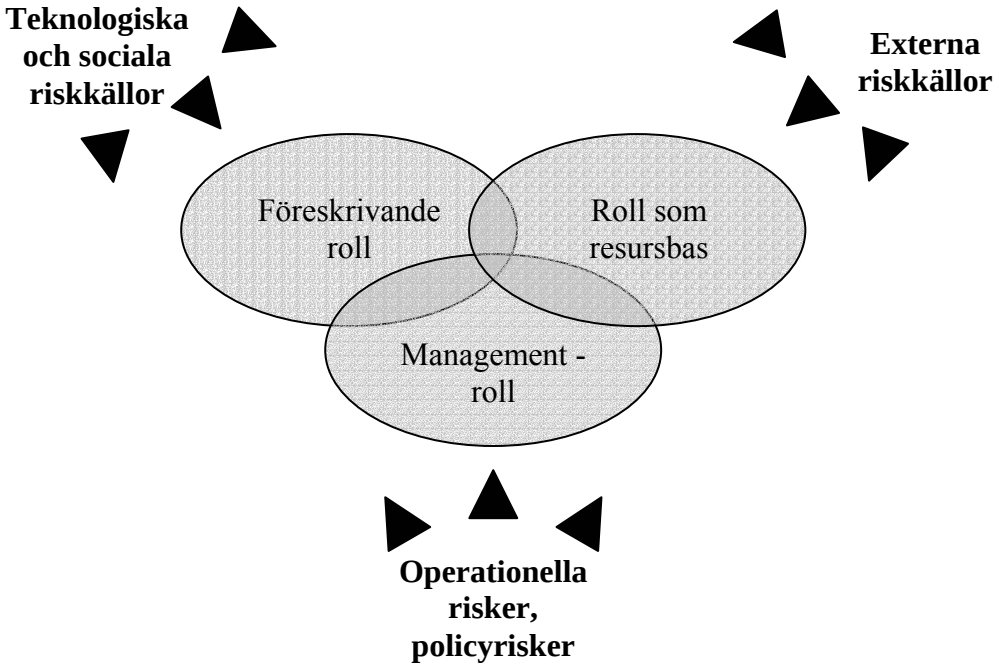
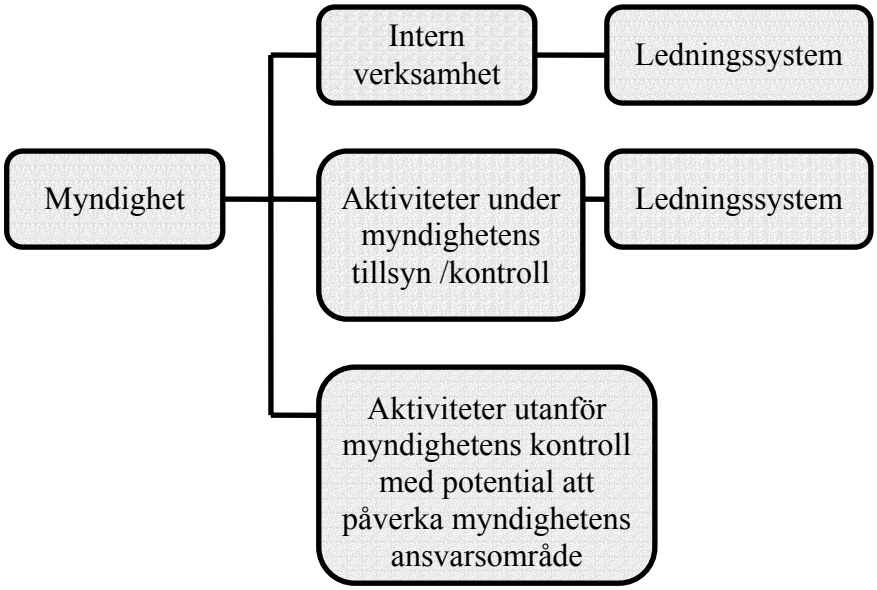


Fig.6.1 Myndigheters olika roller (Strategy Unit, 2002)

6.2 En modell av myndigheters krishanteringsverksamhet

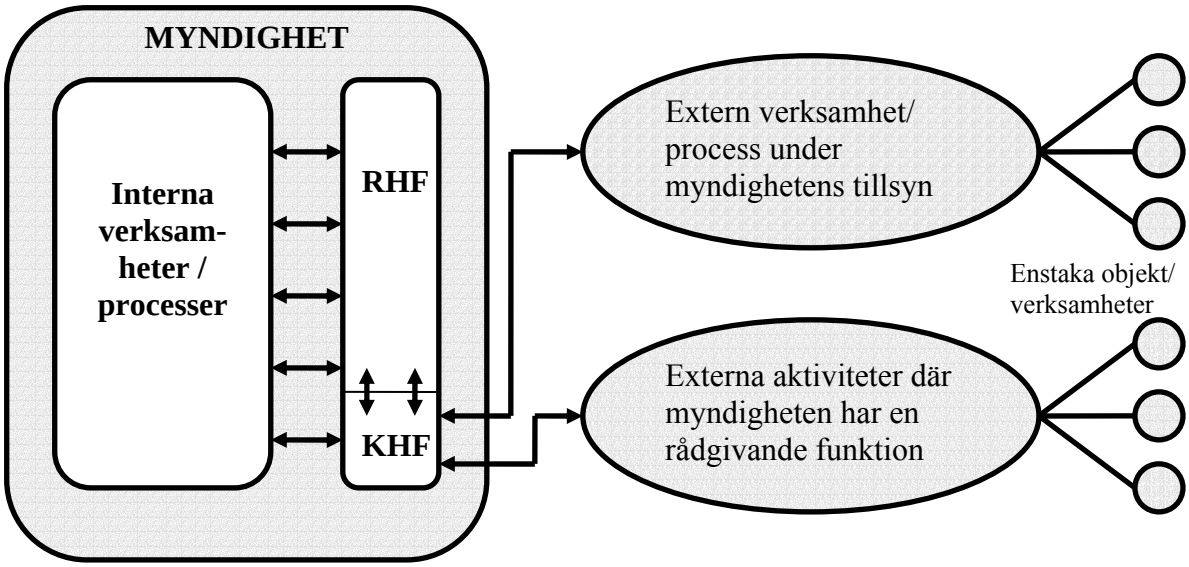
I kapitel 1 återgavs 3 § i *förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap* där varje myndighet åläggs att analysera sårbarhet och risker inom respektive *ansvarsområde*. I figur 6.2 nedan redovisas en indelning i tre delområden som vi anser bör beaktas i analysen enligt 3 §: intern verksamhet, aktiviteter under myndighetens tillsyn/kontroll, samt aktiviteter utanför myndighetens kontroll men som ändå kan påverka verksamhet inom myndighetens ansvarsområde.



Figur 6.2 Delområden som bör beaktas i analysen: intern verksamhet, aktiviteter under tillsyn/kontroll, samt aktiviteter utanför formell kontroll med potential att påverka myndighetens ansvarsområde.

Vi har tidigare även konstaterat att ordalydelsen i förordningens 4 § indikerar att de myndigheter som omfattas av paragrafen bör ha en väl utvecklad organisation för krishantering inklusive riskhantering av risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. Detta inkluderar i vår mening fungerande ledningssystem för hantering av nämnda risker. Riskerna kan finnas dels inom den interna verksamheten, dels inom de verksamheter som står under myndighetens tillsyn/kontroll. Ledningssystem för riskhantering diskuteras vidare i avsnitt 9.4.

Nedanstående figur (6.3) utgör ett försök att beskriva *en* modell för hur krisberedskapen och krishanteringen inom en myndighet kan fungera. Vi vill betona att figuren beskriver en *möjlig* och starkt förenklad organisationsstruktur och att existerande strukturer kan vara helt eller delvis avvikande. Figuren är avsedd att beskriva en principiell uppbyggnad som kan användas som ett diskussionsunderlag.



Figur 6.3 En möjlig modell för myndigheters krishanteringsverksamhet (RHF = Riskhanteringsfunktion, KHF = Krishanteringsfunktion).

Förordningen 2002:472 omfattar i sin 3 § ca 400 myndigheter och det är självklart att krishantering i förordningens mening utgör ett problem och ett verksamhetsområde av mycket varierande betydelse. Alla myndigheter torde emellertid uppleva att verksamheten får stora problem om exempelvis el- och IT-försörjningen slås ut under längre perioder. Slutsatsen blir att i stort sett samtliga myndigheter måste planera för avbrott av denna typ; d.v.s. ha en krishanteringsplan. Mot denna bakgrund föreslår författarna att myndigheterna inrättar en krishanteringsfunktion (KHF), se figur 6.3.

Författarna tolkar detta som ett fundament för att intentionen i förordningen skall kunna uppfyllas; att varje myndighet upprättar en funktion för krishantering med väl specificerad uppgift (inklusive exempelvis reviderbar egenkontroll). Grundläggande för KHF är bl.a. att samla information, analysera och syntetisera denna information, upprätta en krishanteringsplan, genomföra nödvändiga åtgärder och kontrollera deras effektivitet. KHF har att arbeta utifrån två perspektiv; ett inre och ett yttre, se figurerna 6.1 och 6.3. Det inre innebär ansvar för krishanteringen av den egna verksamheten och skydd av den egna resursbasen. Det yttre perspektivet innebär tillsyn, kontroll, inspektion, rådgivning och information rörande krishantering för externa aktiviteter och organisationer inom myndighetens ansvarsområde.

Som en del av risk- och sårbarhetsanalysen bör enligt författarna ingå:

- redovisning av uppbyggnad av krishanteringsfunktionen (KHF),
- redovisning av aktiviteten inom KHF, samt
- redovisning av eventuell krishanterings- eller beredskapsplan.

Med andra ord: det bör ingå en strukturerad analys av hur de processer/aktiviteter som översiktligt beskrivs av figurerna 6.1 och 6.3 genomförs vid myndigheten.

7 Myndighetsföreskrifter på säkerhetsområdet: något om struktur och utveckling

7.1 Inledning

I avsnitt 6.2 talades om begreppet *ansvarsområde* enligt 3 § i förordningen 2002:472 och att verksamheter som omfattas av en myndighets föreskriftsrätt och tillsyn/kontroll bör ingå i detta ansvarsområde. I detta kapitel ges en kortfattad beskrivning av olika typer av föreskrifter och tillsyn/kontrollverksamhet inom säkerhetsområdet.

Samverkan mellan myndigheter är en av grundförutsättningarna i det nya nationella krishanteringssystemet, se exempelvis KBM (2003b). Samverkan skall ske på lokal, regional och nationell nivå. Som bas för denna samverkan ligger de föreskrivande och tillsynsutövande funktionerna främst på nationell nivå.

För att närmare kunna beskriva och förstå funktionen av ovan nämnda föreskrivande och tillsynsutövande funktioner över det breda registret av samverkansmyndigheter bör en del grundläggande problemställningar belysas. Exempel på sådana frågor är:

- Vilka olika former av föreskrifter/kontroll används och hur effektiva är de?
- Hur påverkar utformningen av föreskrifter det praktiska myndighetsarbetet? Fördelar och nackdelar med olika utformningar.
- På vilket sätt bestäms valet av typ av myndighetsföreskrift av den aktivitet som skall regleras?
- Vad kan överföras från ett myndighetsområde till ett annat med en annan typ av teknologi, aktivitet, risk eller jurisdiktion?
- Slutligen: i vilken utsträckning kan föreskrifterna/kontrollen baseras på eller länkas till genomförda risk- och sårbarhetsanalyser?

Avsnitt 7.2 är avsett att ge en bakgrundsinformation för diskussion av dessa frågor.

7.2 Något om olika typer av föreskrifter och kontrollverksamhet

I detta avsnitt ges en mycket kortfattad beskrivning av olika typer av föreskrifter och kontrollverksamhet på säkerhetsområdet. För den som vill fördjupa sig inom området ges en utförligare beskrivning i ursprungsreferensen Hale et al (2002).

7.2.1 Olika typer av föreskrifter

Generellt sett kan sägas att det inom säkerhetsområdet växt fram tre huvudsakliga grupper av myndighetsföreskrifter:

Preskriptiva bestämmelser: Den traditionella strategin vad gäller föreskrifter som blev nödvändiga i och med den industriella revolutionen var att kräva att anläggningar uppfyllde mycket specifika tekniska krav avseende arbetsmiljön och utrustningen. Allt eftersom industrin utvecklades och teknologin blev alltmer avancerad ökade volymen av detaljföreskrifter i en sådan utsträckning att det under perioden 1950 – 1975 i alltfler sektorer

stod klart att hela förfarandet var för otympligt och okontrollerbart för att kunna användas i praktiken. Se Amalberti (2001) som *ett* exempel. Motsvarande exempel finns givetvis inom alla teknikområden.

Det stod klart att ett helt nytt synsätt hade blivit nödvändigt. Detta kom att kallas funktionsbaserade/målorienterade föreskrifter.

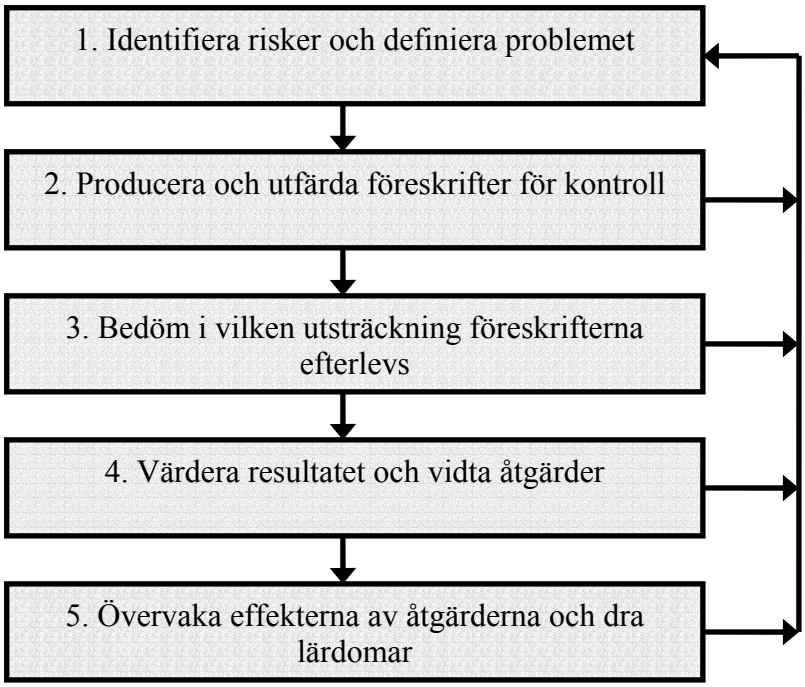
Målorienterade föreskrifter: Tidig skandinavisk lagstiftning under 1960-talet och den s.k. Robens-rapporten (Robens, 1972) i Storbritannien 1972 markerade början till en revolution på området säkerhetsföreskrifter. Mycket allmänt kan sägas att lagstiftningen gick från att ha specificerat standards och procedurer för att höja säkerheten till att föreskriva de säkerhetsmål verksamheten skulle uppfylla. Hur dessa mål kunde uppnås överläts, åtminstone i princip, till verksamhetsansvariga att utforma. Många industrisektorer har anpassat sina föreskrifter till antydd metodik. Problemet för myndigheterna är naturligtvis att för det första ange säkerhetsmål, för det andra definiera acceptanskriteria. En rad nya termer och begrepp har introducerats: bästa tillgängliga teknologi, praktiskt uppnåbar säkerhet, acceptabel/tolerabel risknivå etc. I praktiken kräver definitionen av dessa begrepp hänvisningar till specifikationer, standards och rutiner. Funktionsbaserade föreskrifter kan därför oftast ses som en mer flexibel form av preskriptiva bestämmelser.

Metoder byggda på ledningssystem för säkerhet och säkerhetsrapporter: Under senare år har regelsystemet genomgått en ytterligare förändring. I ökande grad krävs att arbetsgivare och anläggningsansvariga introducerar ledningssystem för säkerhet. I vissa regelsystem specificeras helt enkelt vad ledningssystemet måste uppfylla inom ramen för de generella säkerhetskraven. I andra fall, främst lagstiftningen för allvarliga olyckshändelser där farliga ämnen ingår (*Seveso II direktivet*) utgör ledningssystemet en viktig, obligatorisk, del av strategin med säkerhetsrapporter (se vidare avsnitt 9.4). Ytterligare exempel på viktiga lagstiftningsdokument med krav på ledningssystem utgörs av *AFS 2001:1 ”Systematiskt arbetsmiljöarbete”* och förordning *(1998:901) ”om verksamhetsutövares egenkontroll”*.

Denna typ av lagstiftning kräver att arbetsgivaren demonstrerar för ansvarig myndighet att organisationen har identifierat, bedömt och kan kontrollera viktigare riskkällor, vilket givetvis förutsätter att en riskanalys har genomförts. Seveso II direktivet beskriver relativt detaljerat det ledningssystem som måste implementeras. Vi har alltså återigen en återgång till preskriptiva bestämmelser. Skillnaden är att när tidigare kravsystem specificerade tekniska detaljer så specificerar modern lagstiftning hur ”säkerheten” i form av ledningssystem etc. skall hanteras.

7.2.2 Ett ramverk för bestämmelseskrivande, regelverk och kontroll

I avsnitt 7.2.1 identifierades tre modeller för innehållet i säkerhetsföreskrifter: teknisk beskrivning, funktionsbaserat regelsystem och lagstiftning baserad på säkerhetsrapport och säkerhetsledningssystem. För var och en av de tre föreskriftsregimer som nämns ovan kan aktiviteten beskrivas som en cyklisk process i fem steg:



Figur 7.1 Process för föreskrivande och säkerställande av efterlevnad (översättning från Hale et al 1997)

Vad som intresserar oss här är främst stegen 2 - 3. Hale et al (2002) konstruerade en matris där aktiviteter för stegen 2 och 3 indikeras för de tre föreskriftsregimerna, se figur 7.2 nedan.

Nivå	**Producera och utfärda föreskrifter**	**Kontrollera efterlevnad**
Mål/funktionsbaserade bestämmelser	**A**. Etablera acceptabla risknivåer	**B**. Kontrollera att utdata från verksamheten indikerar måluppfyllnad
Bestämmelser byggda på krav på säkerhetsledningssystem/ säkerhetsrapport	**C**. Skriv regler för säkerhets-ledningssystem och säkerhets-rapporter och hur dessa kontrollerar risker	**D**. Kontrollera struktur på och funktion av ledningssystemet
Direkt riskkontroll, preskriptiv metod	**E**. Utforma detaljregler för operativ nivå och process-utformning. Komponenter i figur 8.1.	**F**. Kontrollera att detaljregler för operativ nivå efterföljs

Figur 7.2 Aktiviteter vid produktion och utfärdande av föreskrifter, samt kontroll av efterlevnad för de tre föreskriftsregimerna (översättning från Hale et al, 2002).

I det refererade arbetet betonas att de sex uppgifterna A-F ovan för given typ av verksamhet i regel måste genomföras samtidigt för att riskerna skall anses kontrollerade.

I en bedömning av sårbarhetsläget inom en given sektor eller verksamhet bör enligt författarna ingå en utvärdering av i vilken utsträckning gällande föreskrifter och utförd kontroll (tillsyn) inklusive egenkontroll är en acceptabel bas för minimering av sektorns sårbarhet. Vad gäller tillsynen konstaterar SOU 2001:41, *"Säkerhet i en ny tid"*, i kapitel 11 att det finns skillnader i tillsynsorganens förutsättningar att effektivt lösa sin uppgift. En del av dessa skillnader kan förmodligen återkopplas till figuren 7.2 med dess tre föreskriftsregimer med åtföljande krav på utformning av tillsynsarbetet. Som betonats tidigare måste i regel samtliga sex aktiviteter A-F genomföras samtidigt för att erhålla en heltäckande kontroll av riskerna i en verksamhet.

Detta ger upphov till en rad (intressanta) frågeställningar:

- Vilken aktör utför de enskilda uppgifterna A-F för den reglerade sektorn eller aktiviteten? Myndighet på nationell, regional eller lokal nivå? Verksamhetsägare? Tredje part?
- I den mån myndigheter är inblandade, hur fördelas ansvaret mellan nationell, regional och lokal nivå och vilka otydligheter i ansvarsfördelningen medför detta?
- Är en sådan områdesuppdelning optimal för en minimering av sårbarheten?

Myndigheter använder i ökande omfattning ackreditering och (tredje parts) certifiering som ett partsoberoende och transparent medel att tillse att organisationer följer föreskrifterna. Möjliga följdproblem inkluderar:

- Att konsumenter och fackföreningar utesluts från inflytande.
- Myndigheternas möjligheter att tillse efterlevnad inskränks.
- Riksdagens lagstiftningsmakt minskar i de konkreta fallen.

Detta är en utveckling som accelererar till följd av den snabba och dynamiska utvecklingen inom nya teknologier och som inte borde lämnas obeaktad.

7.3 Risk- och sårbarhetsanalyser och de tre olika föreskriftsregimerna

I de risk- och sårbarhetsanalyser som myndigheterna skall producera bör enligt författarna ingå en analys av myndighetens funktion och en möjlighet att specificera exempelvis:

- Vem som ansvarar för regelsystem (rutiner, instruktioner) på operativ nivå.
- Vem som kontrollerar efterlevnad på operativ nivå.
- Vem som utfärdar föreskrifter för säkerhetsledningssystem och ledningssystem för krishantering.
- Vem som utvärderar effektiviteten av ledningssystemen.
- Vem som etablerar nivå för acceptabel risk.
- Vem som kontrollerar att denna nivå uppfylls,

samt en genomgång av de problem och dilemman som svaren på frågeställningarna ovan eventuellt skapar.

8 Olika typer av grundorsaker till svåra påfrestningar

Det är naturligtvis en truism att konstatera att en svår påfrestning kan ha en rad olika grundläggande orsaker och vara resultatet av händelsekedjor med vitt skilda karakteristika. Vi har valt att i kapitel 8 särskilja mellan tre typer av grundläggande orsaker:

- Typ 1 kan efter Reason (1997) benämnas organisatoriska olyckor. Orsakerna till dessa olyckor kan vara av mänskligt, organisatoriskt eller tekniskt ursprung. De inträffar relativt sällan, men är ofta katastrofartade om de väl inträffar, i exempelvis kärnkraftverk, kommersiell flygtrafik, petrokemisk industri, kemisk processindustri, transport på järnväg och hav, bankväsendet och samlingspunkter för ett stort antal människor (idrottsanläggningar, brand på diskotek). Till denna grupp kan vi också hänföra fenomen av typen ”allvarlig smittspridning” genom att organisatoriska brister (tillsyn, kontroll) kan anses skapa förutsättningar för uppkomst av svår påfrestning.

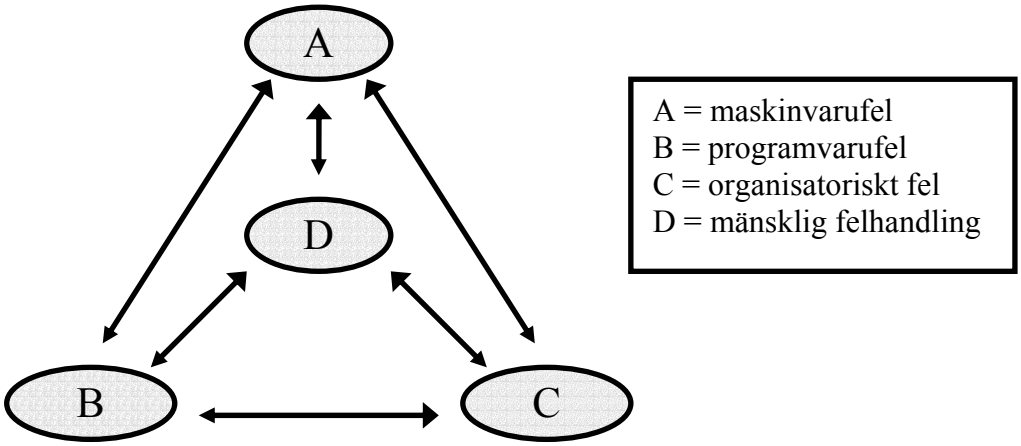
- Typ 2: naturkatastrofer av olika slag.

- Typ 3: terroristangrepp och andra typer av avsiktlig påverkan. Bl.a. refereras kortfattat några synpunkter från en storskalig amerikansk utredning initierad p.g.a. WTC-katastrofen.

Utelämnade är därmed exempelvis påfrestningar som beror av finansmarknadens kollaps, internationella konflikter, etc.

8.1 Grundläggande orsaker till svåra påfrestningar enligt typ 1

Felorsaker för en svår påfrestning av denna kategori kan generellt grupperas enligt figur 8.1 nedan (Haimes, 1998):



Figur 8.1 Felorsaker

En rad undersökningar har visat att ca 80 % av riskrelaterade oönskade händelser och förlopp beror på faktorn C; d.v.s. organisatoriska fel. Innebörden är att om målsättningen med förordning 2002:472 skall kunna uppfyllas bör enligt författarna myndigheternas risk- och sårbarhetsanalyser innehålla en bedömning av den egna förmågan att förhindra att

organisatoriska brister bidrar till att en ”normal” riskkälla utlöser en händelsekedja som i slutändan innebär en svår påfrestning. Detta krav gäller också de externa aktiviteter/organisationer som ligger inom myndighetens kontroll- och/eller tillsynsuppgift eller allmänna ansvarsområde.

Några typiska orsaker till organisatoriska fel (C ovan) är:

- Förbisedda eller ignorerade defekter.
- Dröjsmål med att korrigera defekter.
- Sammanbrott i kommunikation.
- Missade signaler eller annan typ av data till följd av försummad inspektion eller undermåligt underhåll.
- Olösta konflikter mellan ledning och arbetskraft.
- Döljande av misstag på grund av exempelvis konkurrensskäl.
- Effekter av ”down-sizing” och ”outsourcing”.
- Generellt sett undermålig säkerhetskultur.

8.1.1 Olyckor av typ 1. En förklaringsmodell

En ”normal” slumpartad händelse eskalerar till en katastrof genom brister i de olika barriärer d.v.s. försvarssystem och skyddsåtgärder som upprättats. Bristerna kan uppkomma genom aktiva fel och latenta förhållanden (Reason, 1997), se figuren nedan.

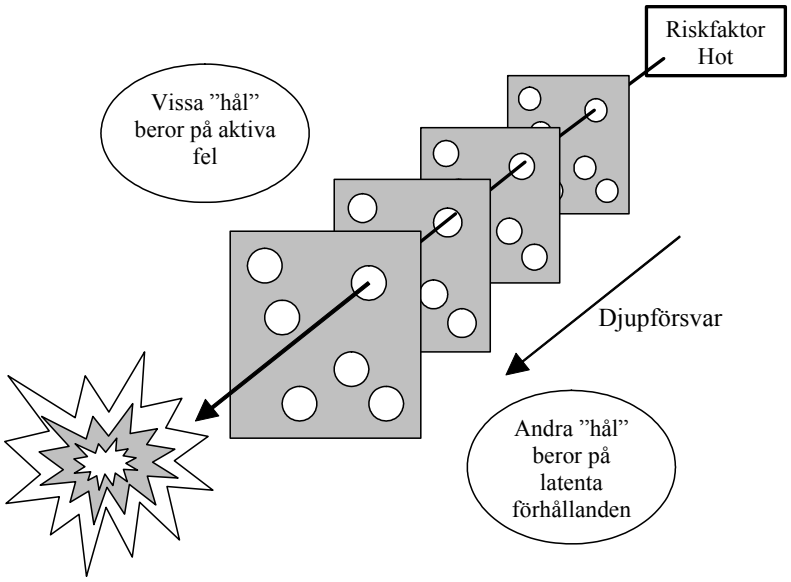


Fig. 8.2 Reasons ”schweizerostmodell” (översatt från Reason, 1997)

I dagens samhälle finns stora komplexa sociotekniska system med potential att åstadkomma allvarliga kriser som kan leda till svåra påfrestningar i samhället. Det finns ofta försvar mot att enstaka händelser ska kunna orsaka sådana kriser. Ofta finns olika typer av försvar som verkar i olika delar av orsaksträdet – det finns ett djupförsvar (defense-in-depth). Krisen uppstår när alla barriärerna bryts igenom. I följande resonemang utgår vi från Reasons (1997) schweizerostmodell (se figur 8.2) för att diskutera organisatoriska olyckor, så stora att de medför svåra påfrestningar. Epitetet ”organisatoriska” betyder att man hittar orsakerna på

olika nivåer i en organisation – i ett system – som kan innefatta hela kedjan från lagstiftare, via tillsyn, strategisk ledning, taktisk ledning till process.

Försvarsbarriärerna illustrerade i figur 8.2 är av olika typ. Här följer ett exempel som illustrerar vilka typer det kan vara.

- Verksamheter som ska öka förståelsen och medvetenheten om faror.
- Stöd för säker styrning/hantering av en process.
- Larm och varningssignaler.
- Metodik eller automatik som återför systemet i ett säkert tillstånd om det hamnat utanför en säker zon.
- Fysiska barriärer mellan riskkällan (energin i vid bemärkelse) och riskobjektet (target = människor, miljö, infrastruktur) om tillämpligt.
- Arrangemang för att innesluta och eliminera energin om den passerat de fysiska barriärerna – om tillämpligt.
- Möjligheter att fly undan faran.

Barriärerna har emellertid brister illustrerade med hålen i ostskivorna (figur 8.2). I modellen kan var och en av skivorna med hål i röra sig i sid- och höjdled, vilket innebär att det kan inträffa att barriärerna intar ett sådant läge att en utlöst riskkälla eller hot inte ”fångas upp” av någon av de barriärer som konstruerats för att bryta förloppet, vilket i nästa steg leder till negativa konsekvenser på systemet och dess omgivning.

Hålen och rörelserna orsakas av s.k. aktiva fel och latenta förhållanden. Medvetna fel och fel med avsikt att skada kan naturligtvis också i hög grad bidra till att barriärerna inte fyller sin funktion.

Aktiva fel är fel som personer gör i direkt kontakt med processen – det kan t.ex. vara en operatör som trycker på fel knapp p.g.a. förväxling eller felbedömning. Det aktiva felet utlöser olyckan/krisen, men det är ofta kontraproduktivt att skylla händelsen på operatörens fel. Människor gör fel. System måste konstrueras så att ett mänskligt fel eller en kombination av några mänskliga fel inte ska kunna utlösa en stor olycka.

Latenta förhållanden är förhållanden som skapats av beslutsfattare och konstruktörer. De har oftast funnits under lång tid före olyckan. De kan bidra till att det aktiva felet görs eller till att det aktiva felet får katastrofala effekter. Latenta fel kan även medföra katastrof utan något aktivt fel (t.ex. Challengerolyckan). Typer av latenta förhållanden är:

- Dålig utformning av människa-tekniksystem.
- Brister i ledningen.
- Brister i underhållet.
- Brister i utbildning och träning.
- Icke-adekvata verktyg/hjälpmedel.

En organisatorisk olycka kan således ha sitt ursprung i strategiska beslut och processer i organisationen som budgetering, annan allokering av resurser, planering, schemaläggning, kommunikation, ledning, revisioner mm – processer färgade av organisationskulturen, speciellt säkerhetskulturen. Under olyckliga omständigheter, oftast inkluderande aktiva fel,

fungerar plötsligt inga barriärer och olyckan är ett faktum – under mycket olyckliga omständigheter blir det en svår påfrestning.

För en proaktiv krishantering är det viktigt att identifiera de beslutsfattare/beslutande organ som kan påverka ett händelseförlopp som kan sluta i en svår påfrestning. Eftersom vi inte kan förutse allt – speciellt svårt är det med komplexa system – måste vi också skapa adaptiva system med återkopplingar/lärande som är mindre känsliga för störningar och snabbt styr mot ett säkert mål. Goda ledningssystem och en god säkerhetskultur är viktiga ingredienser.

8.1.2 Interdependens i tekniska infrastruktursystem; speciellt el- och vattenförsörjning

En mycket viktig undergrupp av förhållanden som kan leda till svår påfrestning av typ 1 är komplexitet och interdependens i tekniska infrastruktursystem. Låt oss betrakta infrastrukturen för el- och vattenförsörjning. Elenergi- och vattenförsörjningen är vitala för samhällets förmåga att fungera. En allvarlig störning på något av dessa system innebär en krissituation som kan ha stora konsekvenser för samhället. Störningen på systemet kan ha mycket olika bakgrund, allt ifrån terrorism och sabotage till tekniska kollapser, naturkatastrofer eller angrepp på informations- och automationssystem. Det finns en mycket nära koppling mellan el- och vattenförsörjningen samt tele- och IT-stöd.

8.2 Grundläggande orsaker till svåra påfrestningar enligt typ 2: naturkatastrofer

Samhällets krisberedskap och krishantering har historiskt sett haft denna typ av svåra påfrestningar som ett av sina huvudansvar. Metodiken att klara dess uppgifter är väl utprovad och beskriven i ett mycket stort antal publikationer. Avseende den förebyggande fasen (mitigation) av krishanteringen utgör FEMA (1997) ett mycket gott exempel.

Vi nöjer oss med att här mycket kort redovisa de huvudsakliga dragen i ett examensarbete från 2001, där Andersson och Kinnerberg (2001) behandlar naturkatastrofers bidrag till riskbilden i EU. Med begreppet katastrof avses i det refererade arbetet situationer där de lokala räddningsresurserna har varit otillräckliga eller då konsekvenserna överstigit vissa nivåer. Naturkatastrofer delas in i följande kategorier: laviner, stormar och tornados, skogsbränder, jordbävningar, vulkaner och skred, dammbrott, översvämningar och flodvågor, torka, och slutligen värmeböljor.

Bland de slutsatser som drogs från arbetet kan nämnas att antalet naturkatastrofer ökar över tiden och ökningen kan förväntas fortsätta i framtiden, att *översvämningar och flodvågor* samt *stormar och tornados* är de två kategorier av naturkatastrofer som är vanligast förekommande inom EU, att *jordbävningar, vulkaner och skred* samt *extremtemperatur* är de kategorier av naturkatastrofer som kräver flest liv per inträffat tillfälle, samt att utvecklingen medför att samhället blir alltmer sårbart p.g.a. fler avancerade tekniska system och en ökad bebyggelse.

8.3 Grundläggande orsaker till svåra påfrestningar enligt typ 3: terrorism och andra typer av avsiktlig påverkan eller skada

Avsiktliga attacker mot exempelvis infrastrukturer kan bara avvärjas om hotet upptäcks i tid och/eller försvarsmekanismer byggts upp som neutraliserar hotet. Självklara begränsningar i tillgängliga resurser innebär, i kombination med den mycket breda hotbilden, att prioriteringar måste göras, d.v.s. kvantifiering i någon form är nödvändig. Problemet är att för ett givet system kategorisera spektrat av existerande hot, finna systemets svagaste punkter och prioritera insatser för förstärkning.

I stort sett omedelbart efter 11 september 2001 påbörjade i USA de ledande vetenskapsakademierna, National Academy of Sciences, National Academy of Engineering och Institute of Medicine, koordinerade av National Research Council (NRC, 2002) en utredning om de tre frågeställningarna:

- Hur identifieras hotbilden?
- Hur identifieras systemets svagaste punkt eller länk?
- Hur prioriteras användning av tillgängliga resurser för att förstärka systemet?

Ett annat perspektiv var att klargöra hur vetenskap och teknologi kan användas för att förstärka försvaret mot terrorism samt de FoU-insatser som bör prioriteras. Utredningen, som hade stora personella resurser till förfogande, delade in arbetet i följande hot/riskområden:

1. Nukleära och radiologiska hot
2. Smittsamma sjukdomar och spridning av farliga biologiska gifter
3. Toxiska kemikalier och explosiva ämnen
4. Informationsteknologi
5. Energisystem
6. Transportsystem
7. Urban bebyggelse och fasta infrastruktursystem
8. Terrorhandlingar och allmänhetens reaktion
9. Komplexa och interdependenta system.

För varje delområde gjordes en genomgång av hotbilden, en lägesbeskrivning av sårbarheten, konkreta åtgärder för att minska densamma, en bedömning av vetenskapens och teknologins roll i sammanhanget samt förslag till utvecklingsåtgärder. För en utförlig beskrivning hänvisas till ursprungsreferensen (NRC, 2002).

8.4 Fenomenet extrema händelser

Begreppen ”extrem händelse” och ”svår påfrestning” har en tydlig koppling. I detta avsnitt diskuteras därför generellt ”extrema händelser” både i avseendet att den utlösande orsaken till den slutliga skadan i sig är av katastrofal storlek och/eller extrem natur (typexempel naturkatastrofer) samt förlopp där den slutliga konsekvensen är av extrem natur.

I detta avsnitt diskuteras generellt ”extrema händelser” både i avseendet att den utlösande orsaken till den slutliga skadan i sig är av katastrofal storlek och/eller extrem natur (typexempel naturkatastrofer) samt förlopp där den slutliga konsekvensen är av extrem natur.

”Extrema händelser” (vilket kan omfatta samtliga tre typer av grundorsaker till svåra påfrestningar) definieras genom att vara sällsynta, ha mycket allvarliga konsekvenser och vara utanför vad som normalt förväntas inträffa inom systemet ifråga. Detta innebär inte nödvändigtvis att de fysiska skadorna i sig är katastrofala; verkan kan förstärkas och förstoras i det allmänna medvetandet genom att händelsen förknippas med en hög grad av fruktan, osäkerhet och ofrivillighet.

Extrema händelser orsakas ofta av icke-linjära fenomen sådana att en relativt liten ändring i en ingångsparameter leder till en stor ökning i konsekvenserna. Byggnadskollapser, dammbrott, härdsmälta i kärnreaktor är exempel på extrema olyckor där en liten ökning i en miljöfaktor (belastning, vattennivå, härdtemperatur) kan resultera i en snabb övergång från en nästan-olycka till en katastrof. Synergistiska effekter är ofta medverkande: vattenmättad mark i kombination med nya kraftiga regn leder till att en ”normal” översvämning blir katastrofartad. Sociala gruppers beteenden kan ibland modelleras som icke-linjära, dynamiska förlopp av den typ som nämnts ovan.

Litteraturen om extrema händelser och metoder för riskanalys är omfångsrik; vi nöjer oss med att referera den översikt som gavs i Bier et al (1999). Författarna påpekar att extrema händelser allvarligt testar den traditionella riskanalysens användbarhet och värde som beslutsunderlag. Speciellt bekymmersam är avsaknaden av tillförlitliga indata, särskilt vad gäller olika felorsakers frekvens. Sett mot bakgrund av riskanalysens generella målsättning att ge en sannolikhetsfördelning för möjliga skador/konsekvenser är detta naturligtvis ett problem. Bier et al påpekar att analysen kan förenklas till att bestämma sannolikheten för ett tröskelvärde; d.v.s. ett enstaka, diskret värde. Som exempel kan nämnas bankkonkurs. Vet vi att en förlust av en viss storlek leder till ett sammanbrott behöver vi inte bekymra oss om sannolikheten för en konsekvens av ännu större förluster. Samma resonemang kan naturligtvis appliceras på en mängd analysområden.

I referensen diskuteras riskanalysens allmänna praktiska användbarhet i generella termer och dessutom beskrivs metoder att förbättra giltigheten. Exempel på sådana metoder är extremvärdesteori, Bayesiansk uppdatering av sannolikheter, metoder att behandla imprecisa sannolikheter, systematisk känslighetsanalys, identifiering av scenarier via metoder som bygger på dekomposition av det aktuella systemet etc.

8.5 Några teorier om krisers orsaker och uppkomst: sambandet riskhantering – krishantering

Det ramverk för krishantering som visas i figuren 4.2 bygger på en helhetssyn som växt fram under det senaste årtiondet. Figuren demonstrerar en process i fyra olika steg eller faser. Krishanteringen har traditionellt varit koncentrerad till faserna 2 – 4 medan fas 1, som väsentligen är en process för risk- och sårbarhetsanalys, ofta har spelat en undanskymd och implicit roll. Till detta har säkert bidragit att två grundläggande frågor får anses outredda:

- I vilken utsträckning kan effekten av stora olyckor och katastrofer över huvud reduceras genom preventiva åtgärder?
- Hur åstadkoms en optimal avvägning mellan åtgärder som hör till fas 1 och åtgärder som definieras av faserna 2 – 4?

Med utgångspunkt från de ”situationer” som anges i 3 § av förordning 2002:472 skall vi här översiktligt försöka skissera den vetenskapliga basen för en diskussion kring frågeställningarna ovan.

Grovt förenklat kan vi urskilja fyra teoribildningar om orsaken till att olyckor och katastrofer inom främst teknologiska system uppkommer.

- Reason’s ”schweizerostmodell” som skisserades i avsnitt 8.2.
- Perrow’s ”Normal Accident Theory” (NAT) redovisad i standardverket från 1984 och i en reviderad version från 1997 (Perrow, 1984; Reason, 1997).
- Modell för ”High Reliability Organisations” (HRO), (La Porte, 1981).
- Turners arbete om ”Man-Made Disasters” och ”Disaster Incubation Theory” (DIT) från 1978 och 1996 (Turner och Pidgeon, 1997).

Ovanstående referenser hänvisar bara till vissa ursprungsarbeten, för andra nödvändiga referenser och en introduktion hänvisar vi till Rijpma (2003).

Perrow’s NAT introducerade den nu välkända hypotesen att stora olyckor är oundvikliga i vissa teknologiska system. System kännetecknade av en interaktiv komplexitet och en tät koppling mellan systemdelarna har denna egenskap. Komplexiteten orsakar oundvikliga och oväntade interaktioner mellan oberoende felkällor. Den täta kopplingen medför att initiella störningar snabbt eskalerar till ett systemsammanbrott.

HRO-skolan intar en nära nog diametralt motsatt attityd: det är fullt möjligt att utforma organisatoriska åtgärder och strategier som i stort sett eliminerar sannolikheten för uppkomst av stora olyckor. Denna slutsats är baserad på undersökningar av och observationer från aktiviteter/organisationer som flygledarcentraler, hangarfartyg och elektrisk kraftproduktion. Fyra egenskaper definieras som karakteristiska: ledningen ser säkerhet och tillförlitlighet som en prioriterad uppgift; tillräcklig redundans i tekniska och personella resurser för att kompensera uppkomna fel; en stark organisationskultur på området tillförlitlighet och, slutligen, ett kontinuerligt organisatoriskt lärande med erfarenhetsåterföring och proaktiva simuleringsövningar.

Turners grundläggande tes (DIT) är att katastrofer framkallas av oförmågan att insamla och tolka information och varningssignaler samt att med utgångspunkt från dessa förutse framtida händelser. Under lång inkubationsperiod ignoreras eller missförstås signaler om framtida hot och faror till dess att katastrofen inträffar. Fast grundad övertygelse om att ingenting kan gå fel kombinerad med fragmentarisk information och en svag och otillräcklig ledningsfunktion leder förr eller senare till en olycka. Ackumulerings- eller inkubationstiden kan sträcka sig över många år.

De olika teoriansatserna ovan ger upphov till olika strategier för förhindrande av uppkomst av svåra påfrestningar och för att minimera den totala skadeeffekten. Som antytts är det ännu outrett vilken teori som bäst ”förklarar” uppkomsten av de situationer som beskrivs i 3 § i förordning 2002:472. Några allmänna slutsatser kan emellertid dras.

- Tre av hypoteserna ovan (Reason, HRO, DIT) innebär en betoning av metoder/åtgärder av typen risk- och sårbarhetsanalyser, kontroll och tillsyn, organisatoriska ledningssystem och revisionsmetoder, förbättring av säkerhetskultur. Innebörden är en ökad betydelse av åtgärder inom ruta 1 av figuren 4.2. Om NAT-

synsättet visar sig vara bästa förklaringsgrunden ökar i motsvarande grad betydelsen av faserna 2 – 4 i figur 4.2.

- Den utveckling som antyddes i avsnitt 4.2.3 avseende 2000-talets kriser antyder att förmågan till effektiva förebyggande åtgärder kan komma att bli mer begränsad, d.v.s. faserna förberedande, akut avhjälpande och återställande ökar i betydelse.

- Den för författarna avgörande slutsatsen är emellertid denna: Vid analys av många stora olyckor har man funnit att management och organisatoriska förhållanden (inklusive säkerhetskultur) haft avgörande betydelse för olyckornas uppkomst, t.ex. Bhopal (1984), Tjernobyl (1986), Herald of Free Enterprise (1987), King's Cross-stationen (1987), Estonia (1994) och diskoteksbranden i Göteborg (1998). Management och organisatoriska förhållanden kan påverka sannolikheten för olycka med flera 10-potenser (Kirwan, 1994). Vi kan inte vänta på att få mer kunskap från katastrofer av dessa magnituder utan måste av etiska skäl arbeta proaktivt. Brister i ledningssystem, management och organisatoriska förhållanden måste åtgärdas.

8.6 Några slutsatser vad gäller risk- och sårbarhetsanalys enligt förordning 2002:472

Av kapitel 8 kan vi dra åtminstone följande slutsatser:

- De tre olika grupperna av risker och hot som beskrivits ovan bör enligt författarna samtliga behandlas i risk- och sårbarhetsanalyserna om dessa skall kunna användas som beslutsunderlag. De kräver också olika åtgärdsstrategier. Oerhört förenklat kan påstås att typ 1 motverkas genom att det normala riskhanteringssystemet fungerar, typ 2 genom att samhällets totala krishantering är effektiv, typ 3 genom speciella åtgärder som förstärkning av skydd mot intrång, etc.

- Författarna vill framhålla den uppenbara länken mellan generell riskhantering och krishantering avseende risker och hot av typ 1 ovan.

9 Standards samt ramverk för riskhantering

Vi har tidigare konstaterat (avsnitt 8.1) att det vore en fördel om myndigheters evaluering av sannolikheten för uppkomst av en svår påfrestning byggde på en bedömning av ifrågavarande verksamhets totala riskhantering.

Generella krav på svenska myndigheters riskhantering har fram till nu bestämts av förordningen 1995:1300 *om statliga myndigheters riskhantering* som bl.a. innehåller följande passus:

> ***”Riskanalys och skadeförebyggande åtgärder***
> ***3 §*** *Varje myndighet skall identifiera vilka risker för skador eller förluster som finns i myndighetens verksamhet. Myndigheten skall värdera riskerna och beräkna vilka kostnader som staten har eller kan få med hänsyn till dessa risker. Resultatet skall sammanställas i en riskanalys.*
> *Varje myndighet skall vidta lämpliga åtgärder för att begränsa risker och förebygga skador eller förluster.”*

Det huvudsakliga syftet med förordningen tycks vara att reglera myndigheternas riskfinansiering och speciellt då försäkringsfrågor. Vi har inte funnit något exempel på att förordningen använts för att organisera och genomföra en myndighets riskhantering i vid bemärkelse.

Författarna anser att statens passivitet ter sig förvånande om man noterar den aktivitet som rått internationellt främst under den senaste 5-årsperioden. I en rad länder har statsmakten (ofta i samarbete med näringslivet) producerat vägledningar, standards, etc. för organisationernas riskhantering. Vi nöjer oss här med att hänvisa till dokument från Storbritannien. I förordet till rapporten från Strategy Unit (2002) konstaterar premiärministern bl.a.:

> *”The report sets out how government should think about risk, and practical steps for managing it better. It proposes principles to guide handling and communication of risks to the public – on which we are seeking views from all interested parties.*
>
> *Risk management – getting the right balance between innovation and change on the one hand, and avoidance of shocks and crises on the other – is now central to the business of good government”*

Samtidigt kan påpekas att svenska kommunförbundet bl.a. genom sin vägledning ”Verksamhetsanalys och säkerhetssamordning” (Kommunförbundet, 2001) har lagt grunden för en förbättrad riskhantering på det lokala planet.

Nedanstående mycket kortfattade sammanfattning av existerande vägledningar på området är främst hämtade från dokument utfärdade av ministerier i Storbritannien (eller av kabinettet). Ibland källorna kan nämnas:

- Strategy Unit report – ”Risk: Improving government’s capability to handle risk and uncertainty” (Strategy Unit, 2002)
- HM Treasury – ”Management of Risk – A Strategic Overview” (Orange book) (HM Treasury, 2001)
- UK Department for Environment, Food and Rural Affairs - ”Risk Management Strategy”, (DEFRA, 2002)

Det bör nämnas att utvecklingen på myndighetsområdet har föregåtts av motsvarande utveckling inom näringslivet. Ett aktuellt exempel utgörs av:

- The Committee of Sponsoring Organizations of the Treadway Commission – *”Enterprise Risk Management Framework”*, (COSO, 2003).

9.1 Vad är ett ramverk för riskhantering?

Vi har tidigare visat ett ramverk för krishantering, se avsnitt 4.2. Dessutom påpekade vi i kapitel 1 och avsnitt 6.2 att formuleringen av krisberedskapsförordningens § 4 föranleder att de myndigheter som omfattas av paragrafen rimligen bör ha etablerat ett ramverk för riskhantering för att intentionen i paragrafen skall kunna anses uppfylld.

En organisations strategi för riskhantering måste vara konsistent och balanserad över organisationens totala verksamhetsområde. Ett ramverk för riskhantering definierar den kontext inom vilken risker hanteras: hur de identifieras, analyseras, kontrolleras, övervakas och bedöms i en fortgående revisionsprocess. Ramverket måste vara konsistent med och förankrat i de processer som ingår i den kontinuerliga ledningen av organisationen; det beskriver hur:

- risker identifieras
- information hämtas in beträffande sannolikhet och potentiella utfall
- de kan kvantifieras eller rangordnas med hänsyn till osäkerheter och tillgång till expertråd
- möjliga metoder att hantera riskerna identifieras
- riskbeslut fattas
- riskbeslut implementeras
- effektiviteten av olika åtgärder/beslut utvärderas
- lämpliga kommunikationsmekanismer sätts upp och implementeras

Det sätt på vilket olika myndigheter behandlar sina risker är naturligtvis delvis unikt. Det finns emellertid ett antal element som alla myndigheter behöver förbättra för att effektivisera sin riskhantering; se figuren 9.1 nedan:

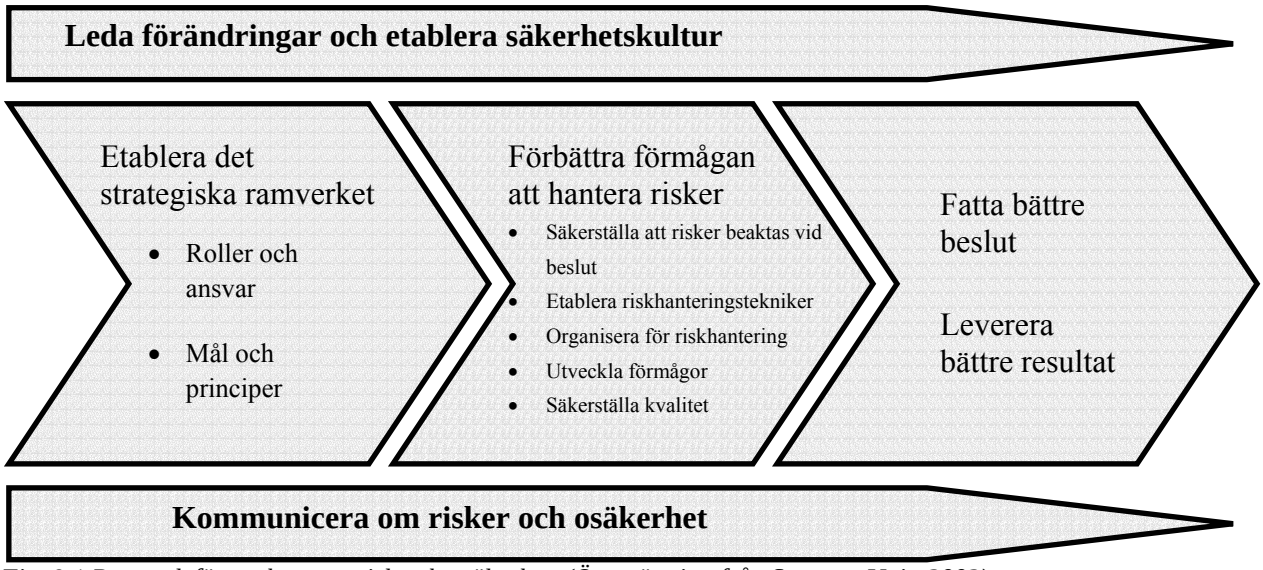
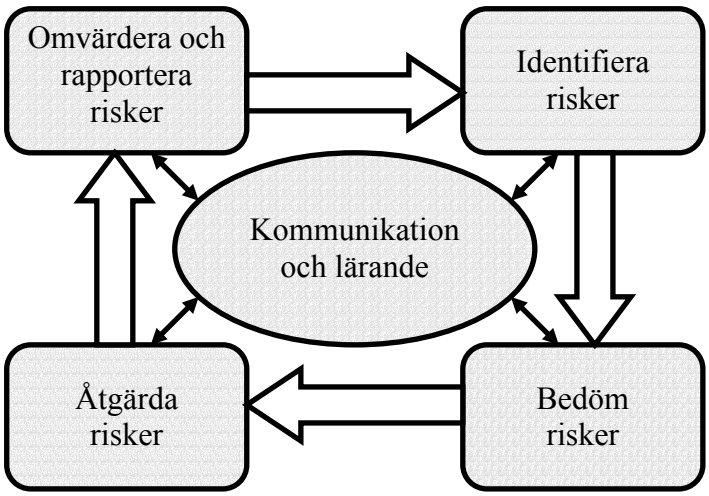


Fig. 9.1 Ramverk för att hantera risk och osäkerhet. (Översättning från Strategy Unit, 2002)

En uppföljning av elementen i ramverket innebär bl.a.

- att alla stora policy- och programbeslut tar explicit hänsyn till riskaspekten och balansen risk/nytta
- att system, processer och incitament för en effektiv riskhantering finns tillgängliga
- att det finns mekanismer för att säkerställa att risker hanteras på den nivå detta sker mest effektivt
- att en riskhanteringskompetens skapas bland beslutsfattare och experter
- att klara kvalitetsstandards och kvalitetssäkringsmetoder har införts
- intern och extern kommunikation om valda metoder att hantera risker bidrar till att öka anställdas och allmänhetens förtroende för fattade beslut
- att hela processen drivs och kontrolleras från myndighetens högsta ledning.

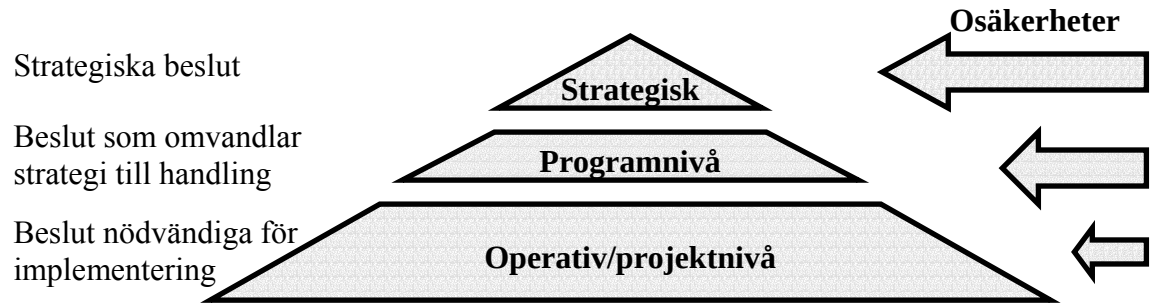
Elementen i figur 9.1 ovan kan lämpligen konkretiseras i ett cykliskt ramverk för riskhantering, se figur 9.2 nedan.



Figur 9.2 Process för riskhantering (Översättning från Strategy Unit, 2002)

9.2 Riskhanteringens tre nivåer, speciellt behandling av strategiska risker

Författarna anser att myndigheter måste kunna hantera risk på åtminstone tre nivåer: strategisk nivå, program/projektnivå och operativ-/anläggningsnivå. Figur 9.3 nedan illustrerar riskhierarkin med en indikation på osäkerheter förknippade med de olika nivåerna.



Figur 9.3 Olika nivåer av riskhantering.

Risk- och sårbarhetsanalyser på de olika nivåerna kommer att diskuteras i del II av detta dokument, här ges bara några kommentarer till begreppet strategiska risker.

Allmänt innebär en god riskhantering på denna nivå att ledning och styrelse kan påvisa att policybeslut och andra viktiga beslut fattas efter en strukturerad och väl underbyggd analys av risker och osäkerheter förknippade med de olika alternativen för handlande. I Krishanteringssammanhang avses dessutom bl.a. att procedurer finns för att säkerställa att risker på lägre nivå inte eskalerar till den nivå som beskrivs i 3 § av förordningen 2002:472 samt att krishanterings- och krisberedskapsaspekter beaktas vid val av policyalternativ. Detta innefattar planering för att kunna upprätthålla kritiska aktiviteter, exempelvis kontinuitetsplanering och insatsplanering, samt för att kunna hantera frågor som rör relationen till allmänheten, exempelvis förtroende och trovärdighetsaspekter. Vid utvärderingen av krishanteringens och krisberedskapens effektivitet bör speciellt dominoeffekter av risker och sårbarhet inom andra myndigheters ansvarsområden beaktas.

9.3 Några kommentarer till den generella riskhanteringsprocessen

Nedan följer några kortfattade kommentarer till figurerna i kapitel 9.1.

<u>Etablera ramverket</u>

Minimikraven på ett ramverk för riskhantering är:

- fastställa myndighetens riskpolicy
- identifiera huvudsakliga problemägare och övriga berörda personer
- klarlägg målsättningen för riskhanteringen
- definiera metoder/angreppssätt för att identifiera risker, bedöma och avrapportera dessa, olika typer av åtgärder
- definiera ansvar för riskhanteringen och avrapportering till högre ledningsnivå. Speciellt gäller detta risker som skär tvärs över enheter av myndigheter

- etablera metoder för kvalitetssäkring som säkerställer att riskhanteringen följer god sed för sådan säkring.

Det är dessutom viktigt att identifiera ”ägare” till/ansvariga för:

- att policydokument produceras
- riskhanteringsprocessen på olika nivåer – strategisk nivå, programnivå och operativ nivå
- genomförande av fattade riskhanteringsbeslut
- interdependenta risker som skär tvärs över myndigheten

Identifiera riskkällor, främst för myndighetsintern verksamhet

Risker som inte blir identifierade blir inte heller analyserade. Riskidentifieringen är alltså avgörande för riskanalysens kvalitet. Vi kommer senare att dels mer noggrant beskriva en allmän metod för riskidentifiering (se bilaga 3), dels ange ett antal checklistor för samma ändamål. Vi nöjer oss här med att ange ett antal mycket allmänna kategorier av risk hämtade från HM Treasury (2001). Jfr också med de riskkategorier som anges i figur 6.1.

Tabell 9.1 Kategorier av risk (från HM Treasury, 2001)

A Externa	
1. Infrastruktur	Samtliga försörjningssystem
2. Ändringar i ekonomiska förhållanden	Faktorer som inflation, räntenivå
3. Lagstiftning	Ökade omkostnader
4. Miljö	Ökade omkostnader
5. Politiska förhållanden	Ny regering
6. Marknaden	Konkurrensförhållanden
7. Externa yttre händelser	Brand, översvämning, extrema väderförhållanden
B Finansiella	
8. Budgetmässiga	
9. Bedrägerier, stöld	
10. Försäkringar	
11. Investeringsbeslut	Felaktiga beslut
12. Ansvarsfrågor	Möjligheten att stämma eller bli stämd
C Aktiviteter	
13. Policy	Kvalitet på policybeslut
14. Operativa risker	Rutiner och instruktioner för att fullfölja vissa uppgifter
15. Information	Kvalitet på information
16. Anseende, tilltro	
17. Transfererade risker	Felaktiga beslut i försäkringsfrågor
18. Teknologi	Användning av fel teknologi eller felaktig användning av teknologi
19. Projekt	Relaterade till projektplanering och ledningsprocedurer
20. Innovation	Felaktig exploatering
D Mänskliga resurser	
21. Personal	Förlust av nyckelpersoner
22. Hälsa och säkerhet	

De uppräknade riskkategorierna är inte oberoende och naturligtvis inte heltäckande. Det kan dessutom i praktiska fall vara tveksamt om en aktivering av riskkällan över huvud taget kan leda till en process som eskalerar till en kris.

Identifiera riskägare

Betydelsen i riskhanteringsprocessen ligger inte bara i att identifiera de problemområden dit resurser måste tillföras i riskhantering, utan också i att formellt ansvar tilldelas för identifierade risker. Innebörden är att en delegering måste ske till lämplig person på lämplig ledningsnivå och att detta dokumenteras. Organisationen bör alltså etablera en senior-struktur för ägande av identifierade risker.

Evaluera riskerna

Riskevaluering innebär att bedöma sannolikhet och påkänning på organisationen/ verksamheten från individuella risker med hänsyn tagen till interdependenser eller andra faktorer inte omedelbart förknippade med den ursprungliga riskkällan. För några typer av risker, som finansiella risker och vissa säkerhetsrisker från storskaliga teknologiska anläggningar kan numeriska värden ansättas, emedan de flesta, som exempelvis negativ publicitet, bara kan beskrivas subjektivt. Det rekommenderas att resultatet redovisas i en s.k. riskmatris , se exempelvis figur 14.2.

I figur 14.2 bedöms konsekvenserna av en svår påfrestning dock endast med avseende på hälsa, miljö och ekonomi. För vissa verksamheter är det rimligt att anta att ett antal konsekvensdimensioner får tillföras, beroende på analyserad risktyp och medföljande skade- eller påkänningstyp. De flesta myndigheter torde kunna gruppera sina riskkonsekvenser i några av följande grupper:

- Politiska (t.ex. besvärande interpellationer i riksdagen)
- Finansiella (smittspridning medför skadeståndsansvar för slaktade djur)
- Sociala (t.ex. långvariga avbrott i viktiga grundläggande försörjningssystem, ryktesspridning till följd av salmonella)
- Operativa (CSN exempelvis, service kan ej levereras)
- Juridiska (skadestånd)
- Miljö
- Rykte, anseende (förlust av allmänhetens förtroende)

Denna kategoriuppdelning av konsekvenser återkommer i figur 13.1.

Acceptabel risk

Skapandet av en riskprofil möjliggör en meningsfull diskussion om en riskkälla är acceptabel eller måste åtgärdas. Beslutet kommer vanligtvis att bero på den upplevda betydelsen av den identifierade risken och är därmed i hög grad politiskt. Är det exempelvis fråga om en begränsning i serviceutbudet och vilken exponering myndigheten kan acceptera avgörs detta, förutom av den skada och det besvär som åsamkas allmänheten, av ett antal parametrar såsom effekten på övriga delar av organisationen, värnandet om myndighetens anseende, politiska följder etc.

Respons på risk

Med riskprofilen som bakgrund kan lämplig åtgärd diskuteras. Dessa kan delas in i fyra kategorier.

Överföra: För vissa risker kan den optimala åtgärden vara en transferering. Detta kan åstadkommas genom försäkring eller genom att betala en tredje part för att ta ansvar för risken.

Tolerera: Förmågan att göra något åt riskkällan med tillgängliga resurser kan vara begränsad eller riskminskningen inte proportionell till kostnaden.

Åtgärda: Det absolut största antalet identifierade risker hör hit. Målsättningen är vanligen inte att eliminera riskkällan utan att hålla risken på en acceptabel nivå. Organisationens aktiviteter med detta syfte kallas ”internkontroll”.

Avsluta: Några risker förknippade med en specifik aktivitet är av sådan natur att de kan hanteras bara genom att aktiviteten upphör. Jfr dock exempelvis räddningstjänst, ordningsmakt.

Utvärdering av åtgärd

När ett ramverk har utvecklats och kontrollåtgärder satts in är det viktigt att åtgärdernas effektivitet utvärderas. Det rapporteringssystem och det system för egenkontroll som är nödvändigt utgör en betydelsefull del av säkerhetsledningsssytemet, se vidare avsnitt.

9.4 Exempel på strategiskt ramverk: begreppet säkerhetsledningssystem

Vi har tidigare framhållit att ledningssystem för säkerhet utgör ett viktigt element i riskhanteringsarbetet såväl för den myndighetsinterna verksamheten som ute i verksamheter som står under myndighetens tillsyn/kontroll. Detta gäller främst påfrestningar av typ 1 enligt avsnitt 8.1. Bakgrunden är givetvis att flera analyser och utredningar av tidigare inträffade svåra olyckor/påfrestningar har visat att brister i ledning av verksamheten är en av de vanligaste bidragande orsakerna. I följande citat från Kemikontoret (1997) ges en motivering till varför ledningssystem för dessa frågor är en nödvändighet för företag inom kemisk industri, en beskrivning som mycket väl kan överföras till myndighetssektorn:

> *”Att styra SHM[5]-frågor i ett företag på ett professionellt sätt bör vara lika självklart som att styra produktions-, marknads-, personal, och ekonomifrågor. Därför behövs formella system och verktyg för detta bland företagets övriga övergripande ledningssystem.*
>
> *SHM-frågorna finns ofta mer eller mindre formellt reglerade i ett företag, ofta genom spridda instruktioner eller kanske en övergripande policy. En del företag har genom långvarig tradition byggt upp en kultur inom ett eller flera av SHM-områdena.*

[5] Kemikontorets handbok avser ledningssystem för Säkerhet, Hälsa och Miljö, SHM. Principen är densamma även om ledningssystemet inte omfattar just dessa tre områden.

För flertalet företag finns ett behov av att samla och reglera SHM-frågorna på ett strukturerat sätt i ett härför särskilt utarbetat system"

Uppbyggnaden av ett ledningssystem inom olika områden kan se ut på många olika sätt och vi redovisar här endast en mycket övergripande struktur från Kemikontoret (1997).

"Ett SHM-ledningssystem bör byggas upp enligt principen:

1. *Policy*
2. *Rutiner*
3. *Instruktioner*

Policyn anger företagets övergripande syn och mål inom området. Rutinerna ger en klar uppfattning om vad som skall göras och i allmänhet också när, var, hur och av vem. I vissa fall behöver rutinerna kompletteras med detaljerade instruktioner om framför allt hur och av vem aktiviteter skall utföras. I vissa fall kan det vara lämpligt att beskriva systemet övergripande i en s k manual eller att samla rutinerna i en handbok".

Det strategiska ramverk för riskhantering som skisserats i avsnitt 9.2 och 9.3 är avsett att fungera för alla myndigheter oberoende av myndighetens storlek och sårbarhetsprofil. Vi har valt att illustrera begreppet genom att kortfattat referera innehållet i ett EU-direktiv om allvarliga olyckshändelser på kemikalieområdet. Direktivet ger dessutom exempel på utformning av ett ledningssystem för säkerhet och hur en säkerhetsrapport till myndigheterna kan struktureras. Begreppet "strategiskt ramverk" motsvaras här av termen "handlingsprogram".

9.4.1 Seveso II direktivet

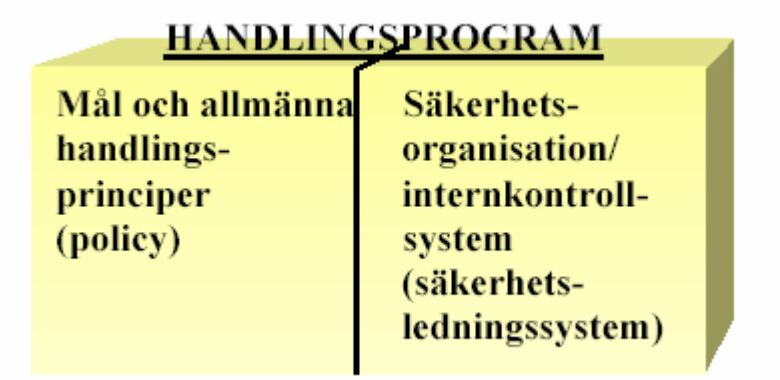
Ett exempel på genomförande av ett strategiskt ramverk enligt 9.2 och 9.3 utgörs av Seveso II direktivet. Under år 1999 infördes EU:s direktiv 96/82/EG om åtgärder för att förebygga och begränsa följderna av allvarliga olyckshändelser där farliga ämnen ingår (Seveso II direktivet) i Sverige genom att flera nya regler inom flera olika myndigheters ansvarsområde trädde i kraft.

Direktivet ses som ett genomarbetat exempel på modern lagstiftning inom området "allvarliga olyckor" och vi kommer att hämta material från de svenska myndigheternas gemensamma vägledning (Räddningsverket m.fl., 2001). Ett övergripande begrepp är termen "handlingsprogram". Likvärdiga ramverk finns exempelvis på kärnkraftsområdet, inom livsmedelsområdet osv.

<u>Handlingsprogram (strategiskt ramverk)</u>

Olika undersökningar har visat att i över 80 % av alla olyckor har brister i de övergripande ledningssystemen varit en bidragande orsak. Sedan Seveso I-direktivet trädde i kraft 1982 har nästan 400 olyckor rapporterats till EU-kommissionen. Av dessa kan över 85% helt eller delvis härledas till sådana brister. Det är mot bakgrund av detta som kravet på ett

handlingsprogram för hur allvarliga kemikalieolyckor ska förebyggas har införts i Seveso II-direktivet och i de svenska bestämmelserna. Ett sådant handlingsprogram är uppbyggt av två delar, dels mål och allmänna handlingsprinciper, dels en säkerhetsorganisation/ internkontrollsystem.

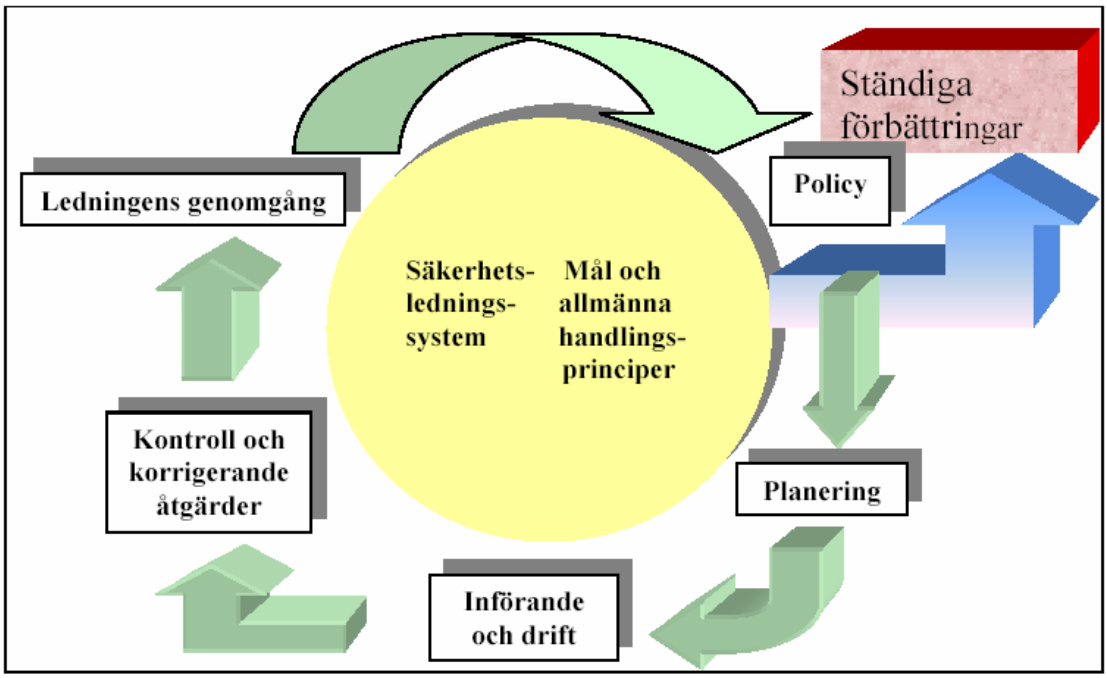


Figur 9.4 Uppbyggnad av handlingsprogram (Räddningsverket m.fl., 2001)

Målen och de allmänna handlingsprinciperna kan beskrivas som en övergripande policy som uttalar verksamhetsutövarens vilja och ambition att förebygga och hantera riskerna för allvarliga kemikalieolyckor. Dessa mål kan sedan uppnås med hjälp av säkerhets-organisationen / internkontrollsystemet (säkerhetsledningssystemet).

Hur fungerar ett handlingsprogram?

Handlingsprogrammet kan beskrivas som en ”spiral” som leder till ständiga förbättringar av verksamheten, fig.9.5. Man går in i systemet på rutan policy, d.v.s. verksamhetsutövaren sätter upp målen för en säker organisation och planerar för hur de ska uppnås. Genom säkerhetsledningssystemet genomförs planerna, följs upp och korrigeras vid behov.



Figur 9.5 Principen för ett handlingsprogram. (Räddningsverket m.fl., 2001)

Vad ska ett handlingsprogram innehålla?

Som nämns ovan innehåller ett handlingsprogram två huvuddelar:

- Mål och allmänna handlingsprinciper för hur risker för allvarliga kemikalieolyckor ska hanteras, d.v.s. en policy.
- Ett säkerhetsledningssystem för att genomföra målen.

Mål och allmänna handlingsprinciper

Mål och allmänna handlingsprinciper är ett skriftligt dokument som ger en översikt av hur en hög skyddsnivå ska säkerställas och kan vara relativt övergripande. Om verksamhetsutövaren redan har någon form av formell säkerhetspolicy, t.ex. för hälso- och miljöskyddsfrågor, kan denna policy granskas och om det är nödvändigt revideras så att den inkluderar Sevesobestämmelsernas krav på en säkerhetspolicy. I vissa fall kan det dock vara lämpligt att upprätta en säkerhetspolicy som ett tillägg till den befintliga policyn.

9.4.2 Säkerhetsledningssystem enligt Seveso II

En detaljerad beskrivning av ett ledningssystem på ett specifikt riskområde kan hämtas från ovan nämnda vägledning för Seveso II direktivet.

Säkerhetsorganisationen / internkontrollsystemet

För att säkerställa en hög säkerhetsnivå vid en verksamhet krävs att den övergripande organisationen vid verksamheten genomför ett system av strukturer, ansvarsområden och rutiner, med lämpliga resurser och tillgängliga tekniska lösningar. Ett sådant system kallas för säkerhetsorganisation/internkontrollsystem och motsvaras av begreppet säkerhets-ledningssystem. Säkerhetsledningssystemet beskriver i detalj hur man går tillväga för att uppnå de mål och följa de handlingsprinciper verksamhetsutövaren satt upp.

Systemet kan integreras i andra ledningssystem som rör t.ex. personalens hälsa, miljö eller kvalitet. Det är alltså möjligt att utöka ett befintligt ledningssystem till att omfatta kontroll av risker för allvarliga olyckor och som uppfyller kraven i lagstiftningen.

Det är sju grundläggande delar som ska ingå i ett säkerhetsledningssystem enligt Sevesobestämmelserna. Dessa punkter beskriver dock inte hela ledningssystemet bl.a. eftersom ett sådant system omfattar även andra säkerhetsaspekter än de som rör risker för allvarliga kemikalieolyckor. Verksamhetsutövarens ansvar är att säkerställa att dessa sju punkter ingår i systemet, inklusive rutiner för resultatuppföljning, utvärdering och revision. Det är en fördel om det vid såväl utvärdering som revision deltar personer som är oberoende av verksamheten. Det är dock fortfarande verksamhetsutövarens ansvar att säkerställa att dessa kontroller genomförs.

Säkerhetsledningssystemet ska minst behandla följande:

1. Organisation och personal
2. Identifiering och bedömning av riskerna för allvarliga kemikalieolyckor
3. Styrning
4. Hantering av ändringar
5. Planering inför nödsituationer
6. Resultatuppföljning
7. Utvärdering och revision

En detaljerad genomgång av de sju delarna kan hämtas från:
http://www.srv.se/funktioner/publish/mallar/2.asp?si_id=648&om_id=48 (2003-09-25)

9.4.3 Begreppet säkerhetsrapport enligt Seveso II

Syftet med att upprätta en säkerhetsrapport är framför allt att visa att riskerna för allvarliga kemikalieolyckor vid en verksamhet har klarlagts och att alla nödvändiga åtgärder har vidtagits för att förebygga sådana olyckor. Syftet är också att visa hur följderna för människor och miljön ska begränsas om en olycka trots allt skulle inträffa.

Med hjälp av informationen i säkerhetsrapporten ska också myndigheterna få tillräcklig information för att kunna upprätta planer för räddningsinsatser vid verksamheterna ifråga samt kunna besluta om lokalisering av nya aktiviteter och markanvändning runt befintliga verksamheter.

Vad ska en säkerhetsrapport innehålla?

I säkerhetsrapporten ska för den högre kravnivåns verksamheter som omfattas av Sevesolagstiftningen såväl som av AFS 1999:5 följande ingå:

- Handlingsprogrammet för hur allvarliga kemikalieolyckor ska förebyggas
- Den interna planen för räddningsinsatser
- Beskrivning av verksamhetens omgivning
- Beskrivning av anläggningar inom verksamheten
- Beskrivning av farliga ämnen
- Identifiering och analys av olycksrisker
- Förebyggande och skadebegränsande åtgärder

För den högre kravnivåns verksamheter som omfattas av Sevesolagstiftningen ska *dessutom* följande ingå i säkerhetsrapporten.

- Underlag för kommunens plan för räddningsinsatser
- Beskrivning av dominoeffekter

9.5 Sammanfattning av kapitlen 1-9

Ett försök att sammanfatta hittills diskuterat material följer.

1. Vi har valt att dela in grundorsakerna till svåra påfrestningar i tre kategorier eller typer:

   - Typ 1 kan betecknas ”organisatoriska” olyckor.
   - Typ 2 är huvudsakligen naturkatastrofer av olika slag.
   - Typ 3 utgörs av terroristangrepp och andra typer av påverkan med avsikt att skada.

2. Det till regeringskansliet inlämnade materialet bör enligt författarna omfatta:

   - Risker i myndighetsinterna aktiviteter.
   - Risker förknippade med externa verksamheter under myndighetens tillsyn och kontroll. Bedömning av effektivitet i föreskrifter och kontroll- och tillsynsprocessen avseende att förhindra uppkomst av svår påfrestning bör ingå.
   - Risker förknippade med externa aktiviteter och skeenden utanför myndighetens ansvarsområde men som kan påverka myndighetens ansvarsområde, exempelvis internationella politiska förhållanden, snabba marknadsförändringar, naturkatastrofer, utslagning av försörjningssystem och funktionssvikt hos andra myndigheter.

   De tre analysområdena kan givetvis vara beroende och överlappande. Med ”risker” avses ovan risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer.

3. Det kan enligt författarna vara ändamålsenligt att gruppera risker/riskkällor i en riskhierarki: strategiska risker, program-/projektrisker samt operativa risker/risker knutna till ett specifikt tekniskt system eller teknisk anläggning. Orsaken till indelningen är att riskidentifieringsprocessen på de tre olika nivåerna åtminstone delvis kräver olika metodik och medverkan av personal på olika nivåer. Indelningen förutsätter att risker på lägre nivå vid en viss storlek behandlas på högre nivå.

4. Som den definieras i figuren 4.1 är krishanteringens första fas, den förebyggande fasen (mitigation), grundläggande för den totala processen. I denna första fas ingår identifiering, bedömning och rangordning av riskkällor, liksom evaluering av risk- och sårbarhetsreducerande åtgärder. Formuleringen ovanför utgör den sedvanliga definitionen på ”normal” riskhantering och återfinns till stora delar i 4 § i förordning 2002:472. Implikationen är att denna krishanteringens första del, åtminstone vad gäller risker av typ 1, förutsätter en väl fungerande generell riskhanteringsprocess hos myndigheten. De risker som avses är fortfarande sådana med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. Vidare är det givetvis så att den totala krishanteringen kräver processer och rutiner utöver den ordinarie riskhanteringen. Författarna anser att § 4 implicit innebär ett krav på väl fungerande risk- och krishanteringsprocesser med tillhörande ledningssystem och rutiner för kvalitetskontroll och internkontroll. I bilaga 1 redovisas exempel på checklistor för evaluering (revision) av nämnda risk- och krishanteringsprocesser.

DEL II –
METODER ATT GENOMFÖRA RISK- OCH SÅRBARHETSANALYSER

Del II – Metoder att genomföra risk- och sårbarhetsanalyser

I denna del av dokumentet diskuteras översiktligt praktiska metoder att genomföra risk- och sårbarhetsanalyser. Vi följer den riskhierarki som tidigare skisserats med en uppdelning i strategiska risker, program-/projektrisker, risker på operativ nivå och på nivån tekniska system. Det är oklart i vilken utsträckning förordningen 2002:472 överhuvud har som mål att 3 § skall omfatta de två övre risknivåerna, d.v.s. på strategisk- och program-/projektnivå. Att skyddsvärda kapaciteter skall analyseras avseende risker på den lägsta nivån är mer eller mindre självklart. Författarna har valt att tolka 3 § som att samtliga risker som synnerligen allvarligt kan försämra förmågan till verksamhet skall beaktas i analysen, d.v.s. även risker på de två övre nivåerna.

Kapitel 10 diskuterar metodik att behandla strategiska risker generellt, kapitel 11 risker på program- och projektnivå som kan leda till en svår påfrestning. Kapitel 12-14 redovisar metoder att analysera risker inom de skyddsvärda kapaciteterna och riktar sig primärt till myndigheter berörda av förordningens 4 §. Kapitel 15 redovisar hur risk- och sårbarhetsanalysens struktur kan förändras när huvudmålet är att beakta avsiktliga hot och attacker samt ger webbadresser till ett antal manualer och vägledningar. Slutligen presenteras i kapitel 16 ett förslag på möjligt innehåll i risk- och sårbarhetsanalyserna enligt förordning 2002:472 samt ges hänvisningar till checklistor för utvärdering av den övergripande riskhanterings- och krishanteringsprocessen.

10 Identifiering och evaluering av strategiska risker

Allmänt om identifieringsprocessen

På denna nivå kan olika riskkategorier behandlas med en i stort sett generell metodik. Fokus ligger på att upptäcka och identifiera nyckelrisker avseende fullföljandet av myndighetens huvudsakliga mål och uppgifter, det vill säga bl.a. de risker och sårbarheter som avses i 3 § av förordningen 2002:472. De frågeställningar som bör tas upp avser myndighetens framtida målsättningar, hur dessa skall uppnås och, i extremfallet, hur den framtida existensen skall säkras. Risker och sårbarheter på denna nivå hotar funktionen hos viktiga delar av myndigheten. Bland riskkategorierna kan nämnas osäkerheter avseende framtida och politiska faktorer, kvaliteten på service till allmänheten, allmänhetens tilltro till myndigheten etc. Risker på lägre nivåer bör vid behov flyttas till den strategiska nivån genom att bedömas mot på förhand definierade eskaleringskriterier, som att skadeverkningar bedöms som oacceptabla, utanför överenskomna gränser, har potential att påverka strategiska målsättningar etc.

Riskidentifieringen kräver kreativitet, påhittighet och ett brett deltagande (inte minst från ledningen) för att säkerställa att nyckelrisker upptäcks. Vanligen krävs en strukturerad omvärldsanalys. Några av de externa faktorer som bör beaktas inkluderar:

Politiska: inflytande från internationella och transnationella myndigheter/ regeringar.

Ekonomiska: den nationella och internationella marknaden, globalisering.

Sociala : huvudsakliga demografiska och sociala trender, nivå på medborgarnas engagemang.

Teknologiska: Framtida utveckling på viktiga teknologiområden.

Interna faktorer inkluderar kvalitetssäkring av det totala ledningssystemet, speciellt av ledningssystemet för inre kontroll och riskhantering etc., se vidare figuren 9.1. Riskkategorierna i tabell 9.1 bör kunna tjäna som checklista och en utgångspunkt för identifieringsprocessen. Relevansen av riskkategorierna i tabellen varierar givetvis starkt mellan olika myndigheter.

Den krävda omvärldsanalysen kan ske med hjälp av en rad olika metoder, exempelvis:

- Delfi-panel (en metod att samla information och bedömningar från expertpaneler).
- Scenariometoder (metoder att framställa och granska möjliga framtida tillstånd).
- Andra typer av workshops och strukturerade gruppdiskussioner.
- Kvalitativa och kvantitativa trendanalyser.

Det existerar en rik litteratur på området, för en översikt se exempelvis ”A Futurists Toolbox” (Performance and Innovation Unit, 2001).

Evaluering av risk och sårbarhet. Inverkan av osäkerheter

Många av de identifierade riskerna kan bara med stor osäkerhet kvantifieras med avseende på konsekvens och sannolikhet. En avgörande faktor är att det ofta är inverkan av allmänhetens riskperception och utformning av myndighetens riskkommunikation som avgör den slutliga skadans storlek.

Figuren 10.1 nedan, hämtad från Strategy Unit (2002) visar hur konventionell riskbedömning för denna typ av risker måste förändras när osäkerheten ökar. Riskkällor som har potentialen att orsaka en svår påfrestning ligger i ytterområdet vad gäller osäkerheter både för sannolikhet och skada. Det kan i sammanhanget vara värt att nämna att den objektiva skadeeffekten kan vara begränsad, men ryktesspridning, inklusive spridning via media, kan ändå medföra en svårartad krissituation (jfr exempelvis SARS och BSE).

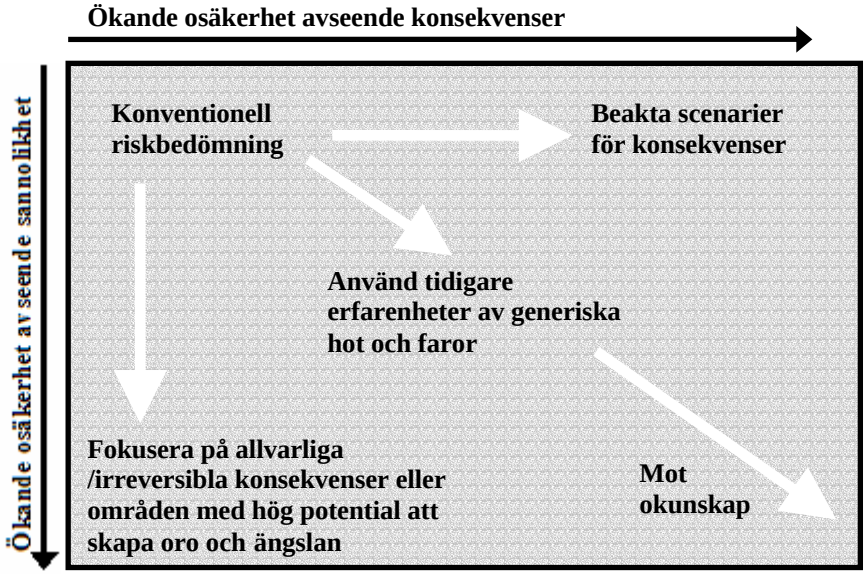


Fig. 10.1. Riskbedömning och osäkerhet, (från Strategy Unit, 2002).

För de fall osäkerheterna ter sig hanterbara kan riskmatrisen i figur 14.2 användas för att skapa en riskprofil. Eventuellt kan den kvantitativa matrisen i figur 14.2 ersättas med en kvalitativ sådan där sannolikhet och konsekvens bedöms på exempelvis en tredelad skala (låg, medium, hög).

Den vetenskapliga bakgrunden för att klassificera risktyper, riskevalueringsmetoder och riskhanteringsstrategier sammanfattas mycket kortfattat i bilaga 2.

Svår påfrestning genererad genom interdependens mellan myndigheter

Definitionen av svår påfrestning som *”ett tillstånd som kan sägas uppstå när en eller flera händelser gemensamt eskalerar och konsekvenserna av dessa händelser omfattar stora delar av samhället”* innebär att potentialen för en svår påfrestning ej kan bedömas enbart på grundval av konsekvenserna av att den egna myndighetsfunktionen allvarligt försvagas. Dels måste inverkan på andra myndigheters ansvarområden beaktas, dels måste den kombinerade effekten av att allvarliga eller extraordinära händelser samtidigt och oberoende inträffar inom annan myndighet studeras.

Worst case scenarios

Eftersom vi här är intresserade av krishanteringsaspekter anser vi att risk- och sårbarhetsanalysen bör bygga på trovärdiga ”worst case scenarios”, jämför med figur 4.2. Återigen är omvärldsanalyser av typen scenarioplanering och ”brainstorming” användbara metoder.

11 Risker på program- och projektnivå

På program- och projektnivå är ledningen ansvarig för att överföra tagna strategibeslut till (nya) metoder och vägar att arbeta för att öka myndighetens nytta och effektivitet. Typiska risker ligger inom det finansiella och organisatoriska området, omfattar säkerhets- och kvalitetsfrågor, processer för krishantering etc. På området projektrisker tillkommer dessutom personella, tekniska, kostnadsmässiga, resursmässiga och kvalitetsmässiga frågeställningar. Andra risker ligger inom området kvalitetssäkring, tillförlitlighet hos underleverantörer, beroendet av samarbete med andra myndigheter och organisationer etc. På programnivå kan en avgörande riskfaktor vara styrning av interdependens och samband mellan de projekt som tillsammans utgör programmet. På projektnivå är dessutom målsättningen att hålla oönskade projektutfall på en minimal nivå. Vikten av att projektriskhantering ingår som en naturlig del i den normala projektledningen uttrycks exempelvis i vägledningsdokument från Project Management Institute (2000).

Liksom för strategiska risker är de huvudsakliga hjälpmedlen strukturerade gruppdiskussioner av typen brainstorming, workshops, Delfi-paneler etc. Bl.a. rapporten från Strategy Unit (2002) rekommenderar en kombination av ”top-down” och ”bottom-up” metoder; exempelvis att kombinera en risköversyn utförd av seniorledning eller ett speciellt utvalt team med en bedömning genomförd av de direkt involverade och säkerställa att utfallet från den kombinerade bedömningen når myndighetens ledning.

Eventuellt kan riskidentifieringen ovan förbättras med användning av traditionella systemanalysverktyg som beslutsträd, PERT (Program Evaluation and Review Technique) och CPM (Critical Path Method), kostnad/nyttoanalys, Monte Carlo simulering, influensdiagram etc.

Som avslutning kan sägas att utveckling av praktiskt användbara checklistor för identifiering och evaluering av risker på program- och projektnivå borde vara både möjligt och till mycket stor nytta. Riskkategorierna i tabell 9.1 borde kunna utgöra en utgångspunkt för ett sådant arbete.

12 Förslag på struktur för risk- och sårbarhetsanalyser av exempelvis skyddsvärda kapaciteter

Kapitel 12 riktar sig i första hand till myndigheter som omfattas av 4 § i förordningen 2002:472. För att den process som leder till svår påfrestning skall kunna analyseras måste förloppet renodlas och struktureras. Vi har valt att göra detta enligt figur 12.1. Utgångspunkten är att vi studerar en s.k. skyddsvärd kapacitet (se Krisberedskapsmyndighetens forskningsstrategi, KBM 2003c) exempelvis:

- Elektroniska informations- och kommunikationstjänster
- Energiförsörjning
- Transport och logistik
- Vatten och annan livsnödvändig försörjning
- Skydd, undsättning och katastrofmedicin
- Betalningsförmedling och finansiella tjänster
- Tvärsektoriell ledning, information och styrelse
- Hälso- och sjukvård, särskilt medicinsk analyskapacitet

För att göra analysen hanterlig är den normala proceduren att dela upp analysobjektet i ett antal delprocesser eller delsystem. För varje delsystem definieras här en analysprocess med två huvudsteg.

Huvudsteg 1, från R1 till R2 (fig. 12.1):

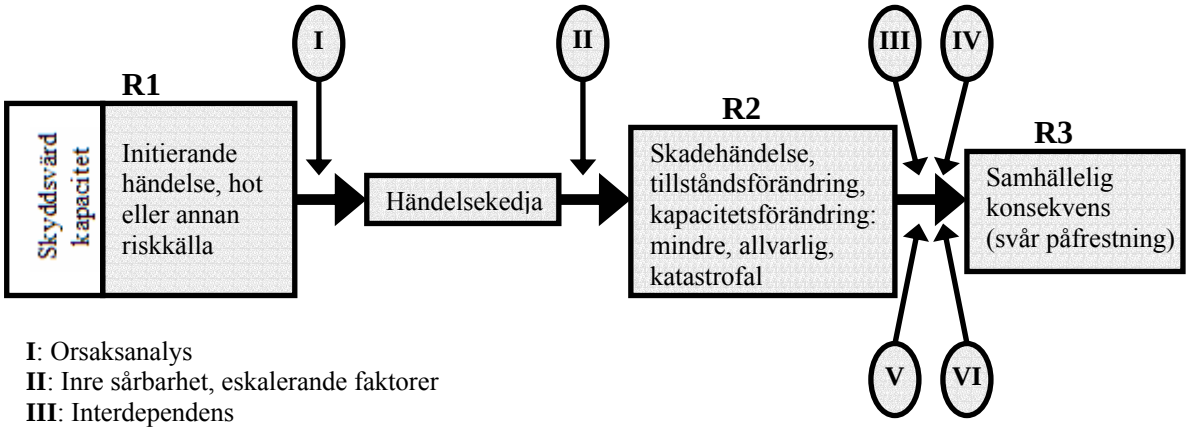
Inventering av felorsaker, initierande händelser, hot och andra riskkällor som kan starta utvecklingen mot svår påfrestning. Inventeringen omfattar felorsaker av typ A – D enligt figur 8.1 och bör bygga på existerande checklistor och erfarenheter av inträffade händelser. En orsaksanalys klargör potentialen för att starta en händelsekedja som leder till en skadehändelse eller tillståndsförändring. Systemets inre sårbarhet avgör skadehändelsens storlek. Vi har valt att definiera tre kategorier av skadehändelser/tillståndsförändringar:

- mindre
- allvarliga
- katastrofala

Vi kommer att återvända till dessa tre kategorier och diskutera hur storleken på skadehändelsen kan komma att påverka den fortsatta analysens utformning. Det bör nämnas att en grundligt genomförd analys av detta steg, som kanske främst riktar sig mot ”typ 1-risker” enligt kapitel 8, är mycket arbetskrävande och oftast faller inom den ”normala” riskhanteringen, se vidare de fem punkterna på nästa sida. Vi har valt att anlägga synsättet att de skadehändelser/tillståndsförändringar som anges i ruta R2 motsvarar de ”situationer” som anges i 3 § i förordning 2002:472.

Huvudsteg 2, från R2 till R3 (fig. 12.1):

innebär att beräkna eller bedöma den slutliga samhällskonsekvensen av skadehändelsen. Bedömningen omfattar eskaleringspotential, inverkan av krishanteringsåtgärder och av den sociala sårbarheten för påfrestningen i fråga.



I: Orsaksanalys
II: Inre sårbarhet, eskalerande faktorer
III: Interdependens
IV: Krishantering
V: Inre sårbarhet
VI: Social sårbarhet, eskalerande

Fig. 12.1. En möjlig beskrivning av en generisk process som leder till svår påfrestning.

Utvecklingen från det att händelsekedjan startar eller initieras till att en svår påfrestning inträffat är en komplex och interdependent process behäftad med stora osäkerheter. Det går därför inte att med en förenklad figur som figur12.1 invändningsfritt klargöra skeendet generellt. Figuren får ses som *en* möjlig beskrivning. Vår förhoppning är att den skall kunna utgöra startpunkten för en mer kvalificerad och detaljerad diskussion av det enskilda fallet. Därvid bör bl.a. punkterna 1-5 nedan beaktas.

1. En risk- och sårbarhetsanalys för krishantering startar förmodligen oftast i ruta 2, R2, d.v.s. med utgångspunkten att en skadehändelse har inträffat.

2. Hur processen eskalerar från R1 till R2 studeras, när det gäller krishantering, främst avseende hur systemet påverkas av externa och avsiktliga hot. Denna sårbarhetsanalys kan ha en speciell utformning som vi återkommer till i kapitel 15.

3. Skadehändelsen i R2 kan i sig själv vara av katastrofal natur; exempel utgör dammbrott och vissa typer av naturkatastrofer (extrema snöfall, etc.).

4. Skadehändelsen i R2 kan i sig vara av relativt obetydlig omfattning men kan ändå orsaka stora konsekvenser i samhället genom exempelvis ryktesspridning, allmänhetens riskperception etc. och därmed utgöra grunden för en svår påfrestning. Exempel utgörs av SARS-epidemin, där skadehändelsen i sig var av relativt begränsad omfattning men påverkan på samhället, exempelvis flygindustrin, var enorm.

5. För studier av processer som går från vänster till höger blir metodiken vad som kan betecknas som ”händelseträdsbaserad”, d.v.s. studier av olika tänkbara scenarier från R2 för att bedöma slutliga konsekvenser i R3. Studeras händelser från höger till

vänster kan ofta någon form av felträdsanalys användas, d.v.s. man utgår från skadehändelsen i R2 eller R3 och försöker finna den kedja av bakomliggande händelser och orsaker som kan leda fram till skadehändelser. Om skadehändelsen i R2 är av katastrofal natur borde sådan analys vara relevant för uppfyllelse av förordning 2002:472. En metodik att göra detta med förslag på hur säkerhet, hälsa och miljö kan beskrivas i ekonomiska termer visas i kapitel 14.

Sammanfattningsvis gäller att figur 12.1 ger möjlighet att definiera ett antal procedurer för risk- och sårbarhetsanalys. Ur dessa har vi valt att närmare diskutera två analysfall:

- Att skadehändelsen R2 är av ”mindre” eller ”allvarlig” art och att vi studerar den potentiella eskaleringen från R2 till R3 (kapitel 13).

- Att skadehändelsen R2 i sig innebär en svår påfrestning (är av katastrofal natur) och att vi använder ett mer direkt angreppssätt att identifiera och karakterisera denna (kapitel 14).

Avseende de två ovan angivna analysfallen har vi i kapitel 13 och 14 försökt att beskriva ett par angreppssätt som kan vara användbara för ett antal myndigheter, kanske främst för sådana med begränsad erfarenhet av att producera risk- och sårbarhetsanalyser. Självklart är inte avsikten att på något sätt föreslå att de myndigheter som kanske sedan lång tid har en väl inarbetad och fungerande metodik ersätter eller ändrar denna. Det skall också nämnas att det inte är praktiskt genomförbart och inte heller nödvändigt att föreskriva på metodnivå hur risk- och sårbarhetsanalyserna bör genomföras. Lämpliga metoder varierar beroende på vilken typ av verksamhet som är aktuell. Många myndigheter använder som nämnts ovan redan idag metoder som är väl anpassade till respektive myndighets verksamhetsområde.

De övergripande angreppssätt som skisseras i kapitel 13 och 14 får ses som förslag för analysarbetet under kommande år, samt som underlag för diskussion och vidareutveckling. Givetvis är det av vikt att ta tillvara de praktiska erfarenheter som erhålls vid myndigheternas analysarbete under de kommande åren för att styra den vidare metodutvecklingen.

13 Att analysera steget från allvarlig händelse till svår påfrestning

Startpunkten är figur 12.1 och eskalering av ”skadehändelse/tillståndsförändring” till ”svår påfrestning” (R2 till R3). Vi utgår återigen från att den primära konsekvensen av skadehändelsen/tillståndsförändringen, exempelvis i form av direkt påverkade människor, påverkan på miljö etc. kan vara av ”mindre”, ”allvarlig” eller ”katastrofal” omfattning enligt den kategorisering som gavs i kapitel 12. Vi vill här återigen framhålla att de ”skadehändelser” eller ”tillståndförändringar” vi talar om anses korrespondera väl med de ”situationer” som avses i 3 § i förordning 2002:472.

13.1 Allmän analysstruktur

I figur 13.1 nedan skisseras den huvudsakliga strukturen i ett möjligt angreppssätt att genomföra analysen. För att exemplifiera strukturen utgår vi från att en ”allvarlig” händelse har inträffat[6], d.v.s. där den primära konsekvensen av skadehändelsen/tillståndsförändringen är av ”allvarlig” karaktär. Ett krav på ”allvarlig händelse” skulle kunna vara att den kräver aktivering av det totala samverkansområdets krishantering.

Figur 13.1 ger en översiktsbild av processen. X_1, … , X_n är de riskfaktorer/orsaker/hot som kan ge upphov till en ”allvarlig händelse”.

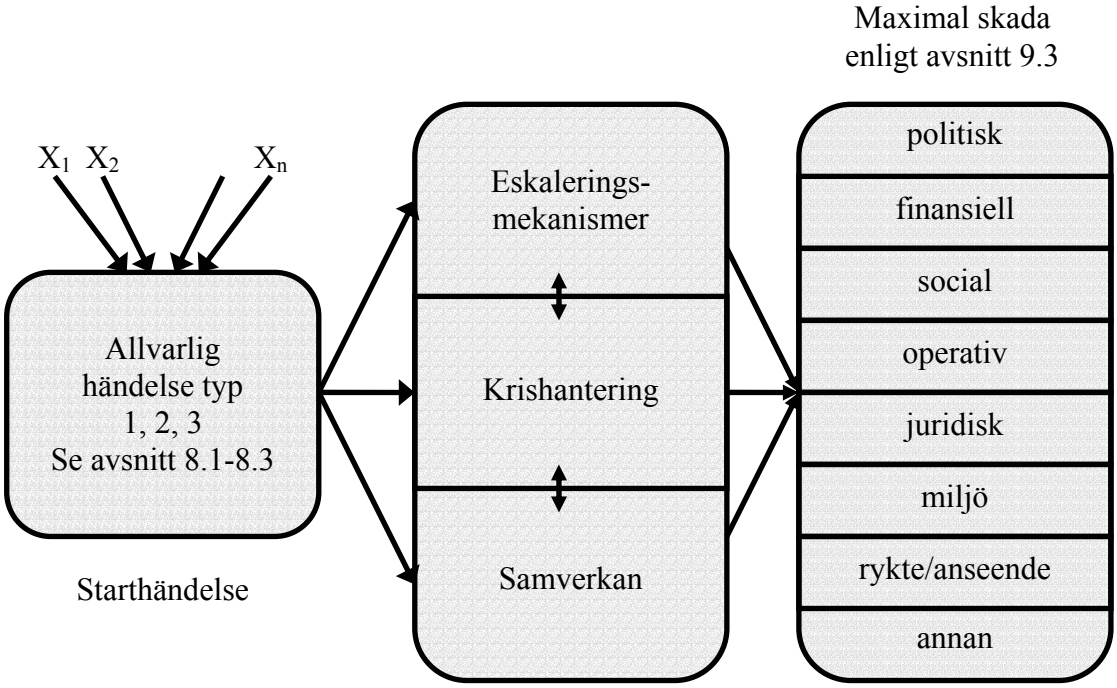


Fig. 13.1 Översiktsbild. Allmän analysstruktur, angreppssätt 1

[6] Strukturen blir i huvudsak densamma i det fall själva skadehändelsen/tillståndsförändringen är av mindre allvarlig karaktär, med bl.a. den skillnaden att större uppmärksamhet ägnas åt potentiella eskaleringsmekanismer relaterade till allmänhetens och inblandade aktörers uppfattning om situationen etc. Angreppssättet är även tillämpbart i de fall skadehändelsen/tillståndsförändringen i sig själv är av katastrofal art, även om fokus då förmodligen kommer att ligga mer på den operativa krishanteringens effektivitet.

Angreppssättet bygger vidare på att man för identifierade ”allvarliga händelser” studerar vilka förutsättningar som krävs för att dessa skall kunna leda till en svår påfrestning på samhället. Konsekvenskategorierna har tidigare angivits i avsnitt 9.3.

Angreppssättet innebär alltså två steg,

- Steg 1: Definiera och beskriv ett antal ”allvarliga händelser”. Lista de faktorer eller omständigheter $X_1, \ldots, X_n$ som bidrar till den allvarliga händelsens inträffande.
- Steg 2: Definiera de omständigheter och händelsekedjor eller scenarier som leder till att en svår påfrestning inträffar, exempelvis potentiella eskaleringsmekanismer kopplade dels till det ”fysiska” skeendet, dels till hur detta skeende uppfattas av allmänheten och inblandade aktörer. Beakta speciellt krishanteringssystemets påverkan, särskilt då samverkan med andra myndigheter lokalt, regionalt och nationellt.

13.2 Steg 1: Identifiering av allvarliga händelser

Problemet är alltså att som utgångspunkt för vidare analys definiera ett antal ”allvarliga händelser” som kan inträffa:

- genom att en eller flera skyddsbarriärer brutits genom efter att en initierande händelse inträffat eller en riskfaktor utlösts
- genom att en extrem yttre händelse inträffat
- genom att terroraktion, sabotage, eller intrång av annan typ genomförts.

Dessa utgångspunkter skall sedan användas för att studera eventuell vidare eskalering och krishanteringens effektivitet; d.v.s. för att genomföra sårbarhetsanalys avseende den yttre sårbarhet som diskuteras i avsnitt 5.3. Speciellt viktig faktor är samverkan över myndighetsgränserna.

En ”allvarlig händelse” kan ofta hänföras till någon av riskkategorierna i tabell 9.1. En del av risktyperna i tabellen avser strategiska risker, andra kategorier kan länkas till en allvarlig händelse på program- eller projektnivå. Erfarenheten visar att det är mer sällan som felhandling på operatörsnivå är en grundläggande orsak till en ”allvarlig händelse”.

Med tanke på det breda spektrum av såväl verksamheter över det totala myndighetsområdet som riskkategorier är det inte möjligt att specificera direkt vilken metod som bör användas vid identifieringen av tänkbara allvarliga händelser utan här ges endast några generella exempel.

På den strategiska nivån är huvudmålet att balansera risk (inklusive sannolikheten att en svår påfrestning inträffar) och möjlighet; d.v.s. man behöver metoder att identifiera framtidsrisker. Bland de metoder som är möjliga kan nämnas kvantitativ trendanalys, kvalitativ trendanalys, Delphipaneler (expertpanel), scenariometoder, workshops, fokusgrupper etc. (se t.ex. Performance and Innovation Unit, 2001).

På lägre nivåer finns ett stort antal analysmetoder för riskidentifiering i allmänna tekniska och sociotekniska system inkluderande samverkan människa – teknik – organisation. Publikationen ”Handbok för riskanalys” (Räddningsverket, 2003) redovisar ett 20-tal sådana

metoder, exempelvis felträdsanalys, grovanalys och HAZOP. En generell struktur för en riskidentifieringsprocess beskrivs summariskt i bilaga 3.

Steg 1 bör emellertid resultera i en lista med ”allvarliga händelser” och ett angivande av de faktorer/orsaker/hot som generellt är förutsättningar för att respektive händelse skall inträffa. Drivs analysen något vidare bör det vara möjligt att strukturerat diskutera den samverkan mellan $X_1, \ldots, X_n$ som resulterar i den allvarliga händelsen.

13.3 Steg 2: Från allvarlig händelse till svår påfrestning: scenariobeskrivning via händelseträd

Baserat på utfallet av riskidentifieringen ovan, d.v.s. ett antal ”allvarliga händelser”, blir sedan det naturliga steget att genomföra någon form av beskrivning av konsekvenserna givet att en ”allvarlig händelse” realiserats.

För att en allvarlig händelse skall utvecklas till en svår påfrestning behövs ofta att en serie omständigheter skall inträffa. Dessa kan med fördel illustreras med hjälp av s.k. händelseträd. Vi ser det som lämpligt att man med utgångspunkt i en given identifierad allvarlig händelse genomför en händelseträdsanalys som visar bedömningarna av sannolikheter för att en händelsekedja skall utvecklas till de valda scenarierna. För genomförande av analysen hänvisas till Räddningsverket (2003).

Inom de olika aktuella verksamheterna finns ofta traditioner att göra riskanalyser enligt vissa metoder. Sannolikt kan dessa även fortsättningsvis användas som huvudsakliga verktyg att genomföra de risk- och sårbarhetsanalyser som krävs enligt förordningen. De måste emellertid i en del fall utvidgas och/eller omformas för att få fram den i sammanhanget relevanta informationen.

14 Identifiering av svår påfrestning med grovanalytisk metod (preliminary hazard analysis)

I kapitel 13 utgick vi från att en ”skadehändelse” eller ”tillståndsförändring” hade inträffat och målsättningen var att studera under vilka förutsättningar (eskaleringsmekanismer, den operativa krishanteringens effektivitet etc.) den situation som då uppstod kan komma att utvecklas till en svår påfrestning på samhället, d.v.s. en form av ”bottom-up”-angreppssätt. Här kommer vi i stället att ha som utgångspunkt att en svår påfrestning inträffat och anlägga ett mer ”top-down”-baserat synsätt.

Figuren 14.1 nedan illustrerar det fall då man utgår från att en fullskalig kris, d.v.s. svår påfrestning, inträffat och man är intresserad av att direkt bestämma de faktorer/händelser/hot som orsakat krisen. Angreppssättet innebär alltså en direkt identifiering av de faktorer/omständigheter som leder till en svår påfrestning i samhället, speciellt brister eller svagheter i krishanteringssystemet, inklusive samverkan mellan myndigheter.

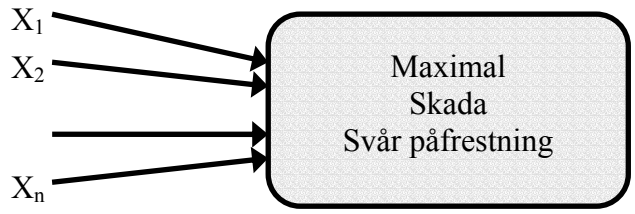


Fig. 14.1 Angreppssätt 2, ”direkt” angreppssätt

Grovanalytisk metod

Målet är alltså att direkt identifiera och beskriva ett antal högprioriterade svåra påfrestningar med hänsyn till inverkande faktorer X_i och konsekvensens storlek.

Identifieringen av svåra påfrestningar föreslås ske via en process där varje avdelning, enhet, projekt, program etc. genomför sin egen evaluering, oftast under ledning av personal från RHF/KHF, se avsnitt 6.2. Att låta extern personal som exempelvis expertkonsulter medverka kan effektivisera processen. Som bas för arbetet används tillgängligt material om tidigare inträffade incidenter och händelser, genomförda riskanalyser, intervjuer med personal etc. För ett antal tekniska områden (olika typer av transport, processanläggningar, kärnkraft etc.) finns extensiva databaser med data och beskrivningar om felaktiga komponenter och olycksförlopp.

En svår påfrestning kan ofta hänföras till någon av riskkategorierna i avsnittet om riskidentifiering i avsnitt 9.3.

Som nämnts tidigare är det inte möjligt att föreskriva generellt användbara metoder för risk- och sårbarhetsanalyserna. Det finns emellertid behov av en enhetlig form för rapportering av resultaten av analyserna för att dessa skall kunna jämföras och för att ge underlag för prioriteringar och åtgärder. Därför rekommenderar vi att som basmetod för detta angreppssätt använda det som brukar kallas grovanalys. Grovanalysen fokuserar större skadehändelser eller störningar med tillhörande scenarier. Vid arbete med framtagande av scenarier i en grovanalys arbetar man oftast med en grupp erfarna personer från olika discipliner. Metoden kan därför

sägas vara expertbaserad. Den innehåller normalt också alla sorters aspekter, såväl tekniska som alla ”mjuka” frågor.

Grovanalys, eller preliminär riskanalys, beskrivs i Räddningsverket (2003) enligt följande. ”En översiktlig s.k. grovanalys eller preliminär riskanalys görs tidigt i ett projekts planeringsstadium, eller vid en översiktlig inledande granskning av en existerande verksamhet. Metoden går ut på att granska verksamheten i stora drag, identifiera riskkällor och möjliga skadehändelser. Checklistor används ofta för att underlätta en systematisk genomgång av typiska riskfaktorer. En grov uppskattning av sannolikheter och konsekvenser bör göras för att underlätta en systematisk värdering av riskerna. Förslag till möjliga åtgärder för att eliminera eller reducera riskerna noteras och eventuella krav på fördjupade analyser ställs.”

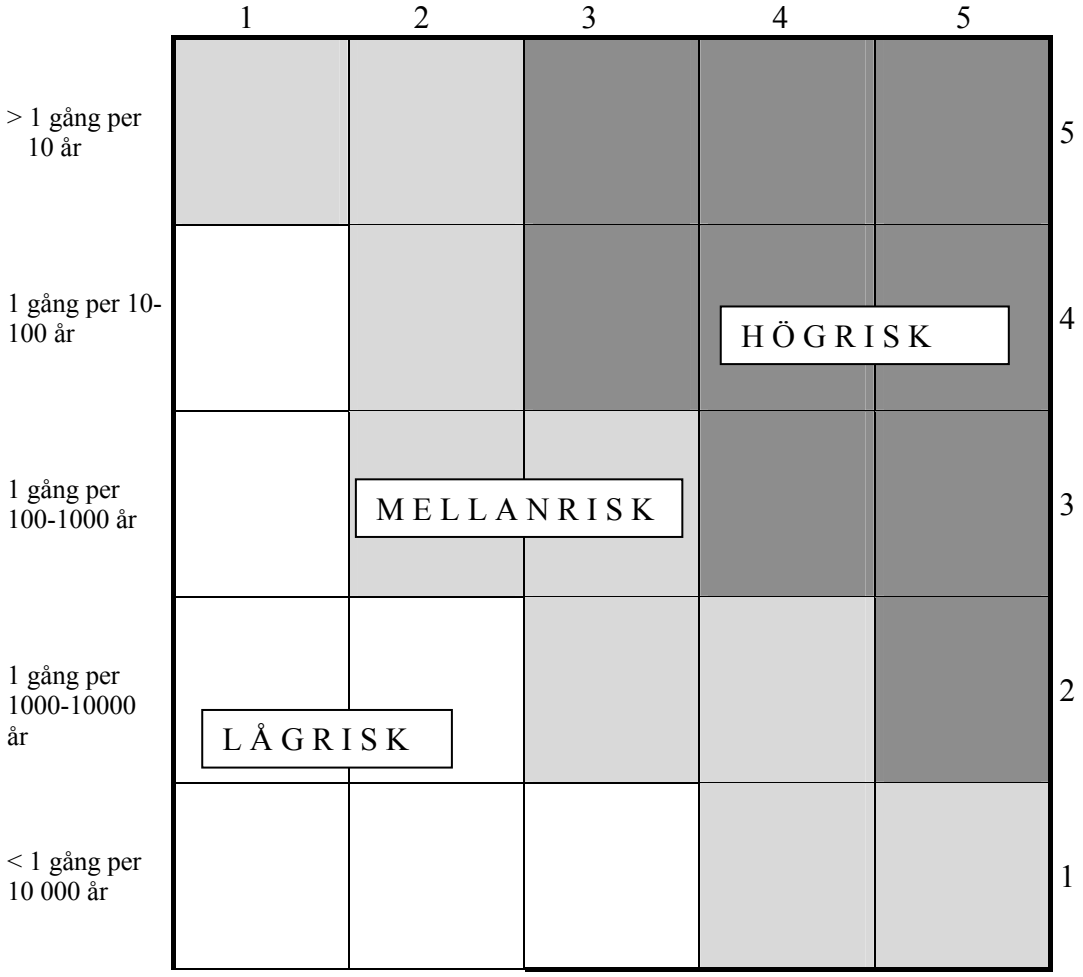
Checklistor, riskmatris

Grovanalysmetoden är alltså ofta baserad på checklistor. Allmänna checklistor för analys av kommunal verksamhet från säkerhetssynpunkt redovisas i skriften ”Verksamhetsanalys och säkerhetssamordning” (Kommunförbundet, 2001). Naturligtvis existerar det en mängd checklistor för ändamålet inom olika områden. Inom företagssektorn finns publikationer med ett stort antal checklistor, ett exempel utgörs av skriften ”Säkra företagets flöden” (ÖCB, 1999). Avseende checklistor eller manualer för specifika tekniska system hänvisar vi här endast till ”Basnivå för IT-säkerhet (BITS)” (KBM 2003d), samt verktyget ”SBA-Check” (Dataföreningen, 2002) avsett att användas vid analys av en organisations informationssäkerhet.

Grovanalysen ger i sin klassiska utformning svar på både omfattningen av konsekvenserna av en skadehändelse och sannolikheten/frekvensen av motsvarande händelse. Konsekvenserna uttrycks oftast i påverkan på liv och hälsa, på miljö och på kostnader för att ersätta egendom och för produktionsbortfall. Givetvis gäller för många av de situationer och händelser som analyseras att det finns andra typer av konsekvenser, såväl kvantifierbara som ej direkt kvantifierbara, som måste tas i beaktande. Exempelvis skulle konsekvenserna av ett långvarigt elavbrott vara svåra att beskriva i endast de termer som nämns ovan. En utmaning ligger alltså i att identifiera de olika typer av konsekvenser som kan tänkas uppkomma.

En relaterad utmaning är kopplad till möjligheten att göra jämförelser mellan olika analyser och olika typer av konsekvenser, d.v.s. att finna någon form av gemensam mätskala för olika typer av konsekvenser. *Ett* synsätt, dock inte ovedersägligt, innebär att man som ett mått på konsekvensen bör ta fram den totala kostnaden för en analyserad skadehändelse eller störning sedd i ett samhällsperspektiv. Tanken är alltså att exempelvis avbrott i viktiga samhällsfunktioner och dylikt kan omvandlas till ekonomisk förlust. I bedömningen av ekonomisk konsekvens skall då alla relevanta kostnader ingå, exempelvis direkta egendomsskador och produktionsförlust, förlust av framtida försäljning, diverse immateriella kostnader etc. Även om risk- och sårbarhetsanalysen inte primärt ger resultat i form av förlust av pengar eller liv/hälsa eller miljö, finns alltid följdverkningar någonstans som kan uppskattas i ekonomiska termer. Denna mer eller mindre grova uppskattning skulle kunna göras för att överföra resultatet av en primär risk- och sårbarhetsanalys till något som kan användas i jämförelser med resultaten från andra verksamheter.
För att konkretisera resonemanget finns i figur 14.2 ett exempel på klassificering av riskerna med en 5-gradig skala för sannolikheten/frekvensen för händelsen och ävenledes en 5-gradig skala för konsekvensen mätt i:

- Ekonomi
- Liv och hälsa
- Miljö



Ekonomi	<10 milj kr	10-100 milj kr	100-1 000 milj kr	1 000-10 000 milj kr	>10 000 milj kr
Hälsa	Enstaka dödsfall och/eller flera svårt skadade	Flera dödsfall och/eller många svårt skadade	10 – 100 döda och/eller hundratals svårt skadade	100 – 1000 dödsfall och/eller tusentals svårt skadade	Mer än 1000 dödsfall och/eller tiotusentals svårt skadade
Miljö	Mindre skadeeffekter; varaktighet < 1år. Liten till stor utbredning. Oftast enkel sanering.	Större skadeeffekter; varaktighet 1-10 år. Liten utbredning (< 10 km^2). Oftast svår eller omöjlig sanering.	Allvarliga skadeeffekter; varaktighet 1-10 år. Stor utbredning (hundratals km^2). Oftast svår eller omöjlig sanering.	Mycket allvarliga skadeeffekter; varaktighet 10-100 år. Stor utbredning (hundratals km^2 eller mer). Oftast svår eller omöjlig sanering.	Mycket allvarliga, permanenta skador. Mycket stor utbredning (landsdelar). Omöjlig sanering.

Fig. 14.2 Riskmatris för ekonomi, hälsa och miljö

15 Externa hot och sårbarhetsanalys av kritiska försörjningssystem och infrastrukturer

15.1 Allmänt

För en allmän bakgrundsbeskrivning hänvisas till avsnittet 3.2.4 *”Samhällviktig infrastruktur och grundläggande resurser”* i skriften *”Samhällets Krisberedskap 2005 Planeringsinriktning”* (KBM, 2003b).

Att alla myndigheter har att redovisa sårbarhet, hot och risker avseende samhällsviktig infrastruktur inom respektive ansvarsområde i analysen enligt 3 § i förordningen 2002:472 är självklart. Dessutom gäller enligt 4 § i förordningen att samverkansansvariga myndigheter ska *”beakta säkerhetskraven för de tekniska system som är nödvändiga för att de skall kunna utföra sitt arbete”*.

15.2 Struktur på analysen: tillgängliga manualer

Internationellt sett har ett stort antal ansvariga myndigheter utfärdat standards, manualer, vägledningar etc. avseende hur sårbarhetsanalys av infrastruktursystem exponerade för främst externa hot skall utföras. Generellt ingår ett antal delsteg i processen:

1. Identifiera kritiska resurser (KR) i form av komponenter, noder, etc.
2. Identifiera vad som skyddar och stöder KR.
3. Identifiera och kategorisera hoten.
4. Identifiera och analysera sårbarheter.
5. Bedöm risk och bestäm prioritering för skydd av KR.
6. Identifiera åtgärder, kostnader och trade-offs.

De manualer och vägledningar som nämns ovan överstiger i volym ofta 100 sidor; d.v.s. sårbarhetsanalysen är utpräglat detaljerad och specifik. I några fall finns nationella arbeten på området. Vi har valt att ge web-adresser till ett antal manualer främst från USA.

Exempel är:

<u>IT-sektorn</u>

- ”*Basnivå för IT-säkerhet (BITS)*”, KBM (2003d) http://www.krisberedskapsmyndigheten.se/verksamhet/information/bas_it-sakerhet_bits_rekomm2003-2.pdf (2004-01-12).

- ”*IT och sårbarhet – Kritiska beroendeförhållanden i den nationella IT-infrastrukturen*”, KBM (2003e) http://www.krisberedskapsmyndigheten.se/verksamhet/information/it_sarbarhet_2003.pdf (2004-01-12).

Elförsörjningens infrastruktur

- ”*Vulnerability Assessment Methodology – Electric Power Infrastructure*” US DoE (Department of Energy) (2002a).
  http://www.esisac.com/publicdocs/assessment_methods/VA.pdf (2004-01-12).

  Innehåller bl.a. ett stort antal arbetsblad/checklistor för att kontrollera interdependensen mellan olika infrastrukturer.

Infrastruktur för energiförsörjning

- ”*Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments”* US DoE (2001).
  http://www.appanet.org/operations/checklist.pdf (2004-01-12).

- *”Energy Infrastructure Risk Management Checklists for Small and Medium Sized Facilities”* US DoE (2002b).
  http://www.esisac.com/publicdocs/assessment_methods/Risk_Management_Checklist_Small_Facilities.pdf (2004-01-12).

Vattenförsörjning

- ”*Instructions to Assist Community Water System in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002”* US EPA (Environmental Protection Agency) (2003).
  http://www.epa.gov/safewater/security/util-inst.pdf (2004-01-12).

Processanläggningar

- ”*Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*”, Centre for Chemical Process Safety of the American Institute of Chemical Engineers, New York, (2002).
  http://www.aiche.org/ccpssecurity/ (2004-01-12).

15.3 Interdependens, speciellt el – tele - it

I en inledande fas förutsätts att denna typ av sårbarhet får behandlas via sönderdelning (dekomposition), samt användning av standards, normer, vägledningar och åtföljande checklistor. Avseende angreppssättet med sönderdelning är dock en nyckelfråga hur ett komplext interdependent system kan uppdelas i subsystem som sedan kan analyseras var för sig utan att dominerande riskkällor negligeras. Avvägningen mellan den vinst i hanterbarhet man kan göra genom att en uppdelning av systemet och den information som går förlorad måste göras med eftertanke.

16 Förslag till möjligt innehåll i risk- och sårbarhetsanalyserna enligt förordning 2002:472

I detta kapitel skisseras ett möjligt upplägg avseende innehållet i de risk- och sårbarhetsanalyser som skall inlämnas till regeringskansliet enligt förordning 2002:472. Förslaget är författarnas och bör ses som ett möjligt komplement till den struktur som ges i vägledningen (KBM, 2003a) och som en möjlig utgångspunkt inför kommande års analyser. Givetvis är det även så att det kan skilja sig (väsentligt) mellan olika myndigheter avseende såväl vad som bör inkluderas i redovisningen som dess detaljeringsgrad.

16.1 Möjligt innehåll i risk- och sårbarhetsanalyserna

Vi har valt att redovisa vad vi anser vore lämpligt att inkludera i risk- och sårbarhetsanalyserna under två huvudrubriker: utvärdering av myndighetens funktion och roll, samt upprättande av register över analyserade händelser och situationer (svåra påfrestningar).

16.1.1 A: Utvärdering av myndighetens funktion och roll

Med utgångspunkt i vad som anförts i kapitel 6-9 anser vi att det kan vara lämpligt att i analysen inkludera punkt 1-5 nedan:

1. Bedömning av föreskrifters effektivitet.
2. Bedömning av tillsynens effektivitet.
3. Bedömning av existerande ramverk för riskhantering (se avsnitt 9.1). Intern verksamhet, extern verksamhet.
4. Bedömning av säkerhetsledningssystemets effektivitet (se checklista i bilaga 1). Intern verksamhet, extern verksamhet.
5. Redovisning av uppbyggnad av myndighetens krishanteringsfunktion, samt utvärdering av krishanteringsplan (se checklista i bilaga 1). Intern verksamhet, extern verksamhet.

Vad som är tillämpligt med avseende på punkt 1 – 5 ovan varierar naturligtvis från myndighet till myndighet. Andra frågor som kan vara aktuella att belysa, där så bedöms relevant, omfattar

- Vem som ansvarar för regelsystem (rutiner, instruktioner) på operativ nivå.
- Vem som kontrollerar efterlevnad på operativ nivå.
- Vem som utfärdar föreskrifter för säkerhetsledningssystem och ledningssystem för krishantering.
- Vem som utvärderar effektiviteten av ledningssystemen.
- Vem som etablerar nivå för acceptabel risk.
- Vem som kontrollerar att denna nivå uppfylls,

samt en genomgång av de problem och dilemman som svaren på frågeställningarna ovan eventuellt skapar.

16.1.2 B: Upprättande av register över analyserade händelser och situationer (svåra påfrestningar)

I KBM:s vägledning (KBM, 2003a) ges en struktur för rapporteringen av analysarbetet. Där efterfrågas bl.a. en översikt av analyserade händelser och situationer att användas som en bas för att vidare kunna värdera aktuell förmåga, förbättringsåtgärder, samverkansbehov etc. Vi anser att det vore värdefullt om det vore möjligt att rangordna de analyserade händelserna och situationerna, samt upprätta ett register som sedan årligen kan uppdateras. Nedanstående punkter kan ingå:

1. Identifiering av de 5-10 allvarligaste krisscenarierna enligt kapitel 12-14 eller med annan lämplig metodik. Detta avser såväl intern verksamhet som verksamheter under tillsyn.
2. Upprättande av åtgärdsförslag.
3. Kvalitetssäkring.

De tre typer av riskfaktorer/hot/händelser som nämnts i avsnitt 8.1-8.3 bör behandlas, i de fall dessa är relevanta.

16.2 Checklista för den övergripande riskhanterings- och krishanteringsprocessen

I detta avsnitt nämns endast helt kort ett par exempel på checklistor som kan användas som stöd för att utvärdera riskhanterings- respektive krishanteringsprocessen vid myndigheten. Checklistorna, som är hämtade från Office of Government Commerce (2001), samt CCMD (2003), återfinns på originalspråket i bilaga 1.

DEL III –

SAMMANSTÄLLNING AV INTERVJUSTUDIEN

17 Intervjustudien

Intervjustudiens syfte och upplägg

Det huvudsakliga syftet med intervjustudien var att föra inledande samtal kring, samt genomföra en översiktlig genomgång av metodik, metoder och procedurer använda av samverkansansvariga myndigheter i deras risk- och krishanteringsarbete. Detta för att söka och lyfta fram generella och fungerande metoder och angreppssätt som skulle kunna ligga till grund för en vägledning för vad som bör ingå i en risk- och sårbarhetsanalys enligt 3 § i förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap. Här bör påpekas att vi inom ramen för projektet låtit begreppet risk- och sårbarhetsanalys omfatta hela processen för att uppnå en säker krishantering.

Förfrågan gick ut till nio centrala myndigheter som valdes ut i samråd med KBM, se nedan. Intervjuerna genomfördes hos respektive myndighet och tog ungefär en halvdag i anspråk. Som regel deltog två representanter från LUCRAM och en till fyra representanter för myndigheten, oftast från någon form av beredskapsfunktion. Vid samtalstillfällena användes ett intervjuunderlag som stöd, vilket följer krishanteringsprocessens olika delar som de definierats i avsnitt 4.2. Efter en första sammanställning av resultatet från intervjustudien gjordes ett utskick med kompletterande frågeställningar till samtliga myndigheter. Svar och kommentarer till detta utskick har inarbetats i detta kapitel.

Urval av myndigheter för intervju

Urvalet av centrala myndigheter att ingå i studien gjordes i samråd med KBM, där avsikten var att identifiera myndigheter med mångårig erfarenhet från risk- och krishanteringsarbete, men även att tillse att de 6 samverkansområdena fanns representerade. De nio myndigheterna redovisas i tabell 17.1 nedan.

Tabell 17.1 Myndigheter som ingick i intervjustudien.

Myndighet	Samverkansområde där myndigheten ingår
Banverket	Transporter
Livsmedelsverket	Teknisk infrastruktur, Spridning av farliga ämnen[7]
Post- och telestyrelsen	Teknisk infrastruktur
Räddningsverket	Spridning av farliga ämnen, Skydd, undsättning och vård
Luftfartsverket	Transporter, Skydd, undsättning och vård
Statens veterinärmedicinska anstalt	Spridning av farliga ämnen
Socialstyrelsen	Spridning av farliga ämnen, Skydd, undsättning och vård
Riksförsäkringsverket	Ekonomisk säkerhet
Svenska Kraftnät	Teknisk infrastruktur

Presentation av resultaten från studien

I detta kapitel redovisas de huvudsakliga resultaten från den genomförda intervjustudien. Presentationen inleds med övergripande slutsatser från intervjustudien, följt av relativt kortfattade redogörelser från respektive intervjutillfälle. Strukturen på presentationen av intervjuerna följer, i den mån det är tillämpligt, de olika faserna i krishanteringsprocessen, förebyggande, förberedande, akut avhjälpande, samt återuppbyggande.

[7] Det fullständiga namnet är ”Spridning av allvarliga smittämnen, giftiga kemikalier och radioaktiva ämnen”.

Övergripande slutsatser från intervjustudien

Vikten av att ta tillvara de erfarenheter och den kompetens som finns i systemet

Flertalet myndigheter har redan i dagsläget väl utvecklade och fungerande system för såväl risk- och sårbarhetsanalys (i generell mening, inte nödvändigtvis riktat mot förordningen 2002:472) som riskhantering. Det är av yttersta vikt att den samlade kompetens som finns i systemet tas tillvara på ett strukturerat sätt. Flera myndigheter lyfte fram arbetet inom samverkansområdena som ett bra exempel på sådan aktivitet. Uppmaningar till Krisberedskapsmyndigheten att även verka för att seminarier, workshops etc. anordnas i detta syfte framfördes.

Risk- och sårbarhetsanalyser enligt förordningen 2002:472 – en ”statusrapportering”

Ett flertal av de intervjuade myndigheterna ser på risk- och sårbarhetsanalysen som en ”statusrapport” av den löpande verksamheten. Det är alltså inte en företeelse som sker isolerat en gång om året. Arbetet med risk- och krishantering är en fortlöpande process vid samtliga myndigheter som ingått i studien.

Vikten av att arbetet med risk- och sårbarhetsanalyser sker inom organisationen

Flera myndigheter poängterar att det är viktigt att arbetet med risk- och sårbarhetsanalyser sker ”internt” så att organisationen över tid kan dra lärdom från detta arbete. Att lägga ut uppdraget på externa konsulter vore ett misstag. Att genomföra risk- och sårbarhetsanalyser under ett antal år kommer att ge en kompetenshöjande verkan inom myndigheten.

Möjligheten att producera fungerande centrala anvisningar för RSA

Avseende risk- och sårbarhetsanalyserna enligt förordning 2002:472 generellt anser flertalet myndigheter att det är omöjligt att ta fram en gemensam metod för hela myndighetssektorn. Bakgrunden till detta är givetvis den diversifierade verksamhet som bedrivs vid de olika myndigheterna.

Förslag framkom dock att Krisberedskapsmyndigheten borde sträva efter att verka för att de olika processer, metoder och modeller som används inom olika samhällssektorer på något sätt levererar jämförbara resultat, jämförbar upplösning och detaljeringsgrad, vilket skulle tjäna som en form av kvalitetssäkring. En övergripande struktur på resultatredovisning i samband med risk- och sårbarhetsanalyserna enligt förordning 2002:472 behövs. Ett forum där metoder för risk- och sårbarhetsanalys kunde diskuteras efterlystes.

Flera myndigheter nämnde också att det mycket väl kan finnas andra, mindre myndigheter som inte har samma erfarenhet av risk- och sårbarhetsarbete, vilka kanske vore betjänta av ett mer direkt metodstöd.

Risk- och sårbarhetsanalysernas offentlighet

Alla intervjuade myndigheter påpekade det problematiska i att sekretessfrågan inte är löst avseende risk- och sårbarhetsanalyserna enligt förordning 2002:472. Dels utgör det en risk i sig att i offentliga dokument beskriva de sårbarheter som finns i systemet, dels (eller som en följd av detta) innebär det att man inte kommer att få fram en rättvisande bild.

Det nödvändiga i att ”skynda långsamt”

Flera myndigheter framhöll att det är av vikt att man låter framtagandet av ett övergripande system för risk- och sårbarhetsanalyser ske över tid och i samverkan mellan de olika myndigheterna, där den mångåriga erfarenhet som finns ute i samhället kan tas tillvara. Det framhölls att det var viktigt att ha realistiska krav på risk- och sårbarhetsanalyserna de första åren.

Specificering av ”vad man vill ha”

Ett flertal myndigheter efterlyser en specificering av vilken typ av information som KBM är intresserad av för att kunna göra den övergripande sammanställningen och analysen. Återigen påpekar man att det inte handlar om en ”metod” utan snarare om strukturen på redovisningen, upplösning mm.

Risk- och sårbarhetsanalyser som ett verktyg för resursfördelning

Vissa myndigheter anser att risk- och sårbarhetsanalyserna kommer att bli en av hörnpelarna i myndighetens anslagsäskande, vilket betonar vikten av ett sammanhängande system för dessa analyser (om än ej gemensam analysmetod).

Scenarier som utgångspunkt för RSA?

Somliga myndigheter ansåg att det vore önskvärt att få en fingervisning om dels vilken typ av information som skall levereras i analyserna, men kanske framför allt en fingervisning om vilken typ av händelser man skall inrikta sig på. Man efterlyser gemensamma scenarier som samtliga myndigheter kan ha som utgångspunkt för sitt analysarbete, detta för att möjliggöra att analyserna blir jämförbara.

Scenariobeskrivningar, antingen de genereras av KBM eller den egna myndigheten, ansågs av flera vara en viktig utgångspunkt för övningsverksamhet. Framtida risk- och sårbarhetsanalyser bedömdes kunna verka ett naturligt sätt att generera ”nya” scenarier för övningar.

Ledningens engagemang / ledningssystem

Flera myndigheter betonade vikten av ledningens engagemang i risk- och sårbarhetsfrågor för att arbetet med dessa skall kunna bli effektivt, samt vikten av att få in dessa frågor i det övergripande ledningssystemet.

Det ömsesidiga beroendet mellan olika infrastruktursystem och samhällssektorer

Ett område som lyftes fram var beroendet mellan olika infrastruktursystem och verksamheter, något som måste utredas noggrannare. Ett exempel är RFV:s beroende av att betalningsväsendet fungerar. Ett annat kan illustreras av LFV:s påpekande att man har relativt god överblick avseende hur flygtransportsystemet påverkas vid olika typer av påfrestningar, men att man har sämre insikt i vad det i sin tur får för återverkningar ute i övriga samhället.

Ett relaterat potentiellt problem är risker/hot/faror som innefattar skeenden som berör flera myndigheters ansvarsområden, där ansvarsförhållanden kan vara svåra att tydliggöra. De intervjuade myndigheterna ser generellt sett mycket positivt på arbetet i samverkansområdena, där förutsättningar finns för att kunna behandla denna typ av frågeställningar.

Flera myndigheter var av uppfattningen att de standards, normer och checklistor som idag finns tillgängliga för risk- och sårbarhetsanalyser inte fungerar tillfredsställande vad gäller analys av inderdependens mellan olika infrastruktursystem.

Metoder för att identifiera allvarliga händelser och eskaleringspotential

Metoder för att identifiera ”vardagsrisker” finns hos de flesta av de intervjuade myndigheterna. Strukturerade metoder för att hitta de händelsekedjor som kan leda till extraordinära händelser och svåra påfrestningar saknas dock i allmänhet.

I de kommande avsnitten ges kortfattade redogörelser för intervjuerna med respektive myndighet.

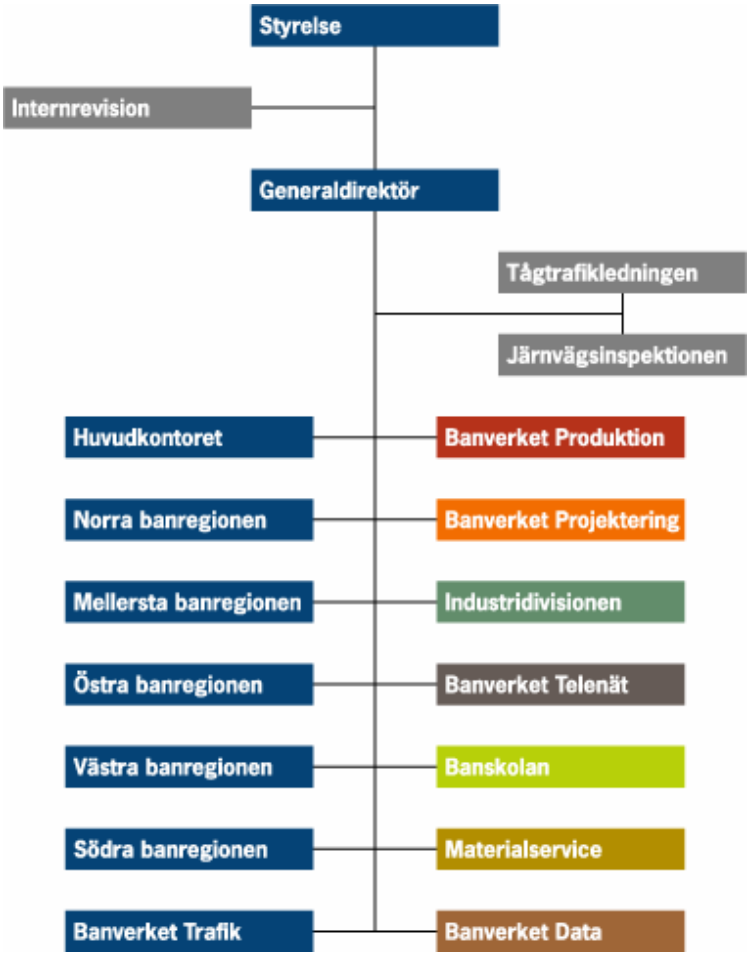
Banverket

Allmänt

Intervjun genomfördes den 13 maj 2003 i Banverkets lokaler i Borlänge. Närvarande var Sten-Sture Sjöö och Mikael Isaksson från Banverket, samt Marcus Abrahamsson och Sven Erik Magnusson från LUCRAM.

Kortfattad beskrivning av verksamheten

Banverket är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, för hela järnvägstransportsystemet (SFS 1998:1392). Som sådan skall Banverket verka för att de transportpolitiska målen uppnås. Verket ansvarar bl.a. för drift och förvaltning av statens spåranläggningar. Banverkets organisationsstruktur redovisas i figur 17.2.



Figur 17.2 Banverkets organisationsstruktur

Banverket ingår i samverkansområde ”Transporter”. Banverket lämnade inte in någon risk- och sårbarhetsanalys enligt 3 § i SFS 2002:472 i första omgången, med hänvisning till att man under de senaste åren startat ett omfattande arbete på risk- och krishanteringsområdet, se nedan. Om ett par år räknar man med att ha ett väl underbyggt underlag för analysen enligt SFS 2002:472.

Förebyggande arbete

Sedan år 2000 pågår ett risk- och krishanteringsprojekt vid Banverket. Projektet kom till bl.a. som en följd av kraven i förordning (1995:1300) om statliga myndigheters riskhantering. En annan initierande faktor var de incidenter som inträffat på senare år, där bl.a. ett antal gasolvagnar spårat ur på bangården i Borlänge, dock utan läckage som följd. Projektet har två delar, en riskhanteringsdel och en krishanteringsdel. Syftet med riskhanteringsdelen av projektet är dels att inventera det arbete som gjorts inom banverket, dels att initiera ett mer ingående riskhanteringsarbete.

En huvuddel i riskhanteringsprojektet har varit och är att genomföra en verksamhetsanalys, med utgångspunkt i den metod som tagits fram av Kammarkollegiet, i syfte att identifiera risker och sårbarheter i Banverkets totala verksamhet. Metoden är baserad på checklistor och finns beskriven i Kommunförbundets skrift Verksamhetsanalys och säkerhetssamordning (Kommunförbundet, 2001). Checklistor mm har dock modifierats för att bättre avspegla Banverkets verksamhet. I detta arbete har stöd erhållits från Kammarkollegiet.

Verksamhetsanalysen har genomförts på samtliga åtta resultatenheter och fem regioner. Själva genomförandet tog ca en dag i anspråk per resultatenhet/region (förberedande möten hade dock hållits), och ca 8-18 personer från respektive enhet, såväl chefer som personer ute i verksamheten, deltog vid analysen. Checklistorna består såväl av diagnostiska frågor, där öppna diskussioner hölls, och ja/nej frågor. Dokumentationen från övningarna har lämnats till chefen för respektive enhet för verifiering. Slutsatser angående risker och sårbarheter har sedan dragits från det verifierade resultatet. Angreppssättet med verksamhetsanalys upplevs som mycket bra för att identifiera svaga punkter och riskkällor.

Användning av risk- och sårbarhetsanalyser inom Banverkets verksamhetsområde

Utöver verksamhetsanalysen som nämnts ovan genomförs ett stort antal riskanalyser i Banverkets ordinarie verksamhet. De flesta av dessa är dock av karaktären ”ingenjörsanalyser”, hållfasthetsberäkningar etc., alternativt rena projektriskanalyser, d.v.s. fokuserar på specifika projekts framgångsfaktorer och risker. Banverket ställer även krav på de entreprenörer som anlitas vid järnvägsbygge att genomföra riskanalyser.

Riskhantering premieras i internförsäkringssystemet

Som ett led i att stärka incitamentet för ett effektivt riskhanteringsarbete inom organisationen har i man försäkringsvillkoren för det interna försäkringssystemet lagt in olika nivåer av premiereduceringar kopplade till genomförande av riskanalys, framtagande av åtgärds-/handlingsplaner etc.

Incidentrapportering och uppföljning

Banverket har olika system för rapportering av incidenter och störningar i systemet. Inom produktionsenheten drivs ett ärendehanteringssystem, SYNERGI, med möjlighet för uppföljning av händelser etc. Systemet används av flera aktörer inom järnvägssektorn, även internationellt, och underlättar kommunikationen och möjligheterna att lära av inträffade händelser.

Förberedande arbete

I krishanteringsdelen av ovan nämnda risk- och krishanteringsprojekt har övningar genomförts med ledningsgrupper på olika platser i landet. Övningarna har genomförts på flera organisatoriska nivåer, samt i samverkan med övriga aktörer inom järnvägssektorn. Övningarna har i hög utsträckning varit scenariobaserade. Exempel på scenario kan vara ett tåg på bana som stannat i norrland med elbortfall under vintertid med 30 minusgrader, där problem kring evakuering, logistik, information etc. måste hanteras. Man ser på kommande risk- och sårbarhetsanalyser som ett naturligt sätt att generera ”nya” scenarier för liknande övningar.

Akut avhjälpande arbete

Organisatoriskt finns det inom banverket en beredskaps- och säkerhetsskyddsenhet. Dess uppbyggnad och funktion diskuterades dock inte under samtalet. Banverket har även ett driftvärn, beredskapsstyrkor. I ett akut läge handlar det för Banverkets del mycket om informationshantering. Planer för informationsspridning finns. En informationsstab finns centralt i Borlänge, dessutom finns det informatörer ute på varje resultatenhet och region.

Avvecklande/återuppbyggande arbete

Denna fas diskuterades inte explicit under samtalet.

Generella kommentarer

Nödvändigheten att kunna sekretesspröva de risk- och sårbarhetsanalyser som genomförs inom verkets ansvarsområde, inklusive de som skall levereras enligt förordningen 2002:472, betonades.

Stor tveksamhet uttrycktes inför en generell metod för risk- och sårbarhetsanalys över hela myndighetssektorn. Man gjorde bedömningen att även verksamheten inom banverket är så differentierad att det vore svårt att hitta en övergripande metod som är användbar i alla lägen.

Den verksamhetsanalys som använts vid banverket bedöms fungera väl för identifiering av ”vardagliga” risker och sårbarheter.

Vikten av ledningens engagemang i risk- och sårbarhetsfrågor, samt vikten av att få in dessa frågor i det övergripande ledningssystemet, betonades. Aktiviteter är på gång inom banverket för att få detta till stånd.

Banverket önskar förtydligande av vilka förväntningar man (KBM) har på myndigheternas risk- och sårbarhetsanalyser enligt förordning 2002:472. Hur skall de utformas för att KBM skall kunna ha nytta av dem?

Arbetet i samverkansområdena upplevs som mycket positivt.

Livsmedelsverket

Allmänt

Intervjun genomfördes den 14 maj 2003 i Livsmedelsverkets lokaler i Uppsala. Närvarande var Christina Nordensten och Per Olldén från Livsmedelsverket, samt Marcus Abrahamsson och Sven Erik Magnusson från LUCRAM.

Kortfattad beskrivning av verksamheten

I förordning (2001:1259) med instruktion för Livsmedelsverket beskrivs verksamhetens målsättning: ”Livsmedelsverket skall som central förvaltningsmyndighet för livsmedelsfrågor i konsumenternas intresse arbeta aktivt för säkra livsmedel av hög kvalitet, redlighet i livsmedelshanteringen och bra matvanor.” Vidare framgår att det är Livsmedelsverkets uppgift att utarbeta regler på livsmedelområdet, samt att Livsmedelsverket har ett överordnat ansvar för att leda och samordna kontrollen av livsmedel, inklusive dricksvatten, i landet.

I figur 17.3 visas Livsmedelsverkets organisation.

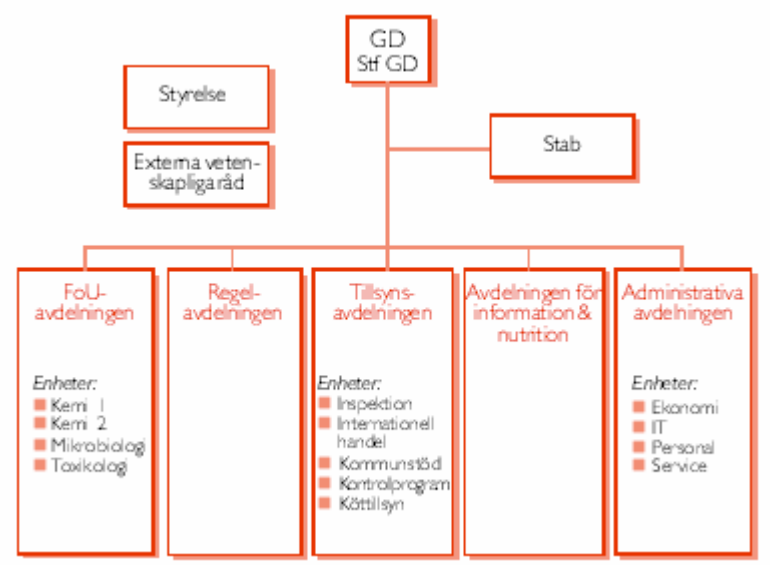


Fig. 17.3 Livsmedelsverkets organisation

Livsmedelsverket ingår i samverkansområde ”Teknisk infrastruktur” samt ”Spridning av allvarliga smittämnen, giftiga kemikalier och radioaktiva ämnen”. Samtalet kom i stor utsträckning att handla om dricksvattenförsörjningen.

Förebyggande

Allmänt:

En gränsdragning görs mellan den ”ordinarie” verksamheten i verket och beredskapsverksamheten. Kärnverksamheten inom verket handlar i hög utsträckning om riskhantering och riskvärdering, exempelvis FoU-verksamhet, regelgivning och tillsyn. Men ”den sidan” fokuserar mest på ”vardagliga olyckor och händelser”. Beredskapssidan arbetar med utgångspunkt i de typscenarier som togs fram i ”Krönmarks utredning” (SOU 1995:19). Myndigheten har tagit fram en krishandbok med scenarier och handlingsplaner som bygger på dessa.

Dricksvattenområdet:

Livsmedelsverket gör ansträngningar för att få ansvaret för beredskapstillsynen på dricksvattenområdet, vilket givetvis skulle leda till bättre styrningsmöjligheter avseende verksamheten ute i kommunerna där produktion och distribution av dricksvattnet sker. I dagsläget har man små formella möjligheter att styra kommunerna i detta arbete och som en följd av detta har man valt att i hög utsträckning arbeta med information och utbildning mot kommuner och länsstyrelser. Exempel utgör projektet ”starthjälpen” som riktas mot kommunerna, samt konferenser om säkerhet och beredskap inom dricksvattenområdet som riktas mot kommuner och länsstyrelser.

Starthjälpen, som är den största satsningen, syftar bl.a. till att ge riskinsikt, inspirera till förebyggande åtgärder (skydd, reservanordningar etc.) och öka beredskapen och krishanteringsförmågan (svåra påfrestningar och höjd beredskap). Starthjälpen börjar med en genomgång av både kända hot och nya sådana, och en genomgång av ett antal checklistor som kan utgöra en god grund för en riskanalys på dricksvattenområdet. Viktiga punkter är förmedling av konkreta råd när det gäller skydd mot sabotage och terrorism, en summering av läget i kommunen och förslag till handlingsplan för det fortsatta arbetet samt slutligen utdelning av dokumentation och litteraturlista. Bland annat innehåller slutdiskussioinen råd till kommunen om ett minimum av handlingsplaner för att hantera fyra ”basscenarier” avseende vattenkvalitet och vattenförsörjning och som kan anses vara delmoment till förmågan vid svåra påfrestningar och höjd beredskap. Dessa fyra basscenarios är stort elavbrott, en stor läcka, en vattenburen smitta, samt en förorening av olja eller kemikalier i en vattentäkt, alternativt i ledningsnätet. Dagen skall ge en gemensam kunskapsplattform över förvaltningsgränserna för kommunens fortsatta arbete, för att öka säkerheten generellt från vattentäkt till konsument, för att höja kommunens beredskap och krishanteringsförmåga och för att kunna hantera svåra påfrestningar och höjd beredskap.

Livsmedelsverket har publicerat ett stort antal skrifter, handböcker mm med checklistor etc. som stöd för arbetet ute i kommunerna, exempelvis ”Förebyggande åtgärder och hantering av akuta incidenter på dricksvattenområdet” (2000), ”Handledning för ökad IT-säkerhet inom dricksvattenområdet” (2003) och ”Riskhandbok för dricksvattenförsörjning” (1997).

Även drickvattenområdet innefattas av Livsmedelsverkets ordinarie tillsyn, med normerande inspektioner och årligen sammanställning av den lokala tillsynsverksamheten.

Förberedande

Myndigheten deltar med jämna mellanrum i seminariedagar och scenariobaserade övningar som genomförs i samverkan med andra aktörer. Denna typ av verksamhet bedöms som mycket viktig inom myndigheten.

Akut avhjälpande

Vid en akut händelse inom Livsmedelsverkets ansvarsområde får verket rollen som expertmyndighet. Det finns en katastrofgrupp som står till länsstyrelsernas och kommunernas förfogande om något inträffar.

Avvecklande/återuppbyggande

Vikten av att informationshanteringen under allvarliga händelser fungerar betonas, dels inom och mellan myndigheter, men även gentemot allmänheten.

Generella kommentarer

Man anser att det är omöjligt att skapa generella riktlinjer för risk- och sårbarhetsanalys över hela samhället (åtminstone på metodnivå), detta mot bakgrund av de vitt skilda verksamheter och ansvarsområden det rör sig om.

Kopplingen till den lokala och regionala nivån är mycket viktig för Livsmedelsverket. Vikten av att det system för risk- och sårbarhetsanalyser som skall tas fram även inkluderar dessa geografiska/administrativa nivåer betonas. Myndigheten bedömer att man kommer att vara beroende av rapportering från kommuner via länsstyrelser för att kunna ge en övergripande bild av risk- och sårbarhetsläget inom myndighetens ansvarsområde.

Man framhåller även att många myndigheter på central nivå redan har system och processer för risk- och sårbarhetsanalysarbete, vilka man förmodligen kommer att vilja nyttja och utveckla vidare i framtiden. Det är mycket viktigt att eventuella kommande riktlinjer och vägledningar för risk- och sårbarhetsanalys möjliggör detta.

Det nödvändiga i att ”skynda långsamt” lyfts fram. Målet måste vara att över tid bygga upp en fungerande process för risk- och sårbarhetsanalysarbetet.

Post- och telestyrelsen

Allmänt

Intervjun genomfördes den 19 maj 2003 i Post- och telestyrelsens (PTS) lokaler i Stockholm. Närvarande var Jonny Nilsson från PTS, samt Marcus Abrahamsson och Sven Erik Magnusson från LUCRAM.

Kortfattad beskrivning av verksamheten

Av förordning (1997:401) med instruktion för Post- och telestyrelsen 1 § framgår att ”Post- och telestyrelsen är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, inom post-, tele- och radioområdena”. PTS organisationsstruktur framgår av figur 17.4.

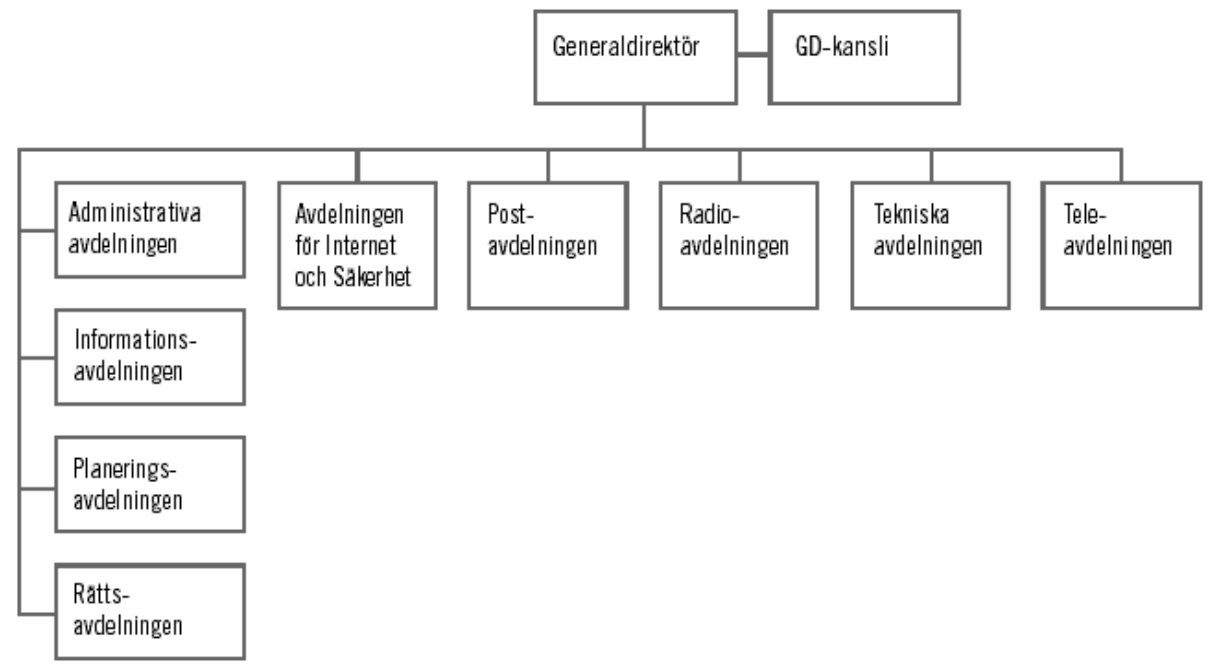


Fig. 17.4 Post- och telestyrelsens organisationsstruktur. (Från Årsredovisning 2002).

Post- och telestyrelsen ingår i samverkansområde ”Teknisk infrastruktur”. PTS delar ut de tillstånd som krävs för aktörerna på telemarknaden.

Förebyggande arbete

PTS jobbar i huvudsak förebyggande. PTS huvudsakliga strategi för att minska sårbarheten i telekommunikationerna är investeringar i infrastrukturen (andras anläggningar), ca 200 milj/år. Dessa medel har hittills använts i huvudsak för centrala delar av telesystemet. Satsningar har även gjorts avseende reservel och redundans i stamnätet. Allt detta sker i nära samarbete med operatörerna (som äger och förvaltar infrastrukturen).

Mest aktuellt just nu är bredbandsutbyggnaden. Ett stort problem är att det saknas anvisningar och regler för hur detta skall byggas och underhållas. PTS arbetar exempelvis mot stadsnätsföreningen, länsstyrelser, kommuner och operatörer för att se till att robusthetsfrågorna kommer med vid byggnationen.

Projekt pågår vid PTS som går ut på att viktigare samhällsanvändare skall kunna få prioritet i telenätet för att komma fram i telefonköer etc.

Ett stort antal utredningar har genomförts inom PTS ansvarsområde. Det gäller fysiska angrepp, elförsörjning, IT-hot mm.

En metod för riskidentifiering som används är s.k. ”red teams”, d.v.s. hackers som anlitas för att försöka ta sig in i operatörernas system. Dessa rapporterar sedan de svagheter de identifierat så att operatörerna kan rätta till dem. En annan metod som används är en form av ”what if” analys. PTS och andra aktörer inom området deltar även i övningar, där nya risker och sårbarheter identifieras. Största delen av risk- och sårbarhetsanalysarbetet inom området sker ute hos operatörerna.

Myndigheten satsar även i hög utsträckning på studier av inträffade händelser för att skapa ett lärande av dessa.

De stora operatörerna har tillståndsplikt, d.v.s. de måste vidta de åtgärder som PTS vill att de skall göra mot en kostnadsbaserad ersättning. Den huvudskaliga strategin är att ”bygga bort” sårbarheter, där finansieringen är den stora frågan. Man talar om ”stat och näringsliv i partnerskap”.

Förberedande arbete

PTS, operatörerna och andra aktörer deltar i olika övningar. Genomförandet av sådana övningar diskuterades inte i detalj.

Akut avhjälpande arbete

PTS har inga eller få uppgifter i en akut kris. Det ligger hos operatörerna. Planer för informationsflöde i en akut situation finns inte vid PTS. En webbaserad portal som utarbetas vid KBM nämns, där myndigheter skall kunna lägga in information. Detta för att man skall kunna gå ut med samma information vid kriser.

Avvecklande/återuppbyggande arbete

Denna fas diskuterades inte explicit under samtalet.

Generella kommentarer

Myndigheten poängterar att det är viktigt att arbetet med risk- och sårbarhetsanalyser sker ”internt” så att organisationen över tid kan bygga upp kompetens och skapa ett lärande på området. Att lägga ut uppdraget på externa konsulter vore ett misstag. Man anser att arbetet med risk- och sårbarhetsanalyser under ett antal år kommer att vara en viktig del i kompetensutvecklingen hos myndigheten inom detta område.

Vikten av att lära av varandra inom ”totalförsvarsfamiljen” poängteras. Arbetet i samverkansgrupperna upplevs som mycket positivt.

Myndigheten framhåller även att samarbetet med operatörerna är A och O. Som exempel nämns att man från PTS sida arbetar för att de stora operatörerna skall bygga sina nät oberoende av varandra, d.v.s. inte lägga ledningar i samma ledningsgrav eller dra dem via samma bro etc.

Angående roller i krishanteringssystemet: Vikten av att tydliggöra olika myndigheters roller vid en akut kris betonas. Inom PTS ansvarsområde kommer en eventuell kris att inträffa ute i verksamheterna, hos operatörerna och de lokala kraftbolagen etc. Samverkan mellan den lokala, regionala och centrala myndighetsnivån samt verksamhetsutövarna måste förtydligas.

PTS anser att Krisberedskapsmyndighetens kanske viktigaste roll kommer att vara att understödja arbetet inom och framför allt mellan samverkansområdena. Man framhåller att flertalet myndigheter redan har väl fungerande system för risk- och sårbarhetsanalyser och riskhantering. Det är av stor vikt att uppbyggnaden av ett system för risk- och sårbarhetsanalyser enligt förordningen 2002:472 baseras på detta förhållande.

Sekretessfrågan kring risk- och sårbarhetsanalyserna måste lösas. Man framhåller att man inom PTS område är beroende av samarbetet med operatörerna och att man utan möjlighet att hemligstämpla material inte kan förvänta sig att få in allt material man skulle önska. Man nämner att KBM har påbörjat ett arbete med att förändra sekretesslagen och konstaterar att så länge den frågan inte är löst kommer ”risk- och sårbarhetsanalyserna vara urvattnade”.

Räddningsverket

Allmänt

Intervjun genomfördes den 20 maj 2003 vid Räddningsverkets (SRV) skola i Skövde. Närvarande var Rainar All, Bo Gellerbring, Jan Schyllander och Mattias Strömgren från SRV, samt Marcus Abrahamsson från LUCRAM.

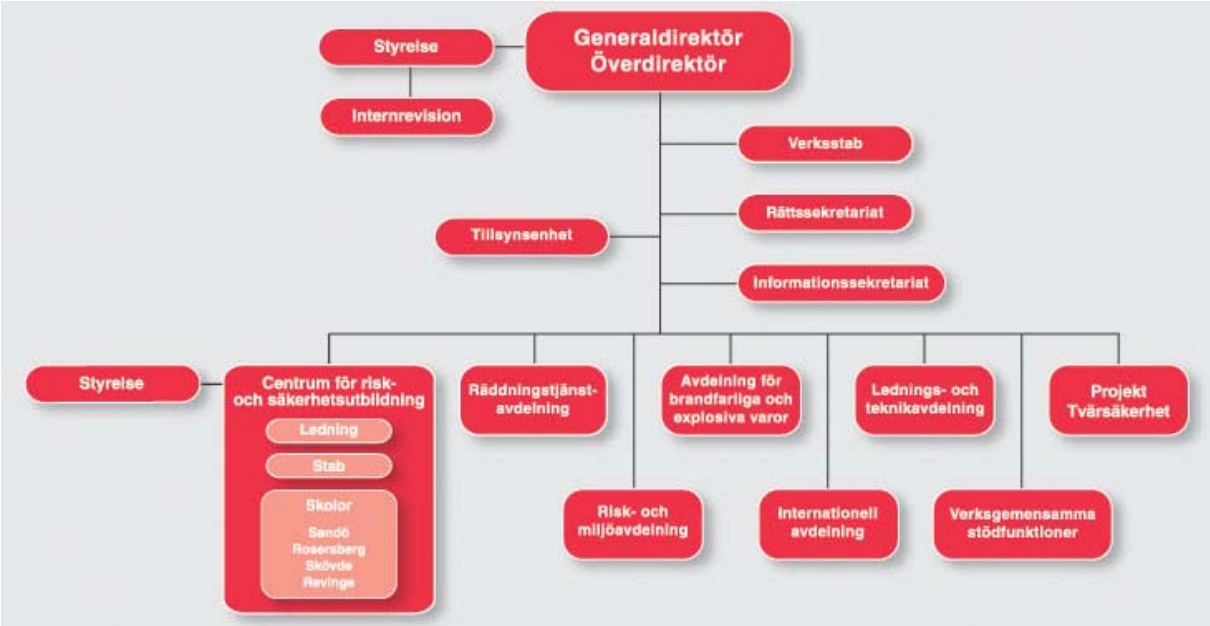
Kortfattad beskrivning av verksamheten

Enligt Förordning (1988:1040), med instruktion för Statens räddningsverk, är SRV central förvaltningsmyndighet för följande frågor, i den mån det inte är en uppgift för någon annan myndighet:

1. räddningstjänst, olycks- och skadeförebyggande åtgärder samt sanering efter utsläpp av radioaktiva ämnen från en kärnteknisk anläggning och
2. landtransporter av farligt gods.

SRV är också central förvaltningsmyndighet för frågor om brandfarliga och explosiva varor samt frågor om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor.

SRV:s organisatoriska struktur visas i figur 17.5:



Figur 17.5 SRV:s organisation

SRV ingår i samverkansområdena Spridning av farliga ämnen samt Skydd, undsättning och vård. Samtliga deltagande i intervjun från SRV:s sida har störst anknytning till verksamhet inom samverkansområdet Spridning av farliga ämnen, varför frågor rörande Skydd, undsättning och vård ej diskuterades i någon större utsträckning.

Förebyggande

Riskanalyser har länge haft en framskjuten roll inom SRV:s ansvarsområde och myndigheten har bl.a. producerat ett antal vägledningsdokument om kommunal riskanalys, en handbok för riskanalys (Räddningsverket, 2003) etc. Myndigheten har ofta en granskande funktion och kommer i kontakt med riskanalyser exempelvis i sin roll remissinstans vid planärenden, samt från verksamheter som prövas i miljödomstolar (verksamheter som omfattas av Seveso II-direktivet).

Det för detta sammanhang problematiska faktum att de flesta riskanalyser som produceras inom SRV:s ansvarsområde inte fokuserar på vad som skulle kunna generera extrema händelser eller svåra påfrestningar lyftes fram. Som exempel nämndes de riskanalyser som genomförts inför Citytunnelprojektet i Malmö. I de riskanalyser som genomförts i detta projekt har grundförutsättningarna varit att elförsörjning, säkerhetssystem etc. fungerar, vilket givetvis leder till att man inte hittar de potentiellt riktigt allvarliga händelserna.

Man har från myndighetens sida inte tagit ställning till några kvantitativa nationella kriterier för vad som kan gälla för acceptabel risk, exempelvis vid processanläggningar. Principen man anammat är att beslut om risker och riskhantering skall ske lokalt, där man även kan göra en bedömning av nyttan. SRV:s strategi i de fall bedömningen görs att en risk är oacceptabel, exempelvis vid remissärenden, är att lyfta frågan till den berörda myndigheten eller verksamhetsutövaren, i andra hand till regeringen. SRV har sällan mandat att ingripa rent formellt. Myndigheten upplever att man får gehör för sina synpunkter hos andra myndigheter och hos regeringen.

En möjlig begränsning som uppmärksammats är att det ofta är starkt fokus på dödsfall i de riskanalyser som SRV kommer i kontakt med. Skador på människor, miljö, och andra störningar i samhället beskrivs mer sällan.

Osäkerheter beskrivs mycket sällan i de riskanalyser som SRV kommer i kontakt med. Ofta förekommer det att författarna till en riskanalys anger att man använt ett konservativt synsätt utan att verifiera detta eller ange hur konservativ man varit. Ett relaterat problem är att riskanalyser ibland används som ”dimensioneringsverktyg” i planeringssammanhang, vilket kan leda till problem relaterade till osäkerheter. ”Riskanalyserna bör fungera som underlag för beslut, besluten skall ej fattas i riskanalysen”.

Vikten av att kartlägga interdependensen mellan olika infrastruktursystem framhölls.

Förberedande

Den förberedande verksamheten sker på lokal och regional myndighetsnivå, samt verksamheternas egen planering. SRV ansvarar för att bedriva utbildningsverksamhet för att tillgodose behov hos kommuner och statliga myndigheter av kompetens för utförande av uppgifter angivna i räddningstjänstlagen (1986:1102). Därutöver driver SRV risk- och säkerhetsutbildningar i syfte att tillgodose behov av kompetens hos kommuner, landsting och statliga myndigheter samt hos organisationer och företag för att kunna hantera störningar i samhällsviktig verksamhet. För myndighetens egen del handlar den förberedande verksamheten i hög utsträckning om medverkan i samverkansområdena.

Akut avhjälpande

Sker på lokal och eventuellt regional myndighetsnivå. Man poängterar att när en allvarlig händelse väl inträffat har myndigheten i praktiken spelat ut sin roll. SRV har i ett akut skede endast en stödjande funktion/expertfunktion.

Avvecklande/återuppbyggande

Denna fas diskuterades inte explicit under samtalet.

Generella kommentarer

SRV framhöll att de olika faserna i krishanteringen måste knytas ihop bättre. Risk- och sårbarhetsanalyser skulle kunna utgöra underlag för samtliga delar. Man måste hitta dels metoder som fungerar för detta, dels sätt att knyta ihop aktörerna i de olika faserna, då det ofta är olika personer som är inblandade i respektive fas.

Vikten av att ensa synen på begrepp etc. betonas. Det är viktigt att ”definiera området” i samverkan, att verka för en gemensam bild och begreppsapparat. Detta blir en viktig uppgift för KBM. Samsyn gäller i högsta grad även den regionala och kommunala nivån, där en stor del av det praktiska krishanteringsarbetet kommer att ske. Seminarier/workshops lyfts fram som lämpliga forum för diskussion. SRV understryker med eftertryck vikten av att utarbeta systemet i samverkan. Det finns mycket kompetens ute hos myndigheterna som måste tas tillvara.

SRV efterlyser även någon form av undersökning av allmänhetens inställning till hur mycket resurser som bör läggas på att försöka förhindra/mildra extraordinära händelser gentemot vad som händer dagligdags. Man efterlyser även utveckling kring hur man kan jämföra konsekvenser av olika typ. Hur skall man exempelvis värdera en ren miljö mot dödsfall i cancer eller skador till följd av olyckor?

Respons på årets risk- och sårbarhetsanalys, dels från KBM dels från departementet, efterlystes. Vikten av någon form av enhetlighet avseende resultatredovisningen i risk- och sårbarhetsanalysen framhölls.

Ett förslag på framkomlig väg att driva risk- och sårbarhetsanalysarbetet vidare var att fortsätta att utveckla ”typscenarier” som samtliga myndigheter kunde ha som ett ingångsvärde till sin analys.

Luftfartsverket

Allmänt

Intervjun genomfördes den 17 juni 2003 i Luftfartsverkets (LFV) lokaler i Norrköping. Närvarande var Håkan Österhed från LFV, Jan Flink från Evolator (konsult som anlitas av LFV), samt Marcus Abrahamsson och Roland Akselsson från LUCRAM.

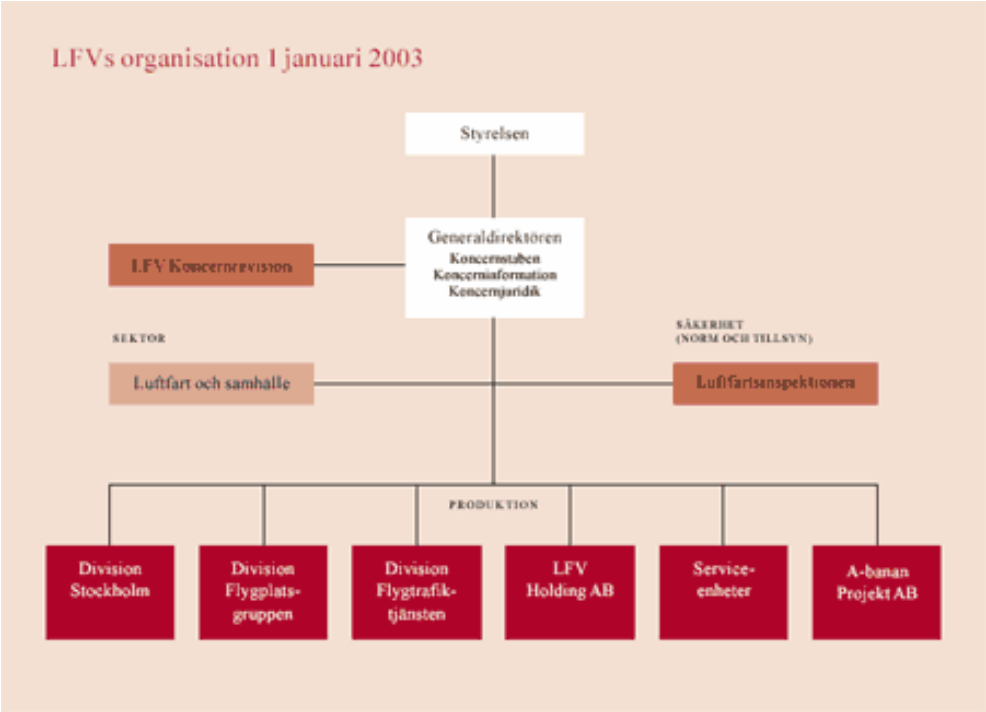
Kortfattad beskrivning av verksamheten

Av förordning (1988:78) med instruktion för Luftfartsverket framgår att Luftfartsverket är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, för den civila luftfarten. Luftfartsverket skall verka för att de transportpolitiska målen uppnås.

Verkets huvuduppgifter är att:

1. främja utvecklingen av den civila luftfarten,
2. ansvara för drift och utveckling av statens flygplatser för civil luftfart,
3. utöva tillsyn över flygsäkerheten för den civila luftfarten,
4. svara för skyddet av miljön mot föroreningar från civil luftfart,
5. ansvara för flygtrafiktjänst i fred för civil och militär luftfart och utbilda flygledare,
6. ombesörja beredskapsplanläggning för civila flygtransporter,
7. verka för att hänsyn tas till funktionshindrade personers behov inom den civila luftfarten,
8. ha samordningsansvaret för trafiksäkerhetsarbetet inom luftfarten.

I figur 17.6. nedan presenteras LFV:s organisationsstruktur.



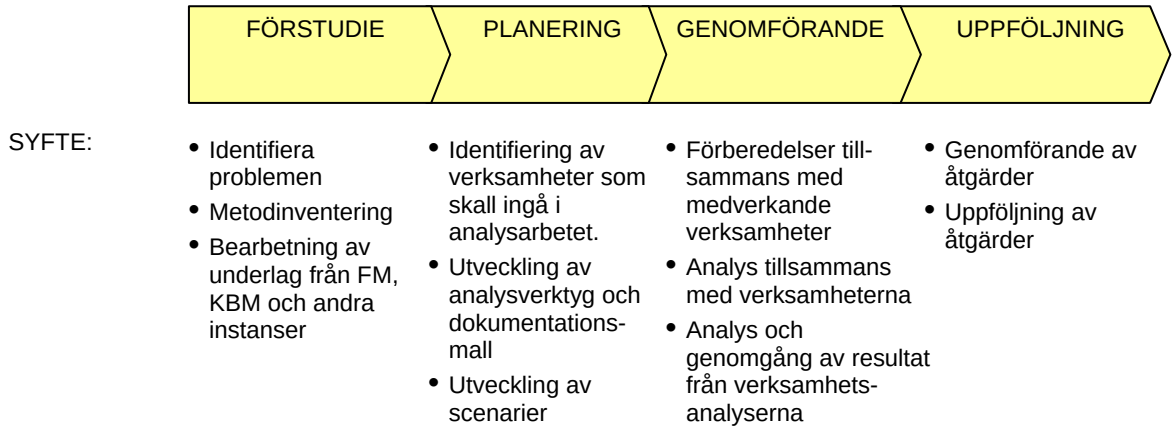
Figur 17.6 Luftfartsverkets organisation (Från årsredovisning 2002).

LFV ingår i samverkansområden Transporter, samt Skydd, undsättning och vård (LFV har ett övergripande ansvar för flygräddningstjänsten).

Förebyggande

Strukturen på detta samtal var sådan att Håkan Österhed och Jan Flink beskrev huvuddelarna i en sårbarhetsanalysmetod som används av LFV i samverkan med övriga aktörer i Luftfartssystemet. I detta avsnitt kommer en mycket kortfattad sammanfattning av metoden att ges. LFV har använt metoden för att analysera dels utvalda flygande aktörer, men även flygplatser, flygledningscentraler och underhållsföretag.

I figur 17.7. visas processen för den sårbarhetsanalysmetod som nämns ovan.



Figur 17.7. Process för den sårbarhetsanalysmetod som används vid LFV. (Från OH-material)

Metoden är i grunden scenariobaserad. Ett scenario består av dels en omvärldsbeskrivning, dels en händelse (ytterligare påfrestning på systemet). Omvärldsbeskrivningen avser bl.a. beredskapsläge (normalt eller höjt) och störningar i samhällets tekniska infrastruktur (el – tele- data etc.). En generell förutsättning vid analysen är att samhällets samlade transportbehov är 100% (d.v.s. om flyget av någon anledning inte (kan) nyttjas måste transporterna ske på något annat sätt). De händelser som man arbetat med handlar om brand, explosion, förgiftning, störningar i flygsektorns tekniska infrastruktur etc. Utgångspunkten vid analyserna har dock alltid varit att ”detta händer, vad får det för konsekvenser (exempelvis i form av ekonomiska termer, påverkan för ägare, produktion, miljö, medarbetare etc.) för er verksamhet?”.

De scenarier som används vid analyserna har arbetats fram av LFV. Myndigheten framhåller dock vikten av spårbarhet mot de omvärldssituationer som regeringen angett i propositionen 2001/02:158 Samhällets säkerhet och beredskap. I övrigt har dialog hållits med försvarsmakten samt post- och telestyrelsen och svenska kraftnät vid utarbetandet av scenarierna. Av vikt är att betona att det rör sig om scenarier av typen ”detta händer”, bakomliggande orsaker kan vara olika och utreds inte närmare.

Frågeställningar som belyses vid genomgång av ett specifikt scenario (exempelvis brand i kopplingsstation med bortfall av el och tele som följd) är av typen:

1. Vilka omedelbara konsekvenser medför scenariot för er verksamhet? Hur påverkas kapaciteten? (Här görs en bedömning hur stor andel av ursprunglig kapacitet som kvarstår givet ett visst scenario, 0-25-50-75-eller 100%).

2. Hur snabbt kan ni återgå till X% kapacitet? (25-50-75-100%) Vad krävs för att nå denna kapacitet, omedelbara aktiviteter/åtgärder?
3. Vilka brister har identifierats i er verksamhet?
4. Vilka riskreducerande åtgärder kan ni vidta?
5. Bedöm kostnader och prioritera.

Analyserna genomförs som nämnts ovan av LFV tillsammans med de olika aktörerna i flygtransportsystemet. Genom detta arbete har ett antal styrkor och svagheter i flygtransportsystemet identifierats. Dessa resultat kommer sedan att ligga till grund för prioriteringar av åtgärder dels inom LFV:s ordinarier verksamhet, men även som underlag för finansiering via utgiftsområde 6 totalförsvar. Resultatet av analysen kan också användas av övriga aktörer så till vida att de får insikt om brister och svagheter inom sin organisation som är värda att beakta och kanske åtgärda även om de inte är av den arten att finansiering från LFV:s sida är aktuell.

LFV gör bedömningen att den använda metoden är generell i den meningen att när nya omvärldsförutsättningar identifieras i försvarsberedningen eller av andra (exempelvis de exempel på svåra påfrestningar som utarbetas vid KBM), kan dessa enkelt arbetas in och användas som ytterligare utgångspunkt i nästa analysomgång.

Förberedande

Omfattningen och utformningen av den förberedande verksamheten med övningar o.s.v. diskuterades inte under intervjun.

Akut avhjälpande

Omfattningen och utformningen av LFV:s roll i en akut avhjälpande situation diskuterades inte under intervjun.

Avvecklande/återuppbyggande

Omfattningen och utformningen av LFV:s roll i en avvecklande/återuppbyggande fas diskuterades inte under intervjun.

Generella kommentarer

LFV betonar att sekretessproblematiken måste lösas kring de analyser som skall lämnas in enligt förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap. En del information har utelämnats i den analys som lämnades in i första omgången. Den utgör endast en översiktlig beskrivning av svagheter och brister o.s.v.

Det huvudsakliga budskapet i den analys som lämnats in är att flygtransportsystemet har en god basförmåga som bygger på flygsäkerhetskraven, men att man i ett kapacitetsperspektiv inte ser lika ljust på situationen.

LFV:s poängterar även det problematiska i det att man har relativt god överblick avseende hur flygtransportsystemet påverkas vid olika typer av påfrestningar, men att man har dålig insikt i vad det får för återverkningar ute i övriga samhället. Detta är dock något som det arbetas aktivt med inom samverkansområdet Transporter.

LFV ser den analys som skall lämnas in enligt förordning (2002:472) som en form av ”statusrapportering” av det löpande arbetet. Vid nästa rapportering kommer en beskrivning av vad som skett sedan den föregående att ges. Vilka åtgärder har vidtagits och vad blev effekterna av dem etc. Under året kommer även ”ett nytt varv” i analysarbetet ute hos aktörerna i flygtransportsystemet att påbörjas, där de nya scenarier som arbetats fram skall vägas in.

LFV framhåller vikten av att kunna göra en bedömning huruvida förmågan att bemöta ett visst hot eller scenario utgör en del av basförmågan (som finansieras av aktörerna själva) eller grundförmågan (att svara upp mot ”extraordinära händelser”) som skall finansieras via KBM.

LFV bedömer att den metod som används för sårbarhetsanalys skulle kunna utvecklas mot andra områden, för att eventuellt möjliggöra värdering ur ett samhällsperspektiv mellan olika områden.

LFV anser att KBM:s roll avseende de analyser som skall lämnas in enligt förordning (2002:472) är att göra en övergripande värdering och ge förslag till prioriteringar mellan samverkansområdena. Man påpekar att KBM behöver förtydliga sin roll och rollen för nämnda risk- och sårbarhetsanalyser.

Statens veterinärmedicinska anstalt

Allmänt

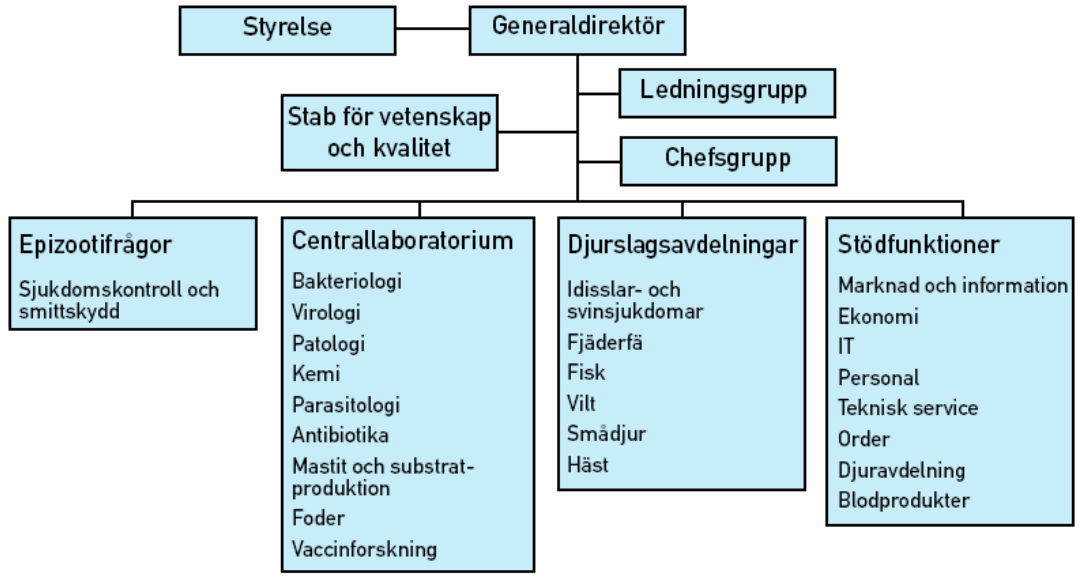
Intervjun genomfördes den 23 juni 2003 i Statens veterinärmedicinska anstalts (SVA) lokaler i Uppsala. Närvarande var Christer Hoel, Ivar Vågsholm och Julia Österberg från SVA, samt Marcus Abrahamsson och Kurt Petersen från LUCRAM.

Kortfattad beskrivning av verksamheten

Av förordning (1999:341) med instruktion för Statens veterinärmedicinska anstalt framgår att SVA har till uppgift att vara veterinärmedicinskt expert- och serviceorgan åt myndigheter och enskilda. SVA skall särskilt

1. utreda smittsamma djursjukdomars uppkomst, orsak och spridningssätt,
2. vara veterinärmedicinskt centrallaboratorium,
3. utföra diagnostik av djursjukdomar inklusive den diagnostik som föreskrivs i EG:s regelverk,
4. vara nationellt referenslaboratorium för zoonoser och zoonotiska agenser,
5. medverka i förebyggande och bekämpande av djursjukdomar,
6. bedriva forsknings- och utvecklingsarbete inom sitt verksamhetsområde, samt
7. följa och analysera utvecklingen av resistens mot antibiotika och andra antimikrobiella medel bland mikroorganismer hos djur.

SVA skall i första hand utföra de undersökningar och utredningar som Statens jordbruksverk begär. Dessa skall planeras och genomföras efter samråd med Jordbruksverket. Veterinärmedicinska anstalten skall om möjligt också med förtur utföra de undersökningar som andra statliga myndigheter begär. SVA:s organisation framgår av figur 17.8. Verksamheten har tre huvudinriktningar, myndighetsuppgifter (ca 30%, finansieras av staten), uppdragsverksamhet (analystjänster, konsulttjänster etc., ca 60%), samt externt finansierad forskning (ca 10%).



Figur 17.8 SVA:s organisation

SVA ingår i samverkansområdet Spridning av farliga ämnen.

Förebyggande

SVA:s huvudsakliga beredskapsverksamhet rör epizootifrågor, och denna del av verksamheten finansieras av staten. SVA är dock en renodlad expertmyndighet, och inget beslutande organ (åtminstone inte i formell mening) i dessa frågor. Alla beslut rörande dessa frågor fattas av andra myndigheter, främst jordbruksverket, men även livsmedelsverket. Där hanteras såväl epizootier som zoonoser. Samtidigt som man fungerar som expertmyndighet ”uppåt” har man en roll som rådgivare ut mot näringslivet inom området. SVA:s stora styrka i detta sammanhang är den kompetens och de faciliteter som finns för analys vid misstanke om allvarlig djursmitta. SVA är Sveriges nationella referenslaboratorium (krav på ett sådant finns i EU:s lagstiftning).

Generellt kan man säga att SVA (och samhällets system för att undvika allvarliga epizootier) använder sig av tre huvudsakliga ”riskidentifieringsmetoder”, eller informationskällor.

- Sjukdomar som omfattas av epizootilagen (1999:657), vilka anges i verkställighetsföreskrifter av jordbruksverket, är anmälningspliktiga för samtliga aktörer, d.v.s. såväl djurägare som veterinärer har anmälningsplikt till jordbruksverket vid misstanke om smitta. SVA:s inkoppling vid sådana fall finns inte reglerad men det är praxis att man blir kontaktad snabbt. Om sådana misstankar finns måste prover tas och då kopplas SVA in per automatik.
- Omvärldsbevakning, såväl nationellt som internationellt, d.v.s. att följa upp sjukdomsläget i omvärlden. Ett aktuellt exempel är spridningen av ”west nile virus” i USA, där SVA följer vad som händer, hur det sprids osv. Inom EU finns samverkan på detta område.
- SVA utför även viss ”screening” avseende vissa sjukdomar i epizootilagstiftningen (exempelvis svinpest). Denna screening görs enligt EU-lagstiftning för att visa att Sverige är fritt från dessa sjukdomar.

En beredskapshandbok har utarbetats, där hantering av ”normala” epizootier beskrivs. Vid eventuella nya hot (t.ex. en ny okänd sjukdom) kan en ”epizootigrupp”, bestående av nyckelpersoner inom SVA, kallas in med kort varsel. Denna grupp gör i sådana fall upp en plan för hur det enskilda fallet skall hanteras.

Förberedande

Eftersom den analysverksamhet som SVA förväntas bistå med i ett akut läge är av samma karaktär som den dagliga analysverksamheten anser myndigheten att man har goda förutsättningar att lösa sin uppgift, åtminstone avseende de kända sjukdomarna och förutsatt att den tekniska infrastrukturen i form av elförsörjning etc. fungerar.

Akut avhjälpande

Det operativa ansvaret vid upptäck av en anmälningspliktig sjukdom enligt epizootilagen (eller annan allvarlig smittspridning) ligger ute på det lokala och regionala planet, via länsveterinärer etc. Där sköts allt det praktiska med avspärrningar mm. De formella besluten avseende sådana åtgärder tas dock av jordbruksverket. Området är väl reglerat. Epizootier

finns även reglerade i EU-lagstiftning. Det finns en form av ”mall” för hur avspärrningar o.s.v. skall utformas.

SVA har dock en 24:h beredskap, där man när som helst kan komma i kontakt med en sakkunnig veterinär i smittskyddsfrågor (vid misstanke om epizooti). Kapacitet finns även för att med sex timmars varsel starta analysverksamhet av ”alla” kända sjukdomar. För detta finns ett joursystem. Denna kompetens (med ständigt övad personal) kan upprätthållas i och med att en stor del av SVA:s verksamhet är uppdragsverksamhet där just denna typ av analyser utförs i det dagliga arbetet.

Avvecklande/återuppbyggande

Ingen direkt diskussion fördes kring denna fas. SVA poängterade dock vikten av att upprätthålla förtroendet för verksamheten dels genom en hög vetenskaplig standard i det vardagliga arbetet, dels genom exempelvis informationsinsatser under allvarliga händelser.

Generella kommentarer

Problemet med att de analyser som skall lämnas in enligt förordning (2002:472) blir offentliga poängterades. Sekretessproblematiken måste lösas.

SVA ser på analyserna ovan som en form av statusrapportering, en beskrivning av hur myndigheten arbetar med dessa frågor. Man efterlyser ett förtydligande avseende vilken typ av information Krisberedskapsmyndigheten önskar få i dessa risk- och sårbarhetsanalyser.

Man nämnde att inom SVA:s område kanske det vore mest givande att genomföra en sårbarhetsanalys på EU-nivå.

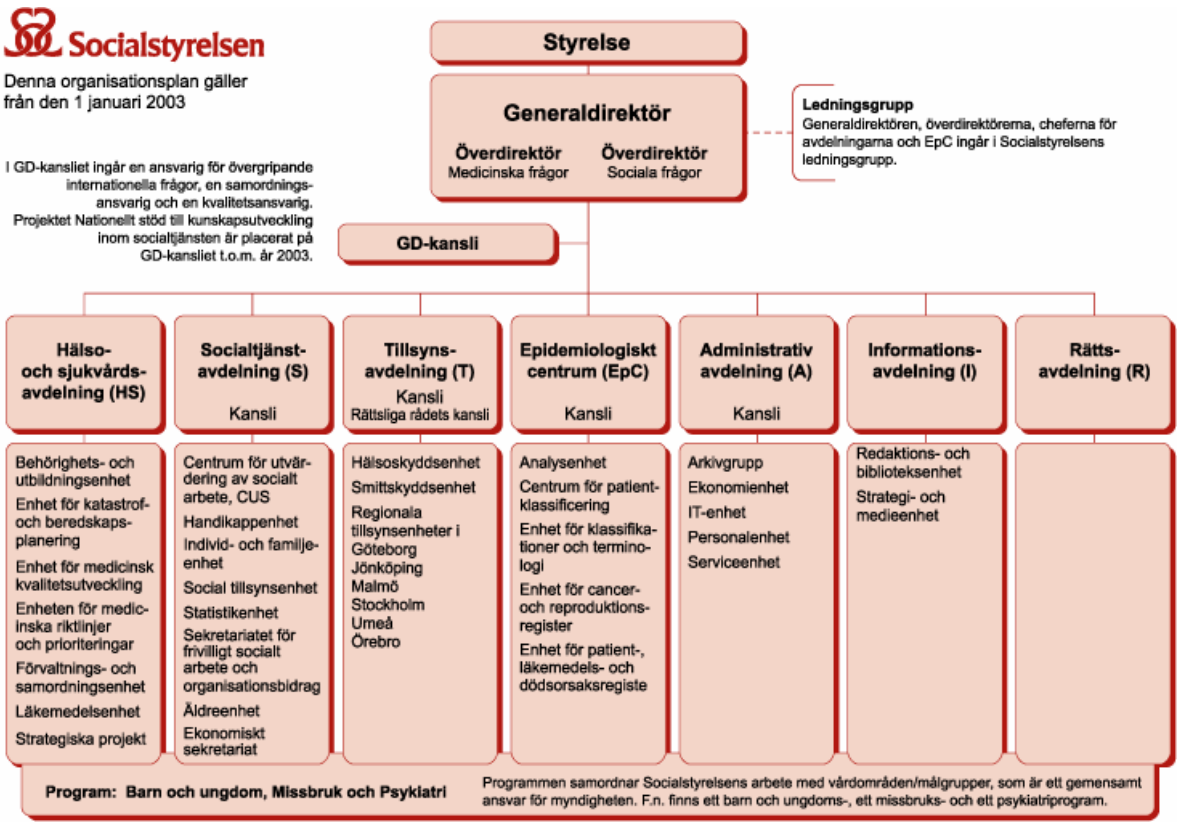
Socialstyrelsen

Allmänt

Intervjun genomfördes den 25 juni 2003 i Socialstyrelsens lokaler i Stockholm. Närvarande var Jonas Holst från Socialstyrelsen, Ingrid Pettersson från Krisberedskapsmyndigheten, samt Marcus Abrahamsson och Roland Akselsson från LUCRAM.

Kortfattad beskrivning av verksamheten

Av förordning (1996:570) med instruktion för Socialstyrelsen framgår att Socialstyrelsen är central förvaltningsmyndighet för verksamhet som rör socialtjänst, hälso- och sjukvård och annan medicinsk verksamhet, tandvård, hälsoskydd, smittskydd, stöd och service till vissa funktionshindrade samt frågor om alkohol och missbruksmedel, allt i den utsträckning det inte är en uppgift för någon annan statlig myndighet att handlägga sådana ärenden. Utöver vad som framgår av förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, skall Socialstyrelsen samordna och övervaka planläggningen av den civila hälso- och sjukvårdens, hälsoskyddets, smittskyddets samt socialtjänstens beredskap. Socialstyrelsen skall samordna förberedelserna för försörjningen med läkemedel och sjukvårdsmateriel inför höjd beredskap och för att upprätthålla en katastrofmedicinsk beredskap.



Figur 17.9 Socialstyrelsens organisation (från www.sos.se)

Socialstyrelsen ingår i samverkansområdena Spridning av farliga ämnen, samt Skydd, undsättning och vård.

Förebyggande

Socialstyrelsen är normsättande myndighet för hälso- och sjukvården utan något egentligt operativt eget ansvar (det operativa ansvaret ligger enligt hälso- och sjukvårdslagen (1982:763) på sjukvårdshuvudmännen). Undantaget är smittskyddsområdet, där man har ett operativt samordningsansvar, men också föreskriftsrätt. Socialstyrelsens styrmedel gentemot sjukvårdshuvudmännen är huvudsakligen föreskrifter, riktlinjer, rekommendationer och guidelines osv. Socialstyrelsen har även tillsynsmöjlighet för hela hälso- och sjukvården Tillsynsansvaret/möjligheten (Socialstyrelsen har enligt sin instruktion skyldighet att genomföra tillsyn, men hur och med vilken frekvens är upp till myndigheten) omfattar dels individtillsynen, men även verksamhetstillsyn, d.v.s. hur fungerar en del av systemet.

Som nämnts ovan är sjukvårdshuvudmännen operativt ansvariga enligt hälso- och sjukvårdslagen. Det har även förutsatts att det har ingått i uppgiften att tillgodose det föreliggande vårdbehovet, att även hålla en katastrofmedicinsk beredskap. Det innebär att Socialstyrelsen kan utföra tillsyn över sjukvårdshuvudmännen, även avseende den katastrofmedicinska beredskapen. Socialstyrelsen håller även på att förbereda en föreskrift för sjukvårdshuvudmännen på detta område, som kommer att bli styrande (målstyrning). Efterlevnad kontrolleras vid tillsyn.

Socialstyrelsen har en viktig uppgift i att underlätta och stödja sjukvårdshuvudmännen på olika sätt. Detta sker exempelvis genom kompetensuppbyggnad genom kunskapscentra som genomför omvärldsbevakning och FoU, samt medicinska expertgrupper. Insatser görs även på utbildningssidan, dels genom att hålla egna kurser men även genom utbildningsbidrag till landstingen.

Socialstyrelsen upprätthåller även beredskapslager avseende läkemedel, sängar, vacciner, utrustning för att kunna arbeta vid saneringsplatser etc.

Risk- och sårbarhetsanalysmodell

Socialstyrelsen har lagt ut ett uppdrag på totalförsvarets forskningsinstitut (FOI) att ta fram en risk- och sårbarhetsanalysmodell för hälso- och sjukvården. Det ”normala” vid den typen av analyser är att man utgår från scenarier och frågar sig: hur hanterar vi detta? Här har man i stället tagit fram en modell som utgår från typskador. Angreppssättet bygger på antagandet vid exempelvis en transportolycka ser skadepanoramat i princip ut på ett visst sätt, x antal skallskadade, x antal bröst- och bukskadade etc. Givet detta försöker man utröna hur sjukvårdsorganisationen klarar dessa olika typskador, vilken kapacitet har man, även efter förstärkning/omdisponering? Man skall även försöka identifiera de gränssättande faktorerna, exempelvis bortfall av teknisk infrastruktur som elförsörjning etc., vad är det som begränsar kapaciteten?

Modellen har några kritiska steg. Man måste utgå ifrån scenarios där man identifierar vilka typskador som kan vara aktuella. Bedömningen är att detta kan göras utifrån statistik. Sedan skall detta matchas mot kapaciteten som finns i sjukvårdsorganisationen, vilket bedöms vara mer problematiskt. Modellen skall ”test”-användas vid två landsting, sedan skall detta utvärderas.

Man påpekar dock att denna modell är avsedd att ge svar på vad organisationen kan hantera. Den kan inte användas för att identifiera vilka risker i samhället som är allvarligast osv.

Uppföljning av arbetet på lokal och regional nivå

Sjukvårdshuvudmännen på lokal och regional nivå har genomfört riskanalyser under lång tid. Dessa analyser har dock i hög utsträckning varit baserade på de typer av risker som räddningstjänsterna arbetar med. Socialstyrelsen har inget systematiserat system för att ta in informationen från sjukvårdshuvudmännens riskanalyser. Dock genomförs vid kunskapscentrat i Göteborg en översikt av sjukvårdshuvudmännens katastrofplaner, där det ingår att bedöma hur väl underbyggda de är bl.a. i vilken utsträckning de är baserade på riskanalyser.

I och med förändringen i hälso- och sjukvårdslagen (som innebar att sjukvårdshuvudmännen är skyldiga att hålla en katastrofmedicinsk beredskap) har Socialstyrelsen nu bättre möjligheter att följa upp sjukvårdshuvudmännens arbete på detta område genom tillsyn. Det saknas dock metoder och verktyg för hur denna tillsyn skall genomföras för att kunna bedöma huruvida den katastrofmedicinska beredskapen hanteras på ett bra sätt.

Förberedande

Vid samtalet diskuterades inte utformning och omfattning av den förberedande verksamheten.

Akut avhjälpande

Som nämnts tidigare är det sjukvårdshuvudmännen som har det operativa ansvaret, d.v.s. som skall agera vid akuta händelser.

För närvarande drivs ett projekt vid Socialstyrelsen som går ut på att ta fram ett IT-baserat ledningssystem för sjukvården, SWEDE. Projektet omfattar dirigering, hänvisning, rapportering och uppföljning. Huvudkomponenterna i systemet utgörs av ledningsprinciper, omgivning och beroenden, informations- och kommunikationssystem, terminologi och definitioner samt utbildning och övning.

Avsikten med SWEDE är att utveckla ett gemensamt ledningssystem som innefattar samtliga ledningsnivåer med tydlig roll- och ansvarsfördelning. Från skadeplats, sjuktransportfordon och sjukvårdinrättningar måste aktuell information kunna överföras på ett sådant sätt att den som har behov av och rättighet till informationen finner den i en för riket gemensam databas/katalog som kan vara lokaliserad till ett flertal platser i landet. Respektive landsting beslutar själv om man skall utnyttja systemet. Socialstyrelsens roll är att vara dels rådgivande, dels i vissa fall styrande. (från www.sos.se)

Värt att notera kan vara att systemet ovan är avsett och utformat för sjukvårdsorganisationen. Vid allvarligare händelser kommer ett flertal andra samhälleliga aktörer att vara inblandade och strävan måste vara att skapa någon form av ”gemensam grundsyn” avseende ledning av stora räddningsinsatser.

Avvecklande/återuppbyggande

Socialstyrelsen har sedan några år huvudmannaskapet för KAMEDO (katastrofmedicinska organisationskommittén), som studerar medicinska effekter av katastrofer och krig.

Generella kommentarer

Det problematiska i att sekretessfrågan inte är löst avseende risk- och sårbarhetsanalyserna enligt förordning 2002:472 påpekades. Dels utgör det en risk i sig att i offentliga dokument beskriva de sårbarheter som finns i systemet, dels (eller som en följd av detta) innebär det att man inte kommer att få fram en rättvisande bild.

Inom Socialstyrelsen ser man ”avrapporteringen” enligt ovan nämnda förordning som en form av statusrapport. Till nästa omgång kommer en tydligare analys av själva myndighetens, Socialstyrelsens sårbarhet att inarbetas.

Avseende risk- och sårbarhetsanalyserna enligt förordning 2002:472 generellt anser myndigheten att det är omöjligt att ta fram en gemensam metod för hela det svenska samhället. Man anser däremot att KBM borde sträva efter att verka för att de olika metoder och modeller som används inom olika samhällssektorer på något sätt levererar jämförbara resultat, jämförbar upplösning och detaljeringsgrad. En form av kvalitetssäkring. Ett forum där metoder för risk- och sårbarhetsanalys kunde diskuteras efterlystes.

Svårigheterna med gränsdragning avseende vad som skall finansieras (i beredskapshänseende) av sjukvårdshuvudmännen själva (”vardagsolyckor” etc.), och vad som skall finansieras via ”KBM-pengarna” betonades. Man anser att risk- och sårbarhetsanalyserna kommer att bli en av hörnpelarna i myndighetens anslagsäskande, vilket betonar vikten av ett sammanhängande system för dessa analyser (om än ej gemensam analysmetod).

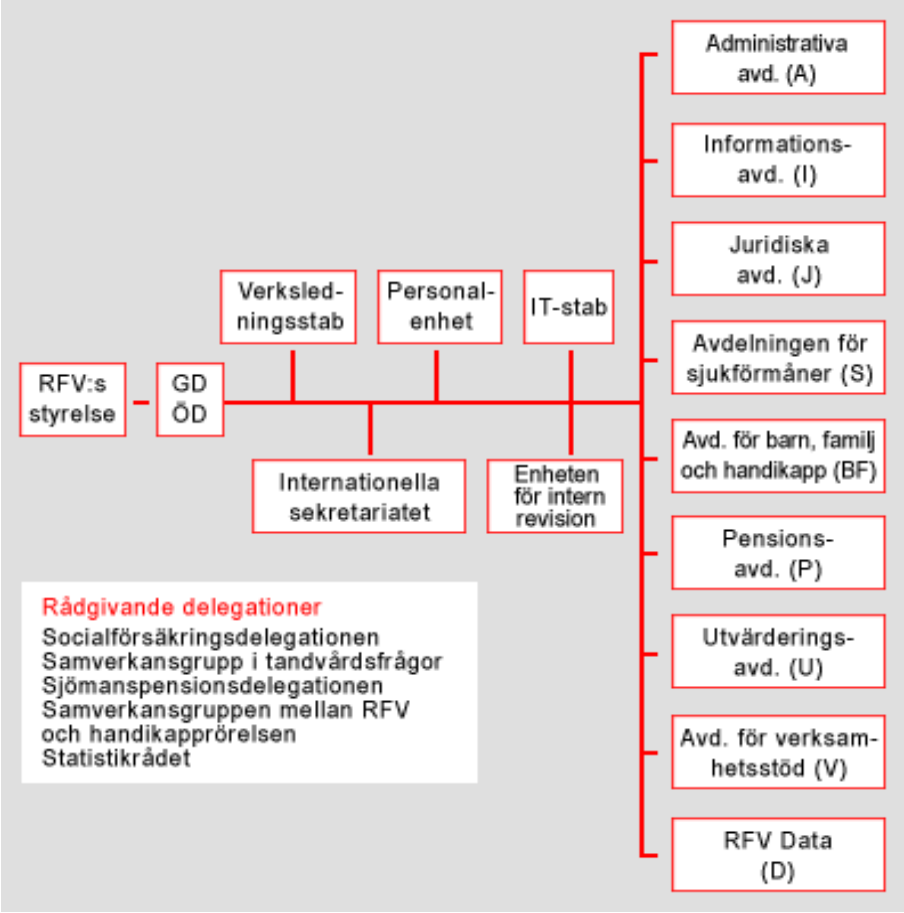
Riksförsäkringsverket

Allmänt

Intervjun genomfördes den 26 juni 2003 i Riksförsäkringsverkets (RFV) lokaler i Stockholm. Närvarande var Monica Lindgren och Berit Sjödin (videokonferens från Sundsvall) från RFV, samt Marcus Abrahamsson och Lars Fredholm från LUCRAM.

Kortfattad beskrivning av verksamheten

Av förordning (1998:739) med instruktion för Riksförsäkringsverket framgår bl.a. att RFV är central förvaltningsmyndighet för socialförsäkringen och anslutande bidragssystem, om inte något annat är särskilt föreskrivet. RFV skall bl.a. särskilt verka för att socialförsäkrings- och bidragssystemen tillämpas likformigt och rättvist, verka för att åtgärder vidtas för att förebygga och minska ohälsa i syfte att minska de långa sjukperioderna, utöva tillsyn över de allmänna försäkringskassorna, samt vara ansvarig systemägare för Riksförsäkringsverkets och försäkringskassornas gemensamma IT-system. Utöver vad som framgår av förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, skall RFV ansvara för att samordna och övervaka planläggningen av de allmänna försäkringskassornas beredskap.



Figur 17.10. Riksförsäkringsverkets organisationsstruktur. (Från www.rfv.se)

Riksförsäkringsverket ingår i samverkansområdet Ekonomisk säkerhet.

Förebyggande

RFV:s risk- och krishantering är av naturliga skäl i hög utsträckning inriktad på utbetalningsfunktionen. Viktiga delar är att kunna hantera allmänhetens kontakt med försäkringskassorna (RFV har i stort sett ingen ”kundkontakt”, det sker via försäkringskassorna), och att allmänheten kan få den ersättning de är berättigade till.

När RFV analyserar de hot och risker som myndigheten ser för socialförsäkringen så arbetar man oftast med en form av scenarioteknik. Detta mot bakgrund av att denna typ av metodik bedöms vara lättanvänd och lättförståelig. De scenarier som genereras bygger på den kunskap som finns om sårbarheten i systemet.

Analyser genomförs av såväl RFV centralt som de enskilda försäkringskassorna. RFV bistår försäkringskassorna med stöd i detta arbete. I den analys som inlämnades enligt förordning 2002:472 arbetades information från försäkringskassornas analyser. RFV tog fram en enkel mall för vilka rubriker analysen skulle innehålla och bjöd även in försäkringskassorna på en informationsdag angående innehållet i analyserna. Inför ”nästa omgång” skall denna gemensamma struktur för analyserna göras ännu tydligare. RFV:s centrala analyser är i hög utsträckning inriktade på det gemensamma IT-systemet och produktionsanläggningen i Sundsvall.

Förberedande

Förberedande övningar har varit eftersatt på senare tid. En scenariobaserad övning som skall hållas i höst med socialdepartementet och övriga ingående myndigheter nämndes.

Akut avhjälpande

En krisledningsgrupp finns inrättad, gruppens uppgifter vid en allvarlig störning av något slag diskuterades dock inte.

Avvecklande/återuppbyggande

Denna fas diskuterades inte explicit under samtalet.

Generella kommentarer

RFV betonade att sekretessproblematiken måste lösas. Som det är nu kommer inte analyserna som lämnas in enligt förordning 2002:472 att ge en rättvisande bild av verksamheten.

Avseende önskat stöd från KBM betonade man att det vore önskvärt att få en fingervisning om dels vilken typ av information som skall levereras i analyserna, men kanske framför allt en fingervisning om vilken typ av händelser man skall inrikta sig på. RFV efterlyser gemensamma scenarier som samtliga myndigheter kan ha som utgångspunkt för sitt analysarbete, detta för att möjliggöra att analyserna blir jämförbara. Som exempel nämndes att den tekniska infrastrukturen varit föremål för analys under lång tid men att andra områden

är mer eftersatta. Att hitta en gemensam metod över hela myndighetsområdet tror man dock inte på, verksamheterna ser för olika ut. (Möjligen kan det finnas andra mindre myndigheter med mindre erfarenhet av riskhanteringsarbete som behöver ett mer direkt metodstöd).

Ett område som lyftes fram var beroendet mellan olika verksamheter, något som måste utredas noggrannare. Som exempel nämndes RFV:s beroende av att betalningsväsendet fungerar. RFV ser mycket positivt på arbetet i samverkansområdena, där förutsättningar finns för att kunna behandla sådana frågeställningar.

RFV ser arbetet med risk- och sårbarhetsfrågor som en process, där man en gång om året lämnar ifrån sig en form av statusrapport. Man betonade också vikten av att skynda långsamt, att fördjupa sig inom ett område i taget för att på så sätt inom ett antal år skaffa sig en bra bild över läget.

Svenska Kraftnät

Allmänt

Intervjun genomfördes den 11 augusti 2003 i Svenska Kraftnäts (SvK) lokaler i Halmstad. Närvarande var Håkan Stomsjö från SvK, samt Gustaf Olsson, Kurt Petersen och Per Runeson från LUCRAM.

Kortfattad beskrivning av verksamheten

”Svenska Kraftnät äger och driver stamnätet för elkraft, vilket omfattar landets totalt ca 15000 km långa 220 kV och 400 kV ledningar med stationer, utlandsförbindelser och IT-system. Till uppgifterna hör att ansvara för att elsystemet kortsiktigt är i balans och att dess anläggningar samverkar driftsäkert, s.k. systemansvar. Verksamheten finansieras genom de avgifter kraftproducenter, industrier och andra förbrukare betalar för att transportera el via stamnätet. Svenska kraftnät är ett statligt affärsverk och en myndighet som startade sin verksamhet den 1 januari 1992”. (från www.svk.se).

Av Förordning (1991:2013) med instruktion för Affärsverket svenska kraftnät framgår dessutom bl.a. att SvK skall svara för den operativa beredskapsplaneringen inom sitt verksamhetsområde under kris- eller krigsförhållanden.

Under samtalet förtydligades att SvK har en dubbel roll, dels som ansvarig för anläggningar i transmissionsnätet, dels som myndighet som skall ansvara för att elförsörjningen till samhällsvitala delar kan säkras.

I figur 17.11 visas SvK:s organisation.

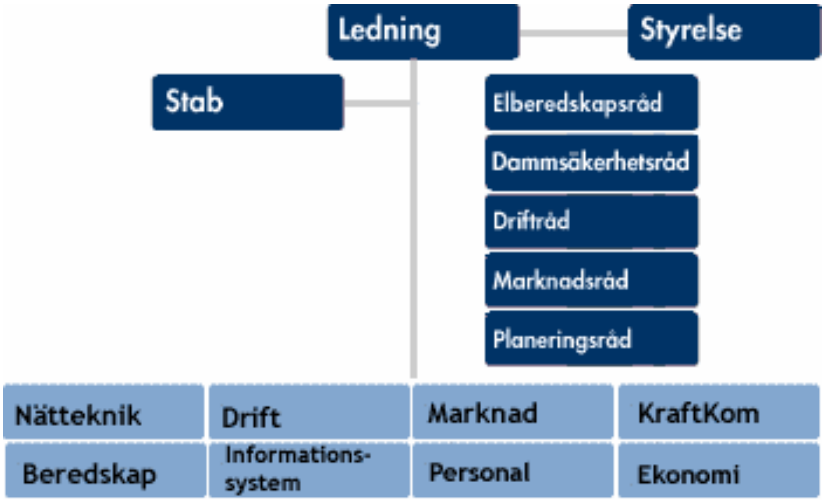


Fig. 17.11. SvK:s organisation. (Från www.svk.se)

SvK ingår i samverkansområde ”Teknisk infrastruktur”.

Förebyggande

SvK måste samverka med flera myndigheter i sin risk- och sårbarhetsanalys. Därför har man regelbundna diskussioner med t.ex. Luftfartsverket och Banverket. Hur beroende är de av elleveranser? Det är givetvis av vikt att förstå sådana kopplingar. SvK har på eget initiativ tagit dessa kontakter för att åstadkomma ett informationsutbyte. Man ser utifrån sitt myndighetsansvar kravet på att också samordna med andra myndigheter. Hittills har ingen annan myndighet haft ett mer övergripande ansvar. Detta borde rimligen falla på KBM.

SvK har ansvar för eget nät, d.v.s. 400 och 220 kV. Dessutom har myndigheten ett beredskapsansvar för helheten. Detta kan betyda att SvK kan behöva göra finansieringsinsatser för att delar av distributionsnätet skall kunna fungera ända fram till kritiska anläggningar. På så sätt kan t.ex. SvK jämföra sina kritiska anläggningar med exempelvis Banverkets kritiska anläggningar. På så sätt kan man som *myndighet* kräva att helheten fungerar och därmed finansiera förstärkning av utrustning.

Det förebyggande arbetet går ut på att reducera katastrofers effekt på människor och egendom. Mycket tid och resurser går åt för det förebyggande arbetet, såsom beskrivits ovan. Samverkan med andra myndigheter är viktig, men man kan konstatera att det idag inte finns en systematiskt utbyggd organisation som tar ansvar för att interdependensen mellan myndigheters ansvarområden fungerar. Däremot kan man konstatera ett SvK tar ett totalansvar utifrån ett elförsörjningsperspektiv.

För att kartlägga hotbild etc. arbetar SvK ihop med bl.a. Säpo och försvarsmakten. Inom SvK arbetar man mest aktivt med sårbarhetsfrågor baserade på de hotbilder som kartlagts. Någon strukturerad riskidentifieringsprocess utöver vad som nämns ovan används inte och SvK framhöll att behovet är stort att få fram en modell som ett ramverk för att genomföra riskanalyserna enligt förordning 2002:472.

SvK framhöll att samarbetet med övriga aktörer inom kraftbranschen är av stor vikt och man har bl.a. etablerat ett utbyte av incidentrapportering (på frivillig basis). Avseende omvärldsbevakning etableras bl.a. ett nätverk mellan de nordiska länderna.

Även den framtida kompetensförsörjningen inom myndigheten och i branschen framhölls som en viktig framgångfaktor.

Förberedande

Fasen förberedande innebär planering för att rädda liv, minimera skada och effektivisera akut insats. Primära ansvaret för SvK är *systemansvaret*. Man måste se till att bibehålla själva systemets funktionalitet. När det gäller att definiera systemet så är frågan hur mycket det handlar om ett tekniskt och hur mycket ett organisatoriskt. Hittills har SvK mest betonat de tekniska aspekterna av risk- o sårbarhetsarbetet, medan de organisatoriska utmaningarna inte fått samma uppmärksamhet.

Som ett exempel på övningsverksamhet har SvK tillgång till simulatorstöd för konsekvensanalys. Aristo (realtidssimulator för svenska kraftnätet) är ett exempel. SvK ser idag inte ett direkt behov av ytterligare simulatorer.

Akut avhjälpande

Den akut avhjälpande fasen innebär en omedelbar insats för att skydda liv och egendom. Det operativa ansvaret vid en akut kris ligger på driftcentralerna. Dessutom finns en krisledningsgrupp, som sitter i Stockholm. Vid en katastrof där flera ägare är inblandade, t.ex. Vattenfall o Sydkraft, finns idag inte en förberedd integrerad krisledning. För den tekniska delen finns en hel del informationsutbyte, men organisatoriskt kanske man inte har samma beredskap. Vid kända typer av störningar finns färdiga handlingsplaner.

Avvecklande/återuppbyggande

Denna fas diskuterades inte explicit under samtalet.

Generella kommentarer

Det finns väldigt mycket empirisk kunskap om hur man arbetar med risk- och sårbarhetsanalys, men myndigheten har ingen utarbetad *systematisk metodik* till sitt stöd. behovet är stort att få fram en modell som ett ramverk för att genomföra risk- och sårbarhetsanalys.

Kopplingen mellan det förebyggande och förberedande arbetet till det akuta avhjälpandet framgår inte tydligt. Den tekniska kunskapen finns antagligen, men frågan är hur den organisatoriska beredskapen ser ut. Kopplingen mellan SvK och driftcentraler, kopplingen till räddningsverk och andra myndigheters akuta räddningsorganisationer är inte klar.

Informationshantering är ett svårt problem. SvK hanterar information på många plan, dels ”off-line” med stora mängder information i förebyggande och förberedande stadier, dels ”on-line” i akuta lägen då en händelse har inträffat. Vad gör man för att förhindra intrång i driftsystemen eller styrsystemen? Detta blir en allt viktigare fråga.

Vem gör en *konsekvensanalys* som sträcker sig *utanför* det specifika elförsörjningssystemet? Exempelvis är Aristo en förnämlig resurs för att analysera konsekvenser av olika händelser i själva elnätet. Däremot: vad händer vid avbrott på olika industrier eller andra delar i samhället? Vem tar ansvar för de icke-samhällsvitala delarna? Vad betyder det att industrin X får ett avbrott på 2 timmar? Detta är frågeställningar som måste beaktas vidare i framtiden.

Referenser

Amalberti R. ”*The paradoxes of almost totally safe transportation systems”*, Safety Science, vol 37, Elsevier, (2001).

Andersson M & Kinnerberg E *”Naturkatastrofers bidrag till riskbilden i EU”*, rapport 5089, Brandteknik, Lunds Tekniska Högskola (2001)

Bier V. M., Haimes, Y.Y., Lambert, J.H., Matalas, N.C. & Zimmerman, R. *”A Survey of Approaches for Assessing and Managing the Risk of Extremes”* Risk Analysis, Vol 19, No 1, (1999).

Blaikie P., Cannon T., Davis I. & Wisner B. “*At Risk: Natural Hazards, People’s Vulnerability and Disasters”* London, Routledge (1994)

Boin A. *”Crisis Management in Europe: A Discussion of Key Factors in Improving Safety”* Paper for The NATO/Russia Advanced Research Workshop: Forecasting and Preventing Catastrophes, University of Aberdeen (2003).

CCMD *“Crisis and Emergency Management: A Guide for Managers of the Public Service of Canada”* Canadian Centre for Management Development, (2003).
Haimes, Y.Y. *“Risk Modeling, Assessment, and Management”* John Wiley & Sons (1998)

CCPS ”*Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*”, Centre for Chemical Process Safety of the American Institute of Chemical Engineers, New York, (2002).

COSO, *“Enterprise Risk Management Framework”*, The Committee of Sponsoring Organizations of the Treadway Commission, (2003).
http://www.erm.coso.org/Coso/coserm.nsf/frmWebCOSOHome?ReadForm (2003-09-20).

Cutter, S.L., J.T. Mitchell, and M.S. Scott, “*Revealing the Vulnerability of People and Places: A Case Study of Georgetown County, South Carolina,*” Annals of the AAG 90 (4): 713-737. (2000)

Dataföreningen *“SBA Check – Checklisteverktyg för nulägesanalys med speciell inriktning på informationssäkerhet”*, Dataföreningen, Stockholm, (2002).
http://www.dfs.se/products/sba/check/ (2003-10-10).

DEFRA “*Risk Management Strategy*”, UK Department for Environment, Food and Rural Affairs, (2002).
http://www.defra.gov.uk/corporate/busplan/riskmanage/riskmanage.pdf (2004-01-13).

de Freitas C.M., Porto M.F.S., de Freitas N.B.B., Pivetta F., Arcuri A.S., Moreira J.C. & Machado J.M.H “*Chemical Safety and Governance in Brazil.”* Journal of Hazardous Materials 86: (1-3), 135-151. (2001)

Dibben C. & Chester D.K. *"Human Vulnerability in Volcanic Environments: The Case of Furnas, Sao Miguel, Azores."* Journal of Volcanology and Geothermal Research, 92: (1-2) 133-150. (1999)

Einarsson, S. & Rausand, M. *"An Approach to Vulnerability Analysis of Complex Industrial Systems"* Risk Analysis, Vol 18, No 5, (1998)

Einarsson S "*Comparison of QRA and Vulnerability Analysis: Does Analysis Lead to More Robust and Resilient Systems?"* I Acta Polytechnica Scandinavica Civil engineering and building construction series no. 114, Espoo, Finland, (1999)

FEMA *"Multi Hazard – Identification and Risk Assessment – A Cornerstone of the National Mitigation Strategy"*, Federal Emergency Management Agency, USA, (1997)

Haimes, Y.Y. *"Risk Modeling, Assessment, and Management"* John Wiley & Sons (1998)

Haimes, Y.Y:, Matalas, N.C., Lambert, J.H., Jackson, B.A. & Fellows, F.R. *"Reducing Vulnerability of Water Supply Systems to Attack"* Journal of Infrastructure Systems, vol 4, no 4, American Society of Civil Engineers, (1998).

Haimes, Y.Y., Lambert, J.H. & Kaplan, S. "*Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling"*. Risk Analysis, Vol. 22, No. 2, Blackwell Publishing, (2002).

Hale A. & Hopkins A. "*Issues in the regulation of safety: setting the scene"* in "Changing Regulation", Hale A., Hopkins A., Kirwan B. (eds), Elsevier Science, Oxford, (2002).

Hale A., Heming B., Carthey J. & Kirwan B *"Modelling of safety management systems"*, Safety Science, vol 26, Elsevier, (1997).

HM Treasury *"Management of Risk – A Strategic Overview – With supplement guidance for smaller bodies"* HM Treasury (2001)
http://www.hm-treasury.gov.uk/media//EC612/orange-book.pdf (2003-09-11)

International Electrotechnical Comission, IEC, "*International Standard - Dependabiliy management part 3*: *application guide - section 9 Risk Analysis of technological systems"* (1995).

Kaplan, S. *"The Words of Risk Analysis"* Risk Analysis, Vol 17, No 4, Plenum Press (1997)

Kaplan, S., Haimes, Y.Y. & Garrick, J. *"Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk"* Risk Analysis, Vol 21, No 5, Blackwell Publishers (2001)

KBM *"Risk- och sårbarhetsanalyser – Vägledning för statliga myndigheter"* (2003a).
http://www.krisberedskapsmyndigheten.se/verksamhet/sarbarhet/risk_sarbarhetsana_vagledn_statliga_mynd_rekom_2003-1.pdf (2004-01-09)

KBM *"Samhällets Krisberedskap 2005 Planeringsinriktning"* (2003b).
http://www.krisberedskapsmyndigheten.se/verksamhet/planering/planeringsinriktning_samhallets_krisberedskap_2005.pdf (2004-01-09)

KBM *”Strategi för forskning för samhällets krisberedskap”* (2003c). http://www.krisberedskapsmyndigheten.se/verksamhet/forskning/forskningsstrategi_20030227.pdf (2003-09-10)

KBM *”Basnivå för IT-säkerhet (BITS)”* (2003d). http://www.krisberedskapsmyndigheten.se/verksamhet/information/bas_it-sakerhet_bits_rekomm2003-2.pdf (2004-01-12)

KBM *”IT och sårbarhet – Kritiska beroendeförhållanden i den nationella IT-infrastrukturen”*, (2003e). http://www.krisberedskapsmyndigheten.se/verksamhet/information/it_sarbarhet_2003.pdf (2004-01-12)

Kemikontoret *”Integrerat Ledningssystem för Säkerhet, Hälsa och Miljö – en handbok med rutiner, om SHM-ledningssystem”* Kemikontoret (1997).

Kirwan B. *“A Guide to Practical Human Reliability Assessment.”* Taylor&Francis (1994)

Klinke, A. & Renn, O. *“A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies”* Risk Analysis, Vol 22, No 6, Blackwell Publishers (2002)

Kommunförbundet *”Verksamhetsanalys och säkerhetssamordning – Metod och vägledning”* Svenska Kommunförbundet, (2001).

Livsmedelsverket *”Riskhandbok för dricksvattenförsörjning”* Livsmedelsverket, Uppsala, (1997).

Livsmedelsverket *”Förebyggande åtgärder och hantering av akuta incidenter på dricksvattenområdet – Handbok med checklistor och hänvisningar till publicerade rapporter”* Livsmedelsverket, Uppsala, (2000).

Livsmedelsverket *”Minimikrav på egenkontrollprogram med HACCP”*, Livsmedelsverket, Uppsala (2002).

Livsmedelverket *”Handledning för ökad IT-säkerhet inom dricksvattenområdet”* Livsmedelsverket, Uppsala, (2003).

Magnusson S E, Göransson P, Petersen K, Malmen Y, Hovden J, Harms-Ringdahl L & Akselsson R “*Co-operative Nordic Risk research”* Report 1001, LUCRAM, Lund University Centre for Risk Analysis and Management, Lund. (1999).

Morgan M G & Henrion M *”Uncertainty – A guide to dealing with uncertainty in quantitative risk and policy analysis”* Cambridge University Press, New York (1990).

Morrow B. H. “*Identifying and Mapping Community Vulnerability Disasters”*, 1999, 23 (1):1-18. (1999)

Nicolet-Monnier M *”Integrated Regional Risk Assessment. The situation in Switzerland.*” International Journal of Environment and Pollution. Vol 6, Nos 4-6. Sid 440-462. (1996).

Nieminen Kristofersson, T ”*Krisgrupper och spontant stöd: om insatser efter branden i Göteborg 1998*.” Lund dissertations in social work, Lund: Socialhögskolan, Lunds universitet (2002)

Nilsson, J., Magnusson, S.E., Hallin, P.O. & Lenntorp, B. *“Integrerad regional riskbedömning och riskhantering”* LUCRAM rapport 1002, Lunds Universitet, (2000).

Nilsson, J. *“Introduktion till riskanalysmetoder”*, LTH Brandteknik, Lunds Universitet, rapport 3124, (2003).

NRC, National Research Council *”Making the Nation Safer – The Role of Science and Technology in Counterring Terrorism”* The National Academies Press, Washington (2002).

Office of Government Commerce *“Draft Guidelines on Managing Risk”* (2001). http://www.ogc.gov.uk/sdtoolkit/reference/ogc_library/generic_guidance/risk_hbook.pdf (2004-01-12).

Otway H J& Von Winterfeldt, D: ”*Beyond acceptable risk: on the social acceptability of technologies”* Policy sciences 14, sid 247-256, (1982)

Performance and Innovation Unit, Cabinet Office *“A Futurist’s Toolbox – Methodologies in Futures Work”*, Cabinet Office (2001) http://www.number-10.gov.uk/su/toolbox.pdf (2003-10-27)

Project Management Institute, *“A Guide to the Project Management Body of Knowledge”*, Project Management Institute, Newtown Square, Pennsylvania, USA, (2000).

Reason J. *“Managing the Risks of Organizational Accidents”* Ashgate Publishing Limited (1997).

Renn O: *”The role of risk perception for risk management”* Reliability Engineering and System Safety 59, Elsevier Science Ltd, Northern Ireland, (1998).

Robens Lord. *“Safety and health at work: report of the committee”* HMSO, London, (1972).

Räddningsverket *”Handbok för riskanalys”*, Beställningsnummer U30-626/02 Räddningsverket, Karlstad, (2003).

Räddningsverket m.fl. *”Myndighetsgemensam vägledning Seveso II direktivet”* (2001). http://www.srv.se/funktioner/publish/doklager/dok2438-48.pdf (2003-09-10).

Stirling, A. *”On Science and Precaution in the Management of Technological Risk”* Final report of a project for the EC Forward Studies Unit under auspices of the ESTO Network. Report EUR 19056 EN. Brussels: European Commision (1999)

Strategy Unit, Cabinet office *”Risk: Improving government’s capability to handle risk and uncertainty”* (2002). http://www.number-10.gov.uk/SU/RISK/REPORT/downloads/su-risk.pdf (2003-09-10)

Sundelius, B., Stern, E. & Bynander, F. *Krishantering på svenska – teori och praktik,* Nerenius & Santérus Förlag AB, Stockholm, (1997).

Timmerman P. *"Vulnerability, Resilience and the Collapse of Society"* Institute of Environmental Studies, University of Toronto, Toronto (1981).

US DoE (Department of Energy) "*Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments"* (2001).
http://www.appanet.org/operations/checklist.pdf (2004-01-12).

US DoE (Department of Energy)*"Vulnerability Assessment Methodology – Electric Power Infrastructure"* US DoE, Office of Energy Assurance (2002a)
http://www.esisac.com/publicdocs/assessment_methods/VA.pdf (2004-01-12).

US DoE (Department of Energy) *"Energy Infrastructure Risk Management Checklists for Small and Medium Sized Facilities"* US DoE, Office of Energy Assurance (2002b)
http://www.esisac.com/publicdocs/assessment_methods/Risk_Management_Checklist_Small_Facilities.pdf (2004-01-12).

US EPA (Environmental Protection Agency) "*Instructions to Assist Community Water System in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002"* US EPA, Office of Water (2003).
http://www.epa.gov/safewater/security/util-inst.pdf (2004-01-12).

Watts M.J. & Bohle H.G. *"The space of vulnerability: the causal structure of hunger and famine"* Progress in Human Geography, no 17, pp 43-67 (1993).

Weichselgartner J *"Disaster mitigation: the concept of vulnerability revisited"* i Disaster Prevention and Management, vol 10, number 2, MCB University Press (2001).

ÖCB "*Säkra företagets flöden"* Överstyrelsen för civil beredskap, Solna (1999).

Bilaga 1 Checklistor för utvärdering av riskhanterings- och krishanteringsprocessen

Checklista för utvärdering av riskhanteringsprocessen

Hämtad från Office of Government Commerce (2001) s 29-31.

The checklists provided in the annexes can be used to help to identify those aspects of risk management that are being applied well or those that are not adequately supported. Checklists included are:

A Effective risk management framework and risk process
B Assignment of risk ownership
C Risk identification
D Risk evaluation and assessment of the organisation's willingness to take on risk
E Risk response
F Monitoring and control mechanisms

A: Checklist on effective risk management framework and risk process

- Is there a formal policy on risk? If 'yes', is this clearly documented, endorsed by senior management and communicated to all staff?
- Is there a clear definition of risk that is understood throughout the organisation?
- Is the organisational structure conducive to the management and communication of risk?
- Is a consistent and systematic approach applied to the management of risk at all levels of the organisation?
- Is the organisation demonstrably committed to providing the required level of skills and training to ensure that staff understand and can manage risk effectively?
- Is tolerance of risk understood by managers and applied consistently throughout the organisation?
- Once identified, are risks appropriately monitored and reviewed, at all levels of the organisation?
- Does the organisation's culture support well thought through risk taking and innovation in an appropriate manner?

B: Checklist on assignment of risk ownership:

- Have owners been allocated for all the various parts of the complete risk process?
- Has the full scope of the risks been catered for, e.g., suppliers may be tasked with ownership of assessing and evaluating some risk as part of their contracts?
- Are the various roles and responsibilities associated with ownership well defined?
- Do the individuals who have been allocated ownership actually have the authority and capability to fulfil their responsibilities?
- Have the various roles and responsibilities been communicated and understood?
- Are the nominated owners appropriate?
- In the event of a change is ownership reassessed; and if necessary, can it be quickly and effectively re-allocated?
- Are the differences between benefit and delivery risks clearly understood and do each types of risk have appropriate owners (who are likely to be different)?

C: Checklist on risk identification

- Has a clear policy on the application of a risk-oriented management process and the scope of risks to be addressed been set at the highest level?
- Has the scope been directly linked to the context and objectives that have been set?
- Has this been agreed and clearly communicated from the outset and reviewed regularly to ensure it is still appropriate – that is, strategic objectives linked to that of the programme, the projects and operations?
- Are changes that have been made to the project objectives being fed back into the risk process and linked back to the entries in the risk register?
- Are decisions taken at project level at risk of being potentially flawed, because the scope of risks being assessed is incorrect?
- Does the risk process cater for all different types of risk?
- Has a full, comprehensive set of risks been identified?
- Has a range of appropriate identification approaches been adopted?

D: Checklist on risk evaluation and assessment of the organisation's willingness to take on risk

- Has the level of analysis that is required to support the decision process been agreed from the outset, e.g., start of the project, acquisition lifecycle etc?
- Is there a demonstrable correlation between the amount of time, effort and cost expended in risk analysis to the difficulty in obtaining decisions, resources and funding for risk management etc?
- Is the level of analysis, where possible, commensurate with the level of risk? For example are detailed assessments of probabilities being carried out on threats which are known to have little, or no, impact?
- Is a consistent approach being taken to assessing potential impact and probability?
- Is there a good understanding as to the relationship between the potential impact against the probability of the risk occurring?
- Is risk information required communicated effectively to support the necessary decision making process, in a timely and cost effective manner?
- Is there a clear understanding of the difference between a problem/issue management process and the risk process and ensuring a suitable means of transferring from one to the other?
- Is there an understanding and commitment as to what level of risk is acceptable, i.e. risk tolerance and willingness to adopt risk for a project, and the ability to communicate this? Does this reflect the potential for accruing benefits?
- Are the appropriate skills required to carry out the analysis available?
- Are risks being understated when assessed or evaluated, whether for commercial, political or individual reasons?
- Is there adequate commitment at all levels to the process of analysing and evaluating the threats?
- Is the process of analysing and evaluating the threats sufficiently flexible to be able to respond to rapid types of changes? Recent examples of this are where e-commerce developments have required IT developers, or other parts of the business, such as customer relationship management, human resources, facilities etc to gear up to deliver solution to the 'market' within abnormally tight

timescales. Three months from strategic concept to delivery of the operation seems to have become the norm.

E: Checklist on risk response

- Have the treatment measures recommended been assessed in terms of:
  - costs compared with the anticipated benefits of treating the risk?
  - the range of responses available?
  - the effectiveness in containing the risk or enhancing the opportunity?
- Do the risks have an adequate description and can be fully understood?
- Have the risk been assessed to see which needs tackling first?
- Has the subsequent required treatment been set?
- Has there been a clear allocation of responsibilities and ownership for actions, decisions etc and the required timescales for completion and review?
- Has the information required for communicating been identified, i.e., to whom, where and when and how?
- Is there a mechanism in place for monitoring and reporting on the effectiveness of the actions being undertaken (see monitoring and reporting)?
- Has adequate contingency been planned ?

F: Checklist of monitoring and control mechanisms

- Has appropriate ownership of the status reporting mechanism been achieved (that is, how it will be used, when and by whom as the owners of that process)?
- Has the organisation put in place mechanisms to monitor the adequacy of processes required to ensure that cultural, political and personal pressures do not hinder truthful representation of status of high profile risks?
- Is there confidence in the accuracy of reporting?
- Is the level of commitment to the reporting process adequate or is there a lack of commitment?
- When assessing and reporting effectiveness are the statements made factual rather than speculative?

Checklista för utvärdering av krishanteringsprocessen

Hämtat från CCMD (2003) s 13.

"Questionnaire on Your Organization's Preparedness

In responding to the following questions, managers can assess broadly their organization's capability to respond to crises and emergencies. The questions are intended to identify the strengths and weaknesses of organizations regarding the activities to put forward in the stages of mitigation, preparedness, response, and recovery:

1. Does your organization have a corporate vision for crisis and emergency management? What is it? Does it address the various phases?
2. Has the proper planning been done regarding who will be involved in each of the phases of crisis and emergency management?
3. List the actual capabilities that your organization has in each area, as well as plans to improve your organization's capabilities.
4. On which phase(s) are the majority of your organization's crisis and emergency management efforts concentrated?
5. On which phase(s) is there a shortage of crisis and emergency management efforts?
6. What kind of attention and rewards do people receive when they contribute to each of the phases?
7. Are there phases for which employees' responsibilities and rewards could be increased or improved?
8. How well does your organization plan for all four phases?
9. What barriers keep people from planning all four phases?
10. How could these barriers be overcome?"

Bilaga 2 Kort sammanfattning av den vetenskapliga bakgrunden för att klassificera risktyper, riskevalueringsmetoder och rikshanteringsstrategier

I litteraturen på området existerar en stor mängd ansatser att kategorisera såväl risker som metoder för att evaluera och hantera dem, alla med mer eller mindre skilda utgångspunkter. Huvuddelen av detta avsnitt kommer att bestå av en kortfattad beskrivning av en föreslagen metodik (Klinke & Renn, 2002) för evaluering och klassificering av risker som bas för att välja lämpligast procedur för att förbättra riskhanteringens kvalitet, acceptans och effektivitet. Som en första del av en vägledning för att välja lämplig riskhanteringsstrategi presenteras nio kriterier för riskevaluering, vilka följaktligen inkluderar såväl fysiska som sociala indikatorer. Kriterierna presenteras i tabell bil. 2.1.

Tabell bil. 2.1 Kriterier för att evaluera risker

Kriterium	**Engelsk (ursprunglig) benämning**	**Beskrivning**
Skadans omfattning	Extent of damage	Ofördelaktiga effekter i naturliga enheter såsom dödsfall, skador, produktionsbortfall etc.
Sannolikhet	Probability of occurrence	Bedömning av den relativa frekvensen av en diskret eller kontinuerlig skadefördelning
Obestämbarhet	Incertitude	Övergripande indikator för olika komponenter av osäkerhet
Geografisk omfattning	Ubiquity	Definierar den geografiska spridningen av potentiella skador
Persistens	Persistency	Definierar den tidsmässiga utsträckningen av potentiella skador
Reversibilitet	Reversibility	Beskriver möjligheterna att återställa situationen till hur det var innan skadan inträffade
Fördröjning	Delay effect	Karakteriserar långtidslatens mellan den initierande (orsakande) händelsen och den faktiska effekten av skadan
Rättvisa	Violation of equity	Beskriver diskrepansen mellan de som åtnjuter fördelarna med en viss verksamhet och de som bär riskerna
Mobiliserings-potential	Potential of mobilization	Tolkad som en kränkning av individuella, sociala eller kulturella intressen och värderingar vilket i sin tur genererar sociala konflikter och psykologiska reaktioner hos individer eller grupper som upplever en påtvingad risksituation.

Dessa nio kriterier är således avsedda att ligga till grund för en heltäckande evaluering av den aktuella risken. För att göra denna evaluering över multipla kriterier mer hanterbar ges även ett förslag på klassificering av risker, där klasserna illustreras av väsen från grekisk mytologi. Dessa klasser och kriterier kopplas sedan via ett beslutsträd, se figur bil. 2.1, till lämpliga strategier för hantering.

Bil. 2.1 Riskklasserna

Riskklass: Damokles svärd. Enligt den grekiska mytologin blev Damokles en gång inbjuden till Kungens hov för en bankett. Han var dock tvungen att äta sin måltid under ett rakbladsvasst svärd som hängde i en fin tråd ovanför hans huvud. Risk och möjlighet blev således tätt kopplat för Damokles och Bilden kan lätt överföras till risker med stor katastrofpotential. Riskklassen karakteriseras således huvudsakligen av *kombinationen låg sannolikhet och stor skadeverkan*. Typiska exempel är teknologiska risker exempelvis förknippade med kärnteknisk energi, storskaliga kemikalieanläggningar och dammar.

Riskklass: Cykloper. Den grekiska mytologin talar även om cykloperna, mäktiga jättar som bestraffats genom att få endast ett öga. Med bara ett öga förloras förmågan till perspektivseende, och endast en sida av verkligheten kan uppfattas. För risker tillhörande denna klass är *sannolikheten för den oönskade händelsen mycket osäker medan katastrofpotentialen är hög och relativt välkänd*. Flera naturrisker, såsom jordbävningar, vulkanutbrott, icke periodiska översvämningar och El Nino tillhör denna kategori av risker.

Riskklass: Pythia. De gamla grekerna konsulterade ibland ett av sina orakel i stunder av tvivel och osäkerhet. Det mest kända var oraklet i Delphi med den blinda sierskan Pythia. Pythia drogade sig själv med gaser för att kunna göra förutsägelser och ge råd inför framtiden, vilket dock även ledde till att hennes utsagor alltid var oklara och svårfattliga. Detta innebär att för risker tillhörande klassen Pythia råder *stor osäkerhet avseende såväl sannolikheten för den oönskade händelsen som konsekvensen av den.* Exempel på risker i denna klass är eventuella risker med genmanipulerade livsmedel, möjligheten till plötsliga, icke linjära klimatförändringar etcetera.

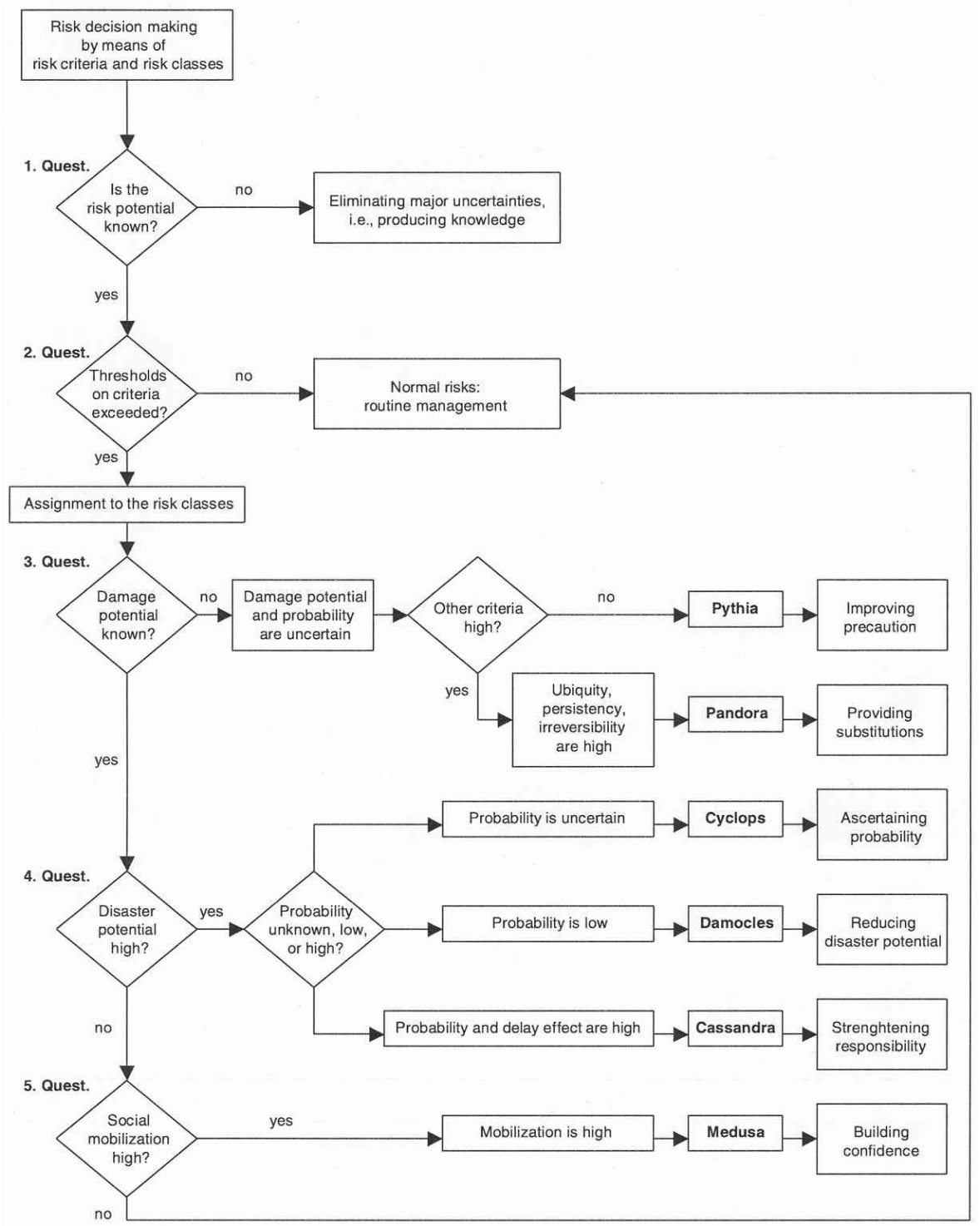
Riskklass: Pandoras ask. I det antika Grekland förklarades många faror med myten om Pandoras ask. Asken fördes till jorden av den vackra Pandora. Olyckligtvis innehöll asken, förutom hopp, många onda ting. Så länge dessa hölls inneslutna i asken fanns ingen anledning till fruktan, man när den öppnades släpptes all den inneboende ondskan lös och orsakade oåterkalleliga och omfattande skador. Denna bild kan överföras till en rad *mänskliga ageranden och ingrepp i naturen vilka leder till omfattande, ibland irreversibla förändringar*. Ett exempel på denna typ av risk är användandet av freoner, vilka anses vara den huvudsakliga orsaken till hål i ozonlagret.

Riskklass: Cassandra. Cassandra, en trojansk sierska, gjorde en korrekt förutsägelse avseende en kommande grekisk seger, men hennes landsmän tog henne inte på allvar. Risker i klassen Cassandra karakteriseras således av att *såväl sannolikheten för en oönskad händelse som effekterna av den är både hög och välkänd, men effekterna kommer inte att visa sig förrän långt efter det att exponeringen inletts*, vilket ofta leder till att denna typ av risker ignoreras eller prioriteras ned. Exempel på sådana fenomen kan vara långsamma klimatförändringar och minskning i biologisk mångfald.

Riskklass: Medusa. Den mytologiska världen i det antika Grekland var fylld av faror som hotade människor, hjältar och de olympiska gudarna. Fantasifiguren Medusa var fruktad eftersom myten sade att den som såg henne skulle förvandlas till sten. På liknande sätt händer det att nya innovationer på olika områden avslås, trots att de ur ett vetenskapligt synsätt inte utgör någon risk, därför att de har vissa karakteristika som gör dem skrämmande eller ovälkomna. Sådana fenomen har en hög potential för social mobilisering. Denna riskklass är endast intressant i de fall det råder stor skillnad mellan hur allmänheten uppfattar risken och hur experterna med hjälp av riskanalys bedömer risken. Ett typiskt exempel är frågan om elektromagnetiska fält.

Som en grund för att evaluera och i förlängningen välja strategi för att hantera risker föreslås en metod för att placera in de riskkällor man har att hantera i de olika klasserna ovan. Detta sker med hjälp av ett beslutsträd, i vilket fem centrala frågor måste besvaras, se figur bil. 2.1.

Bil. 2.1 Beslutsträdet



Figur bil. 2.1 Beslutsträd för att evaluera och klassificera risker (Klinke & Renn, 2002).

För mer detaljerad beskrivning av de olika delarna av beslutsträdet hänvisas till Klinke & Renn (2002). Nedan ges en kortfattad sammanställning av frågeställningarna.

Fråga 1 ”Vet vi något om de huvudsakliga karakteristika för risken?”

Om det är så att vi för den aktuella riskkällan saknar kunskap avseende något av de nio kriterierna ovan, kan vi inte hantera den som om vi hade denna kunskap. Den huvudsakliga uppgiften i detta läge är att säkerställa att kunskap om den okända riskpotentialen genereras.

Fråga 2 ”Överskrider risken på förhand bestämda gränsvärden för ett eller flera av kriterierna?”

Det gäller således att definiera ”gränsvärden” för de olika kriterierna, avsedda att styra huruvida ett ingripande är nödvändigt eller ej. Om inget av dessa gränsvärden överskrids görs bedömningen att riskkällan kan behandlas inom ramen för den rutinmässiga hanteringen på området. Om något av gränsvärdena överskrids blir det nödvändigt att placera in riskkällan i en av de sex klasserna.

Fråga 3 ”Är skadepotentialen känd och kan den beskrivas?”

Om inte skadepotentialen är känd följer även att sannolikheten för ett visst utfall ej kan definieras, vilket innebär att det handlar om klasserna ”Pythia” eller ”Pandoras ask”. Riskklassen ”Pythia” förutsätter att det finns vetenskapliga bevis för samband mellan riskkälla och effekt, men varken skadans omfattning eller sannolikheten kan specificeras. För risker som hamnar i klassen ”Pandoras ask” gäller att endast troliga antaganden om orsakssamband existerar, men inga utförliga bevis. I de fall riskerna bedöms ha en stor geografisk utbredning, lång tidsmässig utsträckning, samt potential för irreversibla effekter påkallas försiktighet. I de fall skadepotentialen är känd och kan beskrivas blir fråga 4 relevant.

Fråga 4 ”Överskrider den bedömda skadepotentialen gränsvärdet för katastrofpotential?”

Om experter bedömer att katastrofpotentialen är hög, men sannolikheten bedöms vara antingen låg eller okänd, passar antingen ”Cykloper” eller ”Damokles svärd” in på beskrivningen. ”Cykloper” karakteriseras av potential för stora skador, emedan sannolikheten för utfallen är osäker. Även ”Damokles” karakteriseras av hög katastrofpotential, men sannolikheten att hotet skall realiseras är liten, ibland minimal. I de fall både skadepotentialen och sannolikheten bedöms vara höga förkastas vanligtvis riskkällan, exempelvis genom förbud. Om det finns en fördröjning mellan den utlösande aktiviteten och den faktiska skadeverkan, leder detta dock ofta till att sådan risker ignoreras. Denna typ av risker hamnar i klassen ”Cassandra”.

Fråga 5 ”Bedöms riskkällan lågt avseende de fysiska kriterierna men högt avseende de sociala?”

I de fall skadepotential, sannolikhet, osäkerhet och andra fysiska kriterier bedöms vara låga är riskkällan oftast inte intressant för vidare hantering. Undantaget är om riskpotentialen väcker oro hos individer, kränker rättvisevärderingar, och /eller har hög potential för social mobilisering hos allmänheten. Denna typ av risker hamnar i klassen ”Medusa”.

Baserat på vilken klass riskkällan bedöms tillhöra ges sedan rekommendationer avseende övergripande hanteringsstrategier.

Bil. 2.3 Tre huvudsakliga grupper av strategier

På liknande sätt som med klassificeringen av risker är det rimligt att skissera en klassificering av generiska riskhanteringsstrategier. Dessa strategier fokuserar på tre huvudsakliga utmaningar vilka karakteriserar hanteringen av riskfrågor i samhället: *komplexitet, osäkerhet* och *oklarhet*.

Komplexitet avser här svårigheten att identifiera och kvantifiera kausala samband mellan en uppsättning av potentiella orsaker och specifika ofördelaktiga effekter. Om hanteringsproblemet karakteriseras av komplexitet, med relativt små inslag av osäkerhet och otydlighet, är det rimligt att låta hanteringen ta sin utgångspunkt i riskanalys, med hanteringsstrategier som kvantitativa mått på tolerabel risk, kostnad-nytta resonemang etcetera.

Osäkerhet skiljer sig från komplexitet. Osäkerhet består av olika komponenter såsom statistisk variation, mätfel och avsaknad av kunskap, vilka alla har det gemensamt att de minskar förtroendet avseende bedömda orsak-verkanssamband. I de fall hanteringsproblemet karakteriseras av osäkerhet blir resiliens, förmåga att hantera oväntade händelser, ledordet för agerandet. De flesta ”försiktighetsbaserade” hanteringsstrategier hamnar i denna kategori. Vid beslutsfattande baserat på hantering av osäkerhet krävs därför mer än input från riskspecialister. Även olika intressenters värderingar, ekonomiska aspekter och sociala utvärderingar måste inkluderas. Det handlar om att hitta en tillfredsställande och rättvis balans mellan kostnaden att vara för försiktig och kostnaden att inte vara tillräckligt försiktig.

Oklarhet betecknar här variationen av (legitima) tolkningar baserade på identiska observationer eller dataanalyser. Flertalet vetenskapliga dispyter inom riskvärderings- och riskhanteringsområdet handlar inte om olikheter avseende metoder, mätningar, dos-responssamband etc. utan om frågan vad allt detta betyder för vår hälsa och miljö. Sådana frågeställningar kan inte lösas varken med vetenskapliga riskanalyser eller genom att bestämma den rätta balansen mellan ”för mycket skydd” och ”otillräckligt skydd”. För att kunna klara av situationer som karakteriseras av oklarhet krävs samtals-/förhandlingsbaserade strategier, där kompromisser och konsensussökande blir ledord.

Bil. 2.3.1 Riskbaserade hanteringsstrategier

Riskklasserna ”Damokles” och ”Cykloper” kräver riskbaserade hanteringsstrategier och bestämmelser. Exempel på verksamheter inom dessa klasser är kärnkraft, stora kemikalieanläggningar, dammar, välkända smittsamma sjukdomar etcetera. Inom riskklassen ”Damokles” är både sannolikheten och skadornas omfattning relativt välkända. Eftersom det är de potentiella konsekvenserna som genererar oro bör hanteringen fokuseras på att minska katastrofpotentialen. Avseende ”Cykloper” är en blandning av riskbaserade och försiktighetsbaserade hanteringsstrategier användbara, eftersom det råder osäkerhet kring sannolikheten att de relativt välkända, stora skadeeffekterna skall realiseras. Strikt ansvar och obligatorisk försäkring kan verka som incitament för de som genererar risken att minska katastrofpotentialen och öka kunskapen för att minska osäkerheterna. Även klassiska tekniska angreppssätt från ”inherent safety”, redundans etc. kan bidra till att minska sårbarheten. Exempel är den barriärmetodik och ”defense in depth” som används bl.a. inom kärnkraftsindustrin.

Bil. 2.3.2 Försiktighetsbaserade hanteringsstrategier

Riskklasserna ”Pythia” och ”Pandora” hamnar inom denna kategori av hanteringsstrategier. Typiska exempel på risker inom dessa klasser är specifika applikationer av genteknologi och ökande växthuseffekt. Gemensamt för dessa risker är att de karakteriseras av relativt stor osäkerhet, vilket leder till att försiktighetsbaserade åtgärder och utveckling av alternativa teknologier blir nödvändiga. Exempel på verktyg för hantering av denna typ av risker är, inneslutning av applikation i tid och rum, övervakning av bieffekter, skapande av ”high-reliability organizations” för att kunna hantera osäkra risker, introducera strikt ansvar etcetera.

Bil. 2.3.3 Samtals-/förhandlingsbaserade hanteringsstrategier

Den tredje kategorin, samtals-/förhandlingsbaserade hanteringsstrategier, är nödvändig i de fall då antingen potentialen för omfattande skador ignoreras till följd av tidsförskjutning mellan orsak och verkan, såsom klimatförändringsfrågan, eller då det omvända inträffar, d.v.s. att vetenskapligt sett ofarliga effekter uppfattas som hot, exempelvis elektromagnetiska fält. Denna typ av risker representeras av ”Cassandra” respektive ”Medusa”. Dessa riskklasser kräver hantering i form av medvetandegörande, förstärkning av förtroende för reglerande instanser, och initiering av kollektiva ansträngningar hos olika institutioner för ett ökat ansvarstagande. Detta är sociala målsättningar som inte kan uppnås av riskexperter och myndigheter för sig själva. I de fall oklarhet är ett påtagligt inslag i riskdebatten krävs samtals-/överläggningsbaserade metoder för beslutsfattande, att klarlägga fakta är inte tillräckligt. Oklara risksituationer kräver allmänhetens (eller den del av allmänheten som påverkas av risken) deltagande i beslutsprocessen.

Bilaga 3 Kortfattad beskrivning av en generell metod att identifiera riskscenarier.

Hierarchical Holographic Modeling (HHM)

HHM utgör en generell metodik att identifiera riskscenarier ur ett mycket brett perspektiv (Haimes et al, 2002, Kaplan et al, 2001), användbar för exempelvis analys av storskaliga komplexa system, såsom tekniska infrastruktursystem. Grundtanken för HHM är att när storskaliga komplexa system, samt övriga faktorer som påverkar funktionen av dessa system, skall modelleras kan detta göras från flera utgångspunkter och perspektiv och troligen leda till fler än en matematisk eller konceptuell modell av systemet. Exempel på sådana utgångspunkter och perspektiv kan vara själva det fysiska systemet, organisatoriska aspekter, externa faktorer etcetera. Avsikten med HHM är att det skall vara möjligt att samla alla dessa modeller och perspektiv under en övergripande ram för att skapa en helhetsbild av vad som skulle kunna få systemet att felfungera.

För att beskriva strukturen i HHM visas i figur bil. 3.1 ett exempel på en hierarkisk holografisk modell över ett vattenförsörjningssystem, med syfte att identifiera riskscenarier (och i förlängningen finna sätt att minska sårbarheten i systemet, se vidare nedan) De 16 olika ”rubrikerna” utgör olika perspektiv på vad som krävs för att systemet skall fungera på det sätt som avses, systemets ”framgångsscenario”. Längre ner i hierarkin inom respektive perspektiv listas sub-komponenter som tillsammans utgör de viktiga elementen i det totala ”framgångsscenariot”. Exempelvis listas under perspektivet ”fysiskt system” hårdvarukomponenterna: rör, pumpar, brunnar/källor, akvedukter, vattenreningsverk samt avloppsreningsverk. För alla dessa sub-komponenter är det möjligt att finna en uppsättning kriterier för framgång, d.v.s. åtgärder, resultat eller som förväntas inträffa som en del i definitionen av systemets framgång.

När systemets ”framgångsscenario” definierats utifrån de skilda perspektiven, är det möjligt att gå in i respektive sub-komponent och börja söka svaret på frågor som: ”vad skulle kunna ske som gör att vi inte uppnår dessa ”framgångskriterier”, eller i linje med AFD: ”om jag ville se till att några av dessa framgångskriterier inte uppnås, hur skulle jag göra då”? På så sätt kommer ett (mycket) stort antal riskscenarier kunna identifieras från flera skilda perspektiv. För att vidare kunna hantera ett så stort antal scenarier behövs en systematisk process att filtrera och rangordna dessa. Detta för att möjliggöra en prioritering av scenarier inför kommande val av hanteringsstrategi. Ett förslag på sådan systematisk process beskrivs utförligt i Haimes et al (2002).

Figur bil. 3.1 återger en hierarkisk holografisk modell över 16 perspektiv som bedöms vara relevanta för möjligheten att stärka vattenförsörjningssystem utsatta för yttre attack (Haimes et al, 1998). Denna modell används som bas för att stärka vattenförsörjningssystem utsatta för yttre attack genom att den möjliggör:

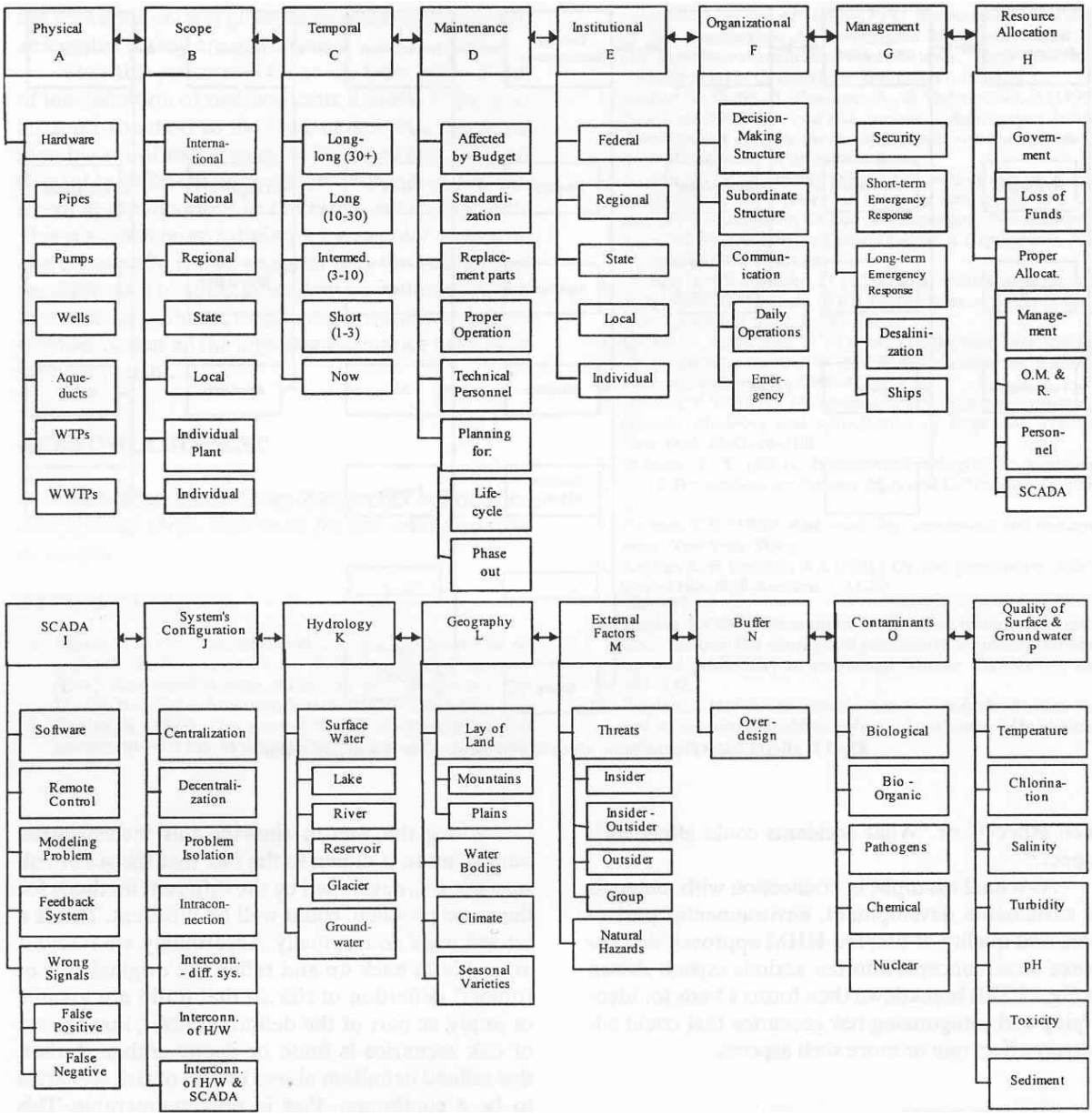
- Ett systematisk angreppssätt att identifiera alla tänkbara riskkällor för systemet, d.v.s. svar på frågorna: vad kan gå fel, och: hur kan man se till att något går fel?

- Bedömning av effektiviteten hos olika åtgärder för att förbättra systemets redundans, robusthet och återhämtningsförmåga. Som exempel kan nämnas underrubriken standardisering (”standardization”) under perspektivet underhåll (”maintenance”).

Genom att standardisera utförandet av viktiga komponenter, exempelvis pumpar med hög kapacitet, kan tiden det tar att byta en pump vid bortfall minskas, och därmed stärks systemets återhämtningsförmåga.

- Identifiering och värdering av alternativa riskhanteringsstrategier.

För en närmare beskrivning av de 16 perspektiven samt åtgärder för att stärka systemet mot yttre angrepp hänvisas till ursprungsartikeln.



Figur bil.3.1. Hierarkisk holografisk modell över olika perspektiv på minskning av sårbarhet i ett vattenförsörjningssystem (Haimes et al, 1998). WTP = water treatment plant; WWTP = waste water treatment plant; O.M. &R.= operation, maintenance and replacement; SCADA = supervisory control and data aquisition; H/W = hardvare

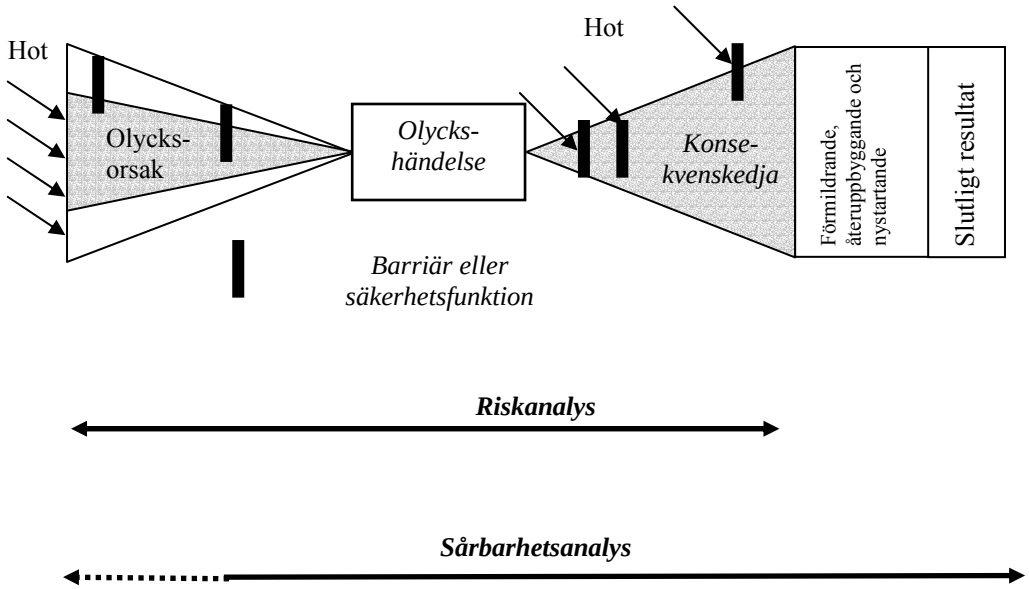
Bilaga 4 Teknisk sårbarhetsanalys

Anm. Hela bilaga 4 är hämtad från Nilsson m.fl. (2000).

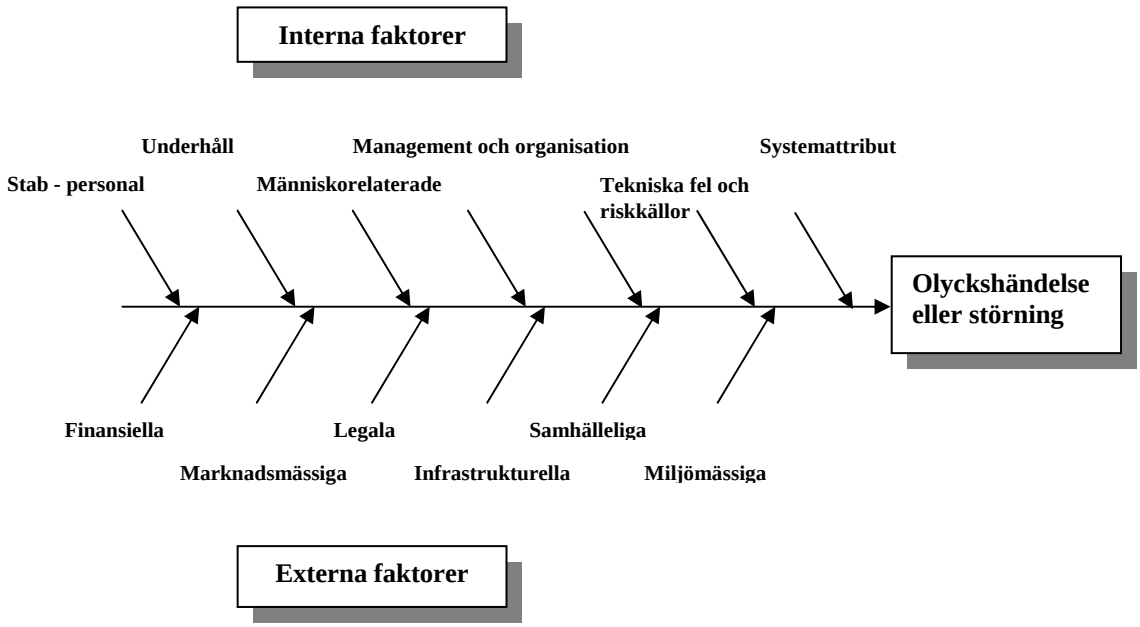
Sårbarhetsanalyserna kan betraktas som släktingar till riskanalyserna och torde liksom dessa kunna delas in i ett spektra från kvalitativa och semi-kvantitativa metoder till kvantitativa. Sårbarhetsanalyser började användas för omkring 15 år sedan, främst för att undersöka sårbarheten i datorsystem och annan informationsteknologi (Einarsson 1999). Sedan dess har sårbarhetsanalyser bl a utnyttjats för att undersöka företagens robusthet och överlevnadsförmåga då de utsätts för olika typer av hot och påfrestningar. På senare tid har emellertid sårbarhetsanalyser också använts för att mäta olika systems sårbarhet i andra sammanhang.

Sårbarhetsanalysen skiljer sig från riskanalysen på flera punkter. En central skillnad är att riskanalysen främst arbetar med de händelser som äger rum inom ett systems fysiska gränser medan sårbarhetsanalysen ser till en öppen systemmodell (Einarsson & Rausand 1998). Riskanalysen undersöker huvudsakligen riskerna från en anläggning mot människor, på eller utanför anläggningen, medan sårbarhetsanalysen ser till interna såväl som externa konsekvenser med särskilt intresse för systemets överlevnadsförmåga. I sårbarhetsanalysen inkluderas därför riskfaktorer av olika slag, såväl inom som utanför systemets fysiska gränser. Dessutom tas i högre grad hänsyn till de skadereducerande faktorer som existerar. Sårbarhetsanalysen anlägger också ett långt tidsperspektiv och fokuserar på ett förlopp från det att en störning inträffar till att ett nytt stabilt tillstånd uppnåtts.

Figur bil.4.1 åskådliggör i grova drag skillnaden mellan omfattningen av en riskanalys och en sårbarhetsanalys. Riskanalysen fokuserar på den konsekvenskedja som kan inträffa till följd av en olycksmässig händelse. De barriärer och säkerhetsfunktioner som är dimensionerade för att begränsa omfattningen av ett skademässigt händelseförlopp studeras främst utifrån tillförlitlighet och kapacitet.



Figur bil.4.1. Skillnaden mellan en sårbarhetsanalys och riskanalys
Källa: Einarsson & Rausand 1998 och Einarsson 1999
Anmärkning: Bilden är en sammanjämkning av olika versioner i de båda källorna samt den text som förklarar dem.



Figur bil.4.2. Interna och externa faktorer som kan leda till en olycksmässig händelse i ett tekniskt system Källa: Einarsson och Rausand 1998

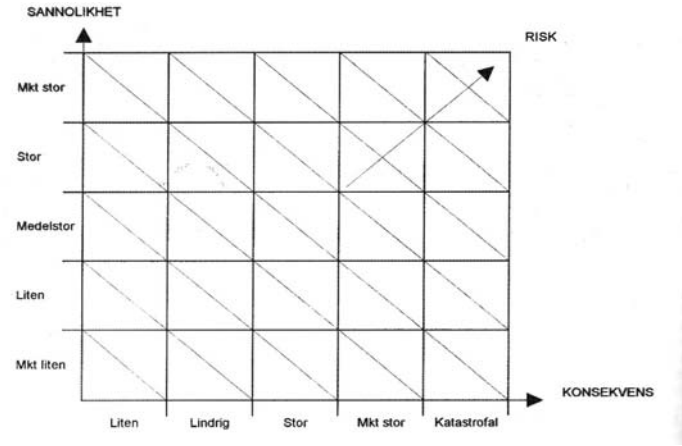
Sårbarhetsanalysen betonar istället systemets överlevnadsförmåga och fokuserar på vilka skadereducerande och återuppbyggande tillgångar som finns för att reducera sårbarheten vid en olyckshändelse.

Ett system påverkas av såväl interna som externa riskfaktorer. I figur bil.4.2 görs en kort översikt över riskfaktorerna i ett industriellt, teknologiskt system. Alla kan inte analogt appliceras på ett socialt, eller ekologiskt system varför uppsättningen riskfaktorer under sådana omständigheter måste modifieras.

Även i riskanalysen anläggs (i varierande grad) en systemsyn. IEC (1995) menar att riskanalysen är en strukturerad process i vilken sannolikheten och omfattningen av skadliga händelser som utgår från en aktivitet, facilitet eller system kan identifieras. Syftet är bl a att klarlägga de viktigaste orsakerna till risker och svaga länkar i systemet, bättre förstå systemet och dess installationer och jämföra risker med de som härstammar från alternativa system eller teknologier. Hänsyn tas även till energi, material och information som är gränsöverskridande samt vilka förhållanden som kan ha en reducerande effekt på konsekvenserna. Det finns alltså en tendens att inom nutida riskanalyser alltmer inkorporera hänsyn till organisatoriska/administrativa faktorer och mänsklig inverkan. På så vis verkar det som att riskanalyser alltmer närmar sig sårbarhetsanalysernas angreppssätt. Det är således viktigt att konstatera att definitionen av riskanalys i figur bil.4.1 endast ser till den snävare och objektorienterade riskanalysen. Gränsen mellan riskanalys och sårbarhetsanalys är m a o diffus och beror på hur riskanalysen definieras. Klart är dock att sårbarhetsanalysen generellt sett kan sägas ta ett brett grepp och att den applicerar en öppen systemsyn.

Sårbarhet i tekniska system

Einarsson och Rausand (1998) har utvecklat en scenariobaserad sårbarhetsanalys för komplexa industriella system och med vars hjälp det är möjligt att kvantifiera konsekvenserna av ett händelseförlopp. Metoden har bl a använts på Island för att undersöka sårbarheten i elsystem. En sådan metod torde emellertid, vilket diskuterats tidigare, även kunna användas för att bedöma sårbarheten i sociala och ekologiska system. Tillvägagångssättet kan ses som en systematisering och vidareutveckling av figur bil.4.3 (sårbarhetsmatris).



Figur bil.4.3 Exempel på riskmatris. Källa ÖCB m.fl. (1998)

Analysen utförs i åtta steg (Einarsson 1999, Einarsson & Rausand 1998):

1. Identifikation av riskkällor m h a checklistor.
2. Identifikation av olycksscenarier. De olika scenarierna kan framställas med hjälp av händelseträd.
3. Uppskattning av scenariernas sannolikhet.
4. Bortgallring av scenarier med låg sannolikhet.
5. Uppskattning av de kvarvarande scenariernas effekter på människor, egendom och affärsliv.
6. Identifikation och utvärdering av skadereducerande resurser.
7. Identifikation och utvärdering av resurser för att återuppbygga och återskapa företaget.
8. Rangordning av scenarier vilket möjliggörs genom att scenarierna kvantifieras. Kvantifieringen bygger på subjektiva värderingar.

Två arbetsblad har utarbetats som ett hjälpmedel. I det första arbetsbladet (se figur bil.4.4) försöker man identifiera de hot som föreligger, vilka scenarion och oönskade effekter de kan leda till och vilka resurser som finns för att möta hoten. I det andra arbetsbladet (se figur bil.4.5) är syftet att grovt kvantifiera och rangordna de olika scenarierna som identifierats i blad 1.

Hot	**Scenario**	**Sannolikt? (ja/nej)**	**Potentiell, omedelbar effekt?**	**Resurser/system/planer för Skadereduktion/ återuppbyggnad/ etc**		**Anmärkning ar**
				Interna	Externa	
(a)	(b)	(c)	(d)	(e)	(f)	(g)

Figur bil.4.4 Arbetsblad nr 1 i Einarsson & Rausands scenariobaserade sårbarhetsanalys
Källa: Einarsson & Rausand 1998

Scenario (brådska)	**Sannolikhet för scenario**	**Konsekvenser av scenario**				**Resurser för skadereduktion/ återuppbyggnad/ etc**		**Summa**
		Påverkan på människa	Miljömässig påverkan	Påverkan på affärsverksamhet	Egendomspåverkan	Interna	Externa	
Nr. och Beskrivning	(4-0)	(4-0)	(4-0)	(4-0)	(4-0)	(4-0)	(4-0)	
1	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
2								
3								

Figur bil.4.5 Arbetsblad nr 2 i Einarsson & Rausands scenariobaserade sårbarhetsanalys
Källa: Einarsson & Rausand 1998

Endast diskreta händelser uppmärksammas i scenarierna. Kontinuerliga och inkrementella förändringar av systemet anses inte relevanta i analysen såvida de inte ger upphov till en specifik händelse. Sannolikheten, konsekvenserna och de interna och externa resurser som finns för att möta scenarierna viktas och den totala konsekvensen av de olika scenarierna erhålles genom enkel summering enligt följande formel (Einarsson & Rausand 1998).

$$C_i = k_h * C_{h,i} + k_e * C_{e,i} + k_b * C_{b,i} + k_p * C_{p,i}$$

Där:
C = konsekvensen av ett scenario och
K = vikt för konsekvensen

Index:
i står för scenario nummer i
h betecknar människor (t ex $C_{h,i}$ = konsekvensen av scenario i med avseende på människor).
e är uttryck för miljö
b betecknar affärslivet
p står för egendom

Den totala rangordningen mellan scenarierna beräknas genom att för varje scenario multiplicera sannolikheten med konsekvensen och sedan dra ifrån (den eventuellt viktade) summan för de skadereducerande resurserna. Scenariot med högst tal är det som betraktas som mest angeläget att åtgärda och hamnar därför högt i prioriteringsordningen. En annan, enklare metod, är att använda en riskmatris (jämför figur bil.4.3).