

# Testpiloten

## Metodmanual

Metod för analys  
av samhällsviktiga  
finansiella tjänster

2007-03-26

## Förord

FSPOS är ett samverkansprojekt inom den finansiella sektorn som bildades år 2005 och leds av Finansinspektionen. Dess syfte är att stärka robustheten och höja beredskapen inom den finansiella sektorn i Sverige.

Arbetsgruppen Kritisk Infrastruktur, som är en arbetsgrupp inom FSPOS, fick under år 2006 i uppdrag att genomföra ett pilotprojekt. Syfte var att testa en lämplig metodik för kartläggning av den infrastruktur som utvalda finansiella samhällsviktiga tjänster är beroende av och att identifiera eventuella sårbarheter i denna infrastruktur, allt i syfte att söka skapa ökad robusthet inom området. Pilotprojektet kallas för "Testpiloten".

Projektet har producerat tre rapporter. Dessa är en Arbetsformsrapport, en Metodrapport och en Resultatrapport. Vissa textavsnitt är gemensamma i de olika rapporterna, eftersom rapporterna är tänkta för olika läsekretsar och skall kunna läsas var för sig.

Denna manual – Metodmanualen – beskriver en generell metod i tre steg för genomförandet av samhällskonsekvensanalys, riskvärdering och kontinuitetsstrategi. Metoden utvecklades parallellt med arbetet att analysera två samhällsviktiga tjänster.

Arbetsgruppen Kritisk Infrastruktur vill rikta ett tack till alla personer i företag och myndigheter som har ställt upp på intervjuer eller på annat sätt bidragit till att dessa rapporter har kunnat produceras.

## Sammanfattning

Det är allmänt känt att organisationer som arbetar på ett aktivt sätt med program för kontinuitetsplanering har bättre förutsättningar att kunna minimera krisers skadliga effekter. Fördelar uppnås bland annat genom förebyggande investeringar i redundans och träning av personal i hantering av oväntade hotfulla situationer. Den förberedda organisationen förmår, tack vare detta, att återta sin leveransverksamhet på ett snabbare och ofta mer kontrollerat sätt än oförberedda organisationer.

Leveranser av samhällsviktiga funktioner utförs vanligtvis i samverkan mellan olika organisationer som är beroende av varandra. Beroendet har gradvis ökat över åren på grund av avreglering av marknader, globalisering, "outsourcing" och utvecklingen av informationsteknologi. I takt med förändringarna har beroendeförhållandena blivit alltmer komplexa så att nya sårbarheter har uppkommit i samhället. Under de senaste trettio åren i en sådan situation är det viktigt för samhället och dess medborgare att säkerställa kontinuiteten i varje länk i kedjan genom att noga följa utvecklingen. Starten för arbetet är gemensamma övergripande analyser av sårbarheter för att sedan kunna identifiera effektiva åtgärder som stärker robustheten hos de deltagande organisationerna.

Samhällets krav avseende kontinuiteten hos en levererande organisation kan sammanfalla med eller avvika från den enskilda organisationens kontinuitetsmål. Det är därför nödvändigt att parterna kommunicerar med varandra på ett stringent och effektivt sätt. För detta krävs en enhetlig metod. Denna metodmanual beskriver en sådan metod. Metoden har kommit att kallas för "Samhällskonsekvensanalys" efter dess första metodsteg. Dessutom ingår två metodsteg till i manualen, ett för riskvärdering och ett för utveckling av kontinuitetsstrategier.

## Innehållsförteckning

Förord.....	2
Sammanfattning .....	3
Innehållsförteckning .....	4
Inledning.....	5
Principer för samhällets krishantering.....	6
Framväxten av kontinuitetsplanering .....	6
Kontinuitet hos samhällsviktiga funktioner.....	7
Erfarenheter av kontinuitetsplanering.....	8
London - terrorattack 7 juli 2005 .....	8
USA & Kanada – elavbrott augusti 2003.....	8
11 september 2001 .....	10
Samhällsperspektivet.....	12
Affärskonsekvensanalys (BIA) och Samhällskonsekvensanalys.....	12
Några viktiga förutsättningar.....	13
Metodik.....	15
Metodsteg 1 - Samhällskonsekvensanalys.....	16
Metodsteg 2 - Riskvärdering.....	23
Metodsteg 3 - Utveckling av kontinuitetsstrategier .....	27
Bilaga 1 Processkarta .....	32

## Inledning

Arbetsgruppen Kritisk Infrastruktur, som är en arbetsgrupp inom FSPOS, fick under år 2006 i uppdrag att genomföra ett pilotprojekt. Syftet var att testa en lämplig metodik för kartläggning av den infrastruktur som utvalda finansiella samhällsviktiga tjänster är beroende av och att identifiera eventuella sårbarheter i denna infrastruktur, allt i syfte att söka skapa ökad robusthet inom området. Pilotprojektet kallas för "Testpiloten".

Projektet har producerat tre rapporter. Dessa är en Arbetsformsrapport, en Metodrapport och en Resultatrapport. Vissa textavsnitt är gemensamma i de olika rapporterna, eftersom rapporterna är tänkta för olika läsekretsar och skall kunna läsas var för sig.

Nedan beskrivs en metod för hur ett strukturerat arbete kan genomföras för att analysera en samhällsviktig tjänst med avseende på dess beroende av infrastruktur. Metoden är framför allt tillämpbar när många organisationer samverkar för att tjänsten ska kunna utföras. I dagens komplexa infrastruktur och samhällskonstruktion är de allra flesta, kanske alla, organisationer beroende av andra för att tjänsten ska kunna levereras. Om en organisation inte längre kan leverera sin del av tjänsten till en annan påverkas denna, som i sin tur påverkar ännu fler organisationer. I samhället är därför helheten, precis som kedjan, inte starkare än dess svagaste länk, det vill säga den enskilda levererande organisationen. En organisations arbete med att säkra sin leveransförmåga är därför av stor vikt inte bara av affärsmässiga skäl, utan även för samhället i stort.<sup>1</sup>

---

<sup>1</sup> Krisberedskapsmyndigheten (2006), Kontinuitetsplanering – en introduktion.

## *Principer för samhällets krishantering*

Tre principer är centrala i samhällets krishanteringssystem: *Ansvarsprincipen*, *likhetsprincipen* och *närhetsprincipen*.<sup>2</sup> Ansvarsprincipen gör gällande att den som har ansvar för en verksamhet under normala förhållanden också ska ha ansvaret under krissituationer. Likhetsprincipen innebär att en verksamhets lokalisering och organisation så långt det är möjligt ska vara den samma såväl under fredstida, normala förhållande som under kris eller annan stor påfrestning. Närhetsprincipen innebär att en kris ska hanteras där den inträffar och av dem som är närmast berörda och ansvariga. Det är därför av stor betydelse att företag planerar för att förbättra förmågan till fortsatt verksamhet vid alla typer av störningar eller händelser samt att kritiska processer kan återstartas inom en för verksamheten och/eller samhället tolerabel tidsrymd.

## *Framväxten av kontinuitetsplanering*

Under senare år har kontinuitetsplanering i ökad utsträckning kommit att stå i fokus som en metod för att säkerställa företags och organisationers leveransförmåga. Kontinuitetsplanering skapar en robusthet i syfte att bättre kunna hantera förluster av delar av, eller hela, den operativa förmågan. Med detta menas att man minskar sin sårbarhet och ökar sin motståndskraft mot olika händelser som kan påverka organisationens mest kritiska verksamhet. Ett finansiellt institut, med ett utvecklat program för kontinuitetsplanering, klarar t ex av att under ett elavbrott med hjälp av reservkraft leverera de tjänster och produkter som är viktigast för företaget och dess kunder samtidigt som de har utvecklade rutiner för att snabbt kunna återgå till normal verksamhet efter avbrottets upphörande.

Kontinuitetsplanering kan bäst beskrivas som en process som består av ett antal komponenter. Dessa komponenter varierar avseende innehåll och benämning inom

---

<sup>2</sup> Krisberedskapsmyndigheten (2006), Att planera inför en pandemi - en vägledning för verksamhetsansvariga, 2006, KBM:s dnr: 0216/2006.

befintliga standarder på området. Det saknas i dagsläget ännu en internationell standard inom kontinuitetsplanering och därmed också en enhetlig terminologi. Dock går viktiga komponenter som affärskonsekvensanalys, riskvärdering och kontinuitetsstrategi att återfinna hos de flesta nationella standarder och riktlinjer inom området.

### *Kontinuitet hos samhällsviktiga funktioner*

Även organisationer inom ramen för privatoffentlig samverkan kan använda delar av metoden för att utforma strategier för de satsningar som behöver göras för att öka robustheten hos en samhällskritisk funktion<sup>3</sup> att klara svåra påfrestningar. Sådana satsningar kan involvera resurser kopplade till såväl enskilda företag med direkt ansvar för att leverera tjänster som stödjer en samhällskritisk funktion som de infrastrukturer denna funktion är kritiskt beroende av.

---

<sup>3</sup> Enligt Krisberedskapsmyndigheten (0253/2005) uppfyller samhällsviktig verksamhet båda eller det ena av villkoren: 1. Ett bortfall av eller svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid kan leda till att en allvarlig kris inträffar i samhället. 2. Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

## Erfarenheter av kontinuitetsplanering

Trots att terror- och naturkatastrofer får de stora rubrikerna är nästan 90 procent av alla kriser i en verksamhet orsakade av händelser som inte får några nyhetsrubriker.<sup>4</sup> Många gånger är dessa kriser orsakade av händelser som gjort det svårt att bedriva affärskritiska processer, så som att leverera tjänster och produkter till kunder. Detta kan i sin tur medföra problem avseende kontinuiteten hos samhällsviktiga funktioner. Genom att sträva efter kontinuitet i dessa verksamheter, oavsett vilka händelser som inträffar, har kontinuitetsplanering som metod väckt ett stort intresse bland företag och andra organisationer runt omkring i världen.

### *London - terrorattack 7 juli 2005*

Ett år efter attackerna mot London den 7 juli 2005 visade en undersökning av 161 företag att arbetet med kontinuitetsplanering framgångsrikt bidragit till upprätthållandet av kritiska verksamheter under och efter krisen. Nästan hälften av de intervjuade företagen aktiverade sina kontinuitetsplaner och 90 procent av dessa var nöjda eller mycket nöjda med effektiviteten i planerna.<sup>5</sup> Erfarenheter som dessa visar att ett effektivt arbete med kontinuitetsplanering skapar en lägre riskprofil för organisationen.

### *USA & Kanada – elavbrott augusti 2003*

I början av augusti 2003 drabbades delar av nordöstra USA och Kanada av ett omfattande elavbrott. Det sammankopplade eldistributionssystemet i nordöstra USA är ett komplext och dynamiskt system som är svårt att överblicka. I detta fall ledde bristande övervakning i samband med ett par simultana fel till kaskadeffekter varvid elförsörjningen i hela regioner slogs ut. På grund av el-bortfallet drabbades även

---

<sup>4</sup> Så kallade "quiet catastrophes", BCI, Business Continuity Institute (2005), Good Practice Guidelines – A framework for Business Continuity Management, [www.thebci.org](http://www.thebci.org).

<sup>5</sup> Både stora och små företag, där knappt 25% av dessa hörde hemma i den finansiella sektorn, 16% i den offentliga sektorn och 7% i energi- och telekomsektorn. ICM and Continuity Centra (2006), July 7th 2005: Looking back for the future, [www.continuitycentral.com](http://www.continuitycentral.com)

andra infrastrukturer av händelsen.<sup>6</sup> Transportsektorn påverkades genom att signalsystem slutade fungera, något som fick konsekvenser för exempelvis tunnelbanesystemet i New York. Vattenförsörjningen i Cleveland och i Detroit påverkades då reningssystemen upphörde att fungera och delar av tillverkningsindustrin i Ohio och Michigan fick stänga ner. Totalt påverkades hela 50 miljoner människor av elavbrottet som också orsakade direkta utgifter på upp till 10 miljarder US dollar.

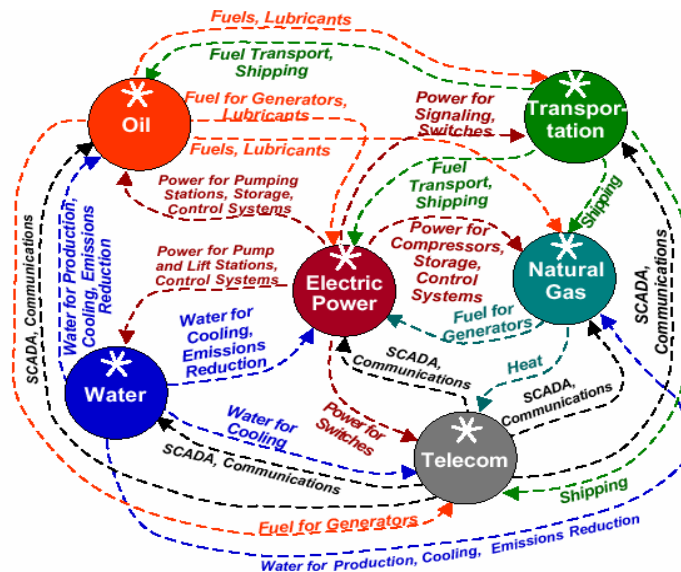
Under elavbrottet visade det sig att enskilda företag och organisationer, som hade tagit höjd för stora elavbrott i sin kontinuitetsplanering kunde fortsätta bedriva sin verksamhet i ringa omfattning, trots gjorda investeringar i reservaggregat och upprättande av planer. Detta berodde på den stora omfattningen av elavbrottet som innebar att de fungerande företagens underleverantörer och kunder i många fall inte kunde verka på grund av deras bristfälliga förberedelser.

Elavbrottet visade att komplexa och kritiska beroendeförhållanden i dagens samhälle skapar ett behov av riktlinjer rörande kontinuitetsplanering och appliceringen därav för att metoden skall vara riktigt effektiv inom exempelvis en sektor eller ett visst geografiskt område.<sup>7</sup> Mot bakgrund av erfarenheter som dessa har en del länder nu utvecklat riktlinjer för kontinuitetsplanering inom kritiska samhällssektorer, så som finans och telekommunikation.

---

<sup>6</sup> R. Zimmerman, C. E. Restrepo (2006), The next step: quantifying infrastructure interdependencies to improve security, *International Journal of Critical Infrastructures* 2006 – Vol 2, No. 2/3 sid 215-230.

<sup>7</sup> Finansinspektionen (2004), *Från elavbrott till 11 September - Kriser, erfarenheter, lärdomar*, [www.finansinspektionen.se](http://www.finansinspektionen.se)



Figur 1. Infrastrukturer är beroende av varandra idag och ingen "snurrar" av sig självt längre.<sup>8</sup>

## 11 september 2001

Terrorattackerna den 11 september 2001 innebar, förutom mycket omfattande förluster av människoliv, att 320 företag inte klarade av att återuppta sina verksamheter och att 135 000 människor förlorade sina jobb. Dock lyckades ett antal organisationer återhämta sig från katastrofen och kunde fortsätta leverera sina tjänster och produkter. Exempelvis kunde företaget Cantor Fitzgerald, som förlorade 658 medarbetare i attacken, återuppta sin verksamhet redan två dagar efter attackerna.

När det södra tornet kollapsade och förstörde kontoret för Deutsche Bank New York, förlorade den tyska bankjätten förbindelsen till USA-marknaderna. Tack vare investeringar i redundanta IT-system, som drevs från Irland, kunde banken ändå bedriva kritisk verksamhet under samma dag som deras byggnad förstördes.<sup>9</sup> Andra

<sup>8</sup> S. Rinaldi, J. Peerenboom, T. Kelly, Complexities in Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, IEEE Control systems Magazine, No. December (2001).

<sup>9</sup> Yossi Sheffi, The Resilient Enterprise, 2005.

exempel på ett snabbt återhämtande av verksamheten i samband med katastrofen är Marsh & McLennan, Morgan Stanley och NY Port Authority.

Ingen av dessa företag kunde förutse scenariot att två flygplan skulle flyga in i båda World Trade Center-tornen och att dessa som en följd härav skulle rasa. Företagen som överlevde katastrofen gjorde det som följd av ett systematiskt arbete som bygger på effektiv, kritisk affärsprocessororienterad hantering av förluster av kritiska resurser såsom lokaler, system och personal – oavsett händelsetyp.<sup>10</sup>

---

<sup>10</sup> Continuity Central, Scenario planning vs resource planning: old school vs new school?, by Saul Midler, MBCI. <http://www.continuitycentral.com/feature0417.htm>

## Samhällsperspektivet

Även samhällsviktiga funktioner och processer som stöds av flera olika företags verksamheter kan analyseras utifrån ett kontinuitetsplaneringsperspektiv. En sådan metodtillämpning kan vara i syfte att generera kunskap om hur en samhällskritisk funktion är beroende av olika infrastrukturer och hur robustheten i funktionen kan ökas. Förutom att söka påverka t ex enskilda finansiella institut att i ökad omfattning arbeta med kontinuitetsplanering, kan organisationer inom ramen för privatoffentlig samverkan använda delar av metoden i syfte att identifiera vilka satsningar som behöver göras för att på ett effektivt sätt stärka t ex den gemensamma återhämtningsförmågan hos en samhällskritisk funktion (tjänst).

### *Affärskonsekvensanalys (BIA) och Samhällskonsekvensanalys*

Inom ramen för kontinuitetsplanering kan enskilda företag genomföra en affärskonsekvensanalys eller, som den också kallas, Business Impact Analysis (BIA). Utgångspunkten här skiljer sig från den i samhällskonsekvensanalysen. I BIA är affärs- eller verksamhetsmål styrande för identifieringen av de processer och aktiviteter som är kritiska för att nå företagets mål. I samhällskonsekvensanalysen är utgångspunkten främst vidmakthållandet av en samhällsviktig funktion. Processer och aktiviteter som är kritiska för sådan funktion stöds vanligtvis av flera olika aktörer. De aktiviteter som analyseras begränsas således till sådana som stödjer den kritiska processen. Dock kan dessa aktiviteter även förväntas vara kritiska för ett enskilt företags affärs- eller verksamhetsmål.

En annan skillnad mellan samhällskonsekvensanalys och affärskonsekvensanalys rör den *kriteriemodell* som utformas i syfte att definiera krav på maximalt tolerabel avbrottstid för en kritisk aktivitet. I affärskonsekvensanalysen finns en tydlig koppling hos kriterierna till det enskilda företagets affärs- eller verksamhetsmål. I

samhällskonsekvensanalysen utformas kriterier utifrån de mål avseende robusthet som definierats för den samhällsviktiga funktion som ska analyseras.

I grund och botten skapar en samhällskonsekvensanalys och efterföljande riskvärdering kännedom om vilka kritiska processer en samhällsviktig funktion har, hur stor toleransen mot störningar är i dessa processer och vilka risker och sårbarheter dessa processer är exponerade mot. Utifrån denna medvetenhet skapas därefter strategier för att säkerställa kontinuiteten av denna samhällsviktiga funktion. I takt med omvärldsförändringar och att kritiska processer, aktiviteter, resurser och infrastruktur utvecklas måste kontinuitetsstrategier uppdateras och på nytt verifieras. Uppgiften ska ses som ett löpande kontinuerligt arbete.

### *Några viktiga förutsättningar*

Innan grunderna i metodiken bakom samhällskonsekvensanalys, riskvärdering och kontinuitetsstrategi beskrivs, behöver några viktiga förutsättningar klargöras för att arbetet ska kunna genomföras inom ramen för en privatoffentlig samverkan.

Legitimitet: De personer som utför metoden behöver ha legitimitet för att få ta del av all relevant information och analysera denna. Sådan legitimitet kan fås från organisationernas ledningar eller från t ex tillsynsmyndigheter.

Uppgiftslämnare: För att kunna jämföra situationen mellan olika institut bör personer som lämnar underlag för analysen från dessa, ha likvärdig bakgrund och ställning i organisationen samt ha nödvändig kompetens och kunskap om t ex den egna organisationens prioriteringar i händelse av störningar. Dessutom bör uppgiftslämnaren vara utsedd av organisationens ledning.

Stöd och engagemang: Det är viktigt att få stöd för arbetet hos organisationens högsta ledning.

Öppenhet och sekretess: Det ligger i samhällskonsekvensanalysens natur att information som samlas in omfattas av sekretess. Deltagarna bör därför underteckna särskilda sekretessförbindelser och det bör finnas färdiga rutiner att ta i bruk för att hantera och presentera informationen. I projektet "Testpiloten" förvarades fysiska dokument i värdeskåp och elektroniska dokument lagrades på väl skyddade servrar. Rapporterna skrevs däremot på ett sätt där enskilda parter situation inte kan härledas. På så sätt kunde rapporterna spridas utan omfattande restriktioner om sekretesshantering.

Korrekthet: Det är viktigt att sammanställa information som samlas in så att det går att avgöra om informationen är korrekt och att regelbundet korskontrollera informationen.

"Helikopterförmåga": Personer som deltar i arbetet bör ha "helikopterförmåga". Med detta avses att deltagarna förmår att se hur en delprocess samverkar med helheten, inte bara i den enskilda processen utan också i företaget, myndigheten och framför allt i samhället, men samtidigt även ha förmåga att tränga in i detaljer på "lägre" nivåer.

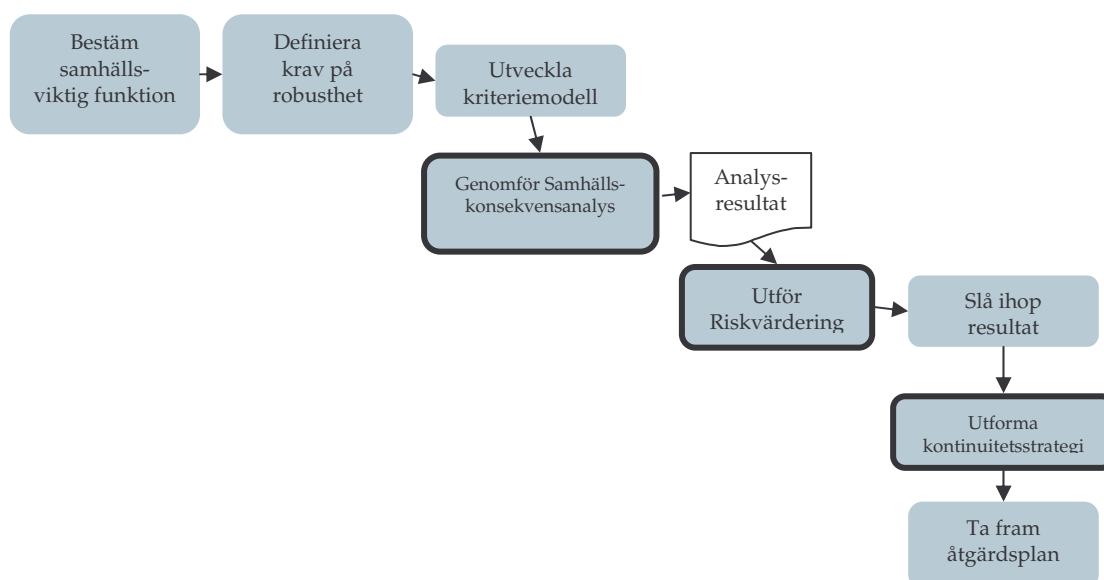
Prioriteringar: Personer som deltar i arbetet bör dela värderingar om att samhällets överlevnad kommer före den egna organisationens.

Tidigare kontinuitetsarbete: Det kan vara en fördel att ta del av och vidareutveckla eventuella befintliga kontinuitetsplaner hos de organisationer som ingår i analysen.

Organisation av arbetet: Stor omsorg bör läggas på hur arbete bäst organiseras. Metoden ger inga anvisningar om detta. Projektet "Testpiloten" arbetade med ett lag utredare som var konsulter. Dessa genomförde intervjuer och sammanställde materialet. Arbetet kan även organiseras på andra sätt.

## Metodik

Den metodik som beskrivs nedan för samhällskonsekvensanalys, riskvärdering och kontinuitetsstrategi bygger i grunden på komponenter som återfinns hos olika nationella standarder på området.<sup>11</sup> Metodiken har dock anpassats för att kunna tillämpas inom ramen för privatoffentlig samverkan med fokus på samhällsviktiga funktioner snarare än ett enskilt företags affärskritiska processer.



Figur 2. Illustrering av nödvändiga steg för att identifiera åtgärder för att stärka kontinuiteten hos en samhällsviktig funktion.

<sup>11</sup> NFPA 1600, BS 25999-1 och HB 221:2004 tillsammans med bidrag från Japanese Industrial Standards Committee och Standards Institution of Israel, ska enligt beslut från den internationella workshopen ISO IWA on Emergency Preparedness, 24-26 april 2006, utgöra grunden i framtagningen av en internationell standard på området.

## *Metodsteg 1 - Samhällskonsekvensanalys*

Att genomföra en samhällskonsekvensanalys handlar om att skapa kunskap om en samhällsviktig funktions kritiska processer, aktiviteter och resurser. Olika aktörer utför i regel olika aktiviteter som stödjer en eller flera samhällskritiska funktioner. Aktiviteterna utförs med hjälp av resurser av olika slag, så som personal, system, utrustning, etc., vars tillgänglighet i sin tur är beroende av kritisk infrastruktur – transporter, el, o dyl.

### **Samhällskonsekvensanalys - sammanfattning**

Projektgruppen menar att en samhällskonsekvensanalys bör innefatta följande moment:

- Identifiera samhällskritiska funktioner (tjänster) inom sektorn.
- Identifiera delprocesser och de aktörer som stödjer leveransen av en samhällskritisk funktion.
- Identifiera de aktiviteter som stödjer de kritiska delprocesserna. Dessa aktiviteter levereras normalt av en enhet, avdelning eller funktion inom en organisation.
- Definiera de krav organisationen måste uppfylla avseende maximalt tolerabel avbrottstid för varje kritisk aktivitet och besvara frågan: Hur lång tid kan leveransen av en kritisk aktivitet ligga nere utan att detta skapar oacceptabla konsekvenser för den samhällskritiska funktionen?
- Identifiera kritiska resurser i form av personal, system, utrustning, tjänster, etc., som stödjer genomförandet av de kritiska aktiviteterna.
- Definiera krav på maximal återhämtningstid för de kritiska resurserna.
- Identifiera kritisk infrastruktur som dessa resurser är beroende av för att kunna fungera.

Samhällskonsekvensanalysen dokumenteras på så kallade "kartor". Ett exempel på en sådan karta som projektet Testpiloten använde återfinns i bilaga 1.

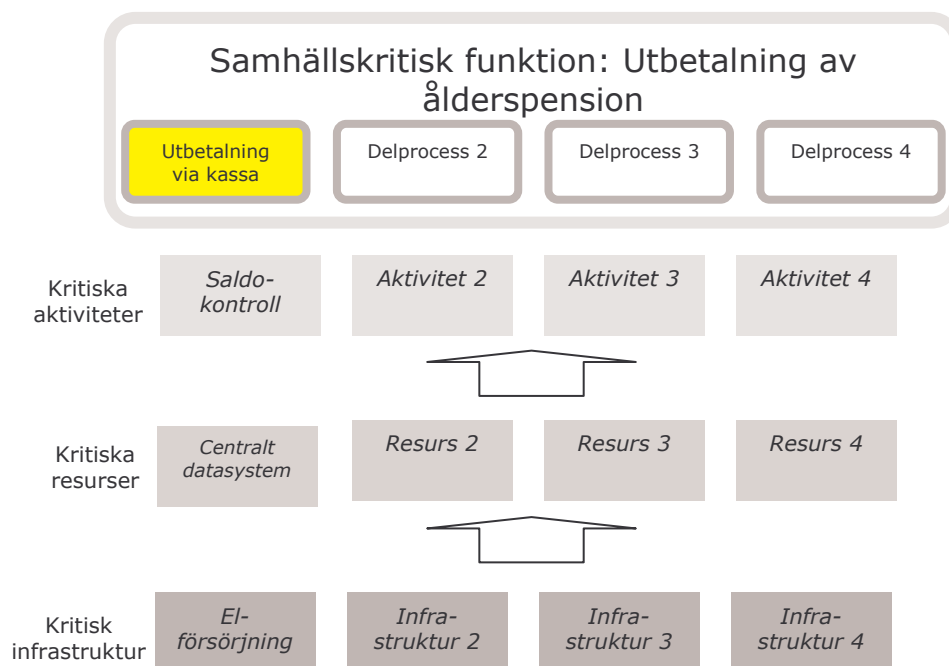
### **Kritiska delprocesser, aktiviteter, resurser och infrastruktur**

En samhällskritisk funktion kan t ex vara utbetalningar från Försäkringskassan (vilken förmedlar 25 procent av svenska folkets hushållskassa). Ett antal aktörer såsom Försäkringskassan, Riksgälden, bankernas huvudkontor och lokala bankkontor, utför aktiviteter som är kritiska för denna funktion. Med "kritiska aktiviteter" avses i samhällskonsekvensanalysen de aktiviteter som måste genomföras för att nödvändiga delprocesser ska fungera, så att den samhällsviktiga funktionen möter de krav på kontinuitet/robusthet som har definierats.<sup>12</sup>

För ett lokalt bankkontor är till exempel uttag av pengar via kassa en delprocess som är kritisk för att kunden ska kunna få ut sin pension. En kritisk aktivitet som stödjer denna delprocess är saldokontroll, se figur 3 nedan. Vissa dagar i månaden, när pension betalas, är det särskilt kritiskt att denna aktivitet fungerar för att den samhällskritiska funktionen inte ska påverkas.

---

<sup>12</sup> Jämför definition av "critical activities" i BS 25999-1:2006 – Business continuity management – Part 1, Code of Practice.



Figur 3. Kartläggning av kritiska delprocesser, aktiviteter, resurser och infrastruktur som stödjer leveransen av en samhällskritisk funktion. Analysresultatet är viktigt för genomförandet av riskvärderingen.

Kunskapen om hur kritiska resurser kan påverka det finansiella institutets förmåga att utföra en kritisk aktivitet är viktig. Med "kritiska resurser" avses här de resurser som måste finnas tillgängliga för att kunna utföra de kritiska aktiviteterna som identifierats.

Resurserna kan finnas internt hos det organisationen eller köpas av en leverantör. En fördjupad beroendeanalys ökar kunskapen om vilka resurser som är kritiska för verksamheten och vilken part som ansvarar för resursen. Kritiska resurser för att utföra saldokontroll i exemplet ovan kan vara det lokala bankkontorets datorer och huvudkontorets centrala datasystem. Dessa är beroende av kritisk infrastruktur, t.ex. elförsörjning, för att fungera. Med "kritisk infrastruktur" avses således den infrastruktur som är nödvändig för tillgängligheten av en kritisk resurs.

Uppdelningen mellan kritiska resurser och kritisk infrastruktur kan variera och styrs av behovet att kunna tydliggöra olika typer av beroenden, se figur 4.

Begrepp	Innebörd
<i>Kritisk aktivitet</i>	De aktiviteter som måste genomföras för att leverera de delprocesser som är nödvändiga för att den samhällsviktiga funktionen ska möta det krav på kontinuitet som definierats.
<i>Kritisk resurs</i>	De resurser i form av personal, system, utrustning, lokaler, leverantörer, etc. som måste finnas tillgängliga för att kunna leverera de kritiska aktiviteterna som identifierats.
<i>Kritisk infrastruktur</i>	Den infrastruktur (t.ex. elförsörjning, kommunikation) som är nödvändig för tillgängligheten hos en kritisk resurs.

Figur 4. Innebörden av centrala begrepp som används i samhällskonsekvensanalysen.

Kartläggningen i steg 1 görs med hjälp av intervjuer och informationen fylls i "kartan" under intervjun. På så sätt kan reflekterande frågor enklare ställas, resultaten direkt visualiseras och eventuella missförstånd undvikas. När kartbilden känns komplett är det dags att genomföra nästa steg, den efterföljande riskvärderingen men först beskrivs ytterligare viktiga komponenter i kartläggningen.

### **Maximalt Tolerabel Avbrottstid (MTO), Återhämtningstid (RTO) och Återhämtningspunkt (RPO)**

Förutom identifieringen och kartläggningen av kritiska processer, aktiviteter, resurser och infrastruktur är det i samhällskonsekvensanalysen även viktigt att definiera maximala tolerabla avbrottstider, eller MTOs (Maximum Tolerable Outages), för varje kritisk aktivitet. Svaret nås genom att ställa frågor. För exemplet ovan ställs till exempel frågan: "Om saldokontroll, oavsett orsak, inte alls kan utföras – hur länge kan avbrottet tolereras utan att det får betydande effekter för delprocessen, d.v.s. utbetalning via kassa?"

För att bedöma effekterna av ett avbrott hos en kritisk aktivitet är en viktig komponent i samhällskonsekvensanalysen framtagandet av en kriteriemodell. Kriteriemodellen är unik och måste utformas utifrån den samhällsviktiga funktion som studeras och de krav på robusthet som har definierats avseende denna. Observera att det är viktigt att samma kriteriemodell tillämpas konsekvent för att definiera samtliga aktiviteters maximalt tolerabla avbrottstider. Figur 5 nedan illustrerar hur en allmängiltig kriteriemodell kan se ut.

EFFEKT PÅ	Låg	Medel	Hög
<b>Kritisk delprocess</b>	Delprocess påverkas utan risk för avbrott	Delprocess påverkas, risk för avbrott liten	Delprocess påverkas, risk för avbrott betydande
<b>Andra kritiska aktiviteter</b>	Annan kritisk aktivitet påverkas, utan risk för avbrott (delprocess)	Annan kritisk aktivitet påverkas, risk för avbrott (delprocess) liten	Annan kritisk aktivitet påverkas, risk för avbrott (delprocess) betydande

Figur 5. Ett exempel på kriteriemodell.

Kunskaper avseende maximal tolerabel avbrottstid (MTO) skapar förutsättningar för att kunna planera för att säkerställa tillgängligheten hos de kritiska aktiviteterna när de verkligen behövs. Avsikten är också att dessa kunskaper ska tjäna som krav avseende återhämtningstider, eller RTOs (Recovery Time Objectives), och

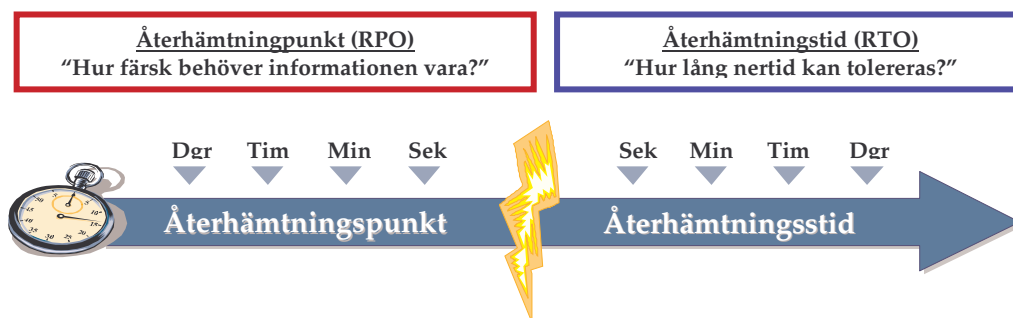
återhämtningstidpunkter, eller RPOs (Recovery Point Objectives) för de resurser som stödjer de kritiska aktiviteterna.<sup>13</sup>



Figur 6. Avbrott i en kritisk aktivitet, här saldokontroll.

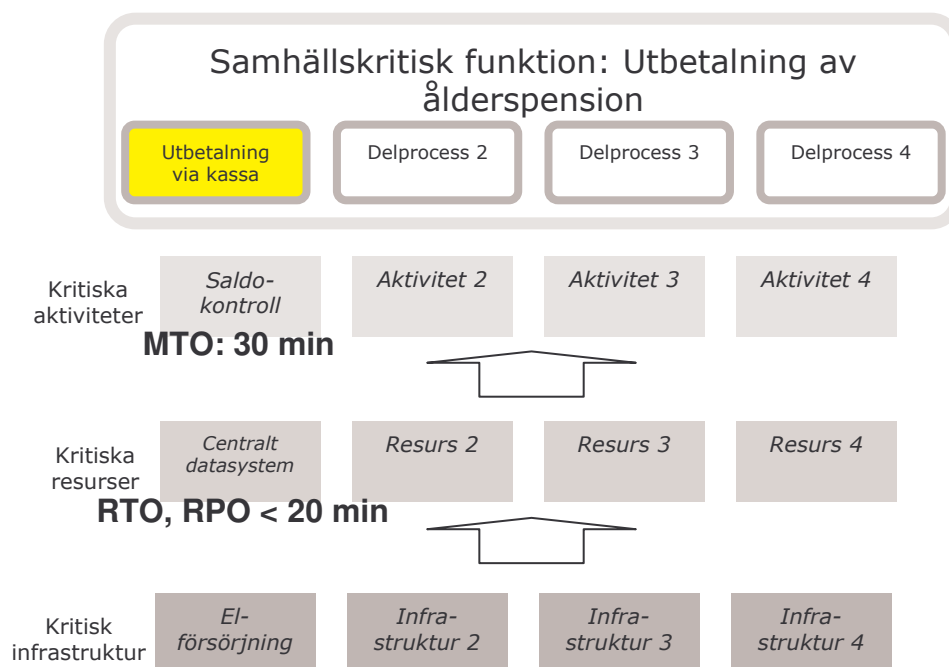
Till exempel kan det vara så att den maximalt tolerabla avbrottstiden för saldokontroll är 30 minuter. Men för att kunna återuppta saldokontrollen inom 30 minuter krävs att informationen i det centrala datasystemet inte är mer än 20 minuter gammal, d.v.s. säkerhetskopior (back-ups) måste kunna tas var 20:e minut. Återhämtningstiden (RPO) för systemet ska därför kravsättas till 20 minuter, under förutsättning att det saknas möjligheter att återskapa aktualiteten hos informationen på annat sätt. Eftersom kravet på återhämtningstid är kortare än kravet på maximalt tolerabel avbrottstid (30 minuter) hos den kritiska aktiviteten, blir detta krav styrande även för återhämtningstiden (RTO) för det centrala datasystemet. Återhämtningstiden ska då kravsättas till mindre än 20 minuter, vilket i sin tur ger indikationer om hur kritisk tillgängligheten på reservkraft för elförsörjningen är för aktiviteten.

<sup>13</sup> Den engelska benämningen för kravet på återhämtningstid är Recovery Time Objective, RTO. Även Recovery Point Objective, RPO, är ett väsentligt krav i detta sammanhang för att säkerställa att färskheten i det för aktiviteten nödvändiga arbetsmaterialet (i datalagrings-sammanhang bör exempelvis krav ställas rörande hur gammal data maximalt får vara för att medge funktionalitet i den kritiska aktiviteten).



Figur 7. Återhämtningstid (RPO) och återhämtningstid (RTO).

Vid hög belastning, t.ex. vid månatliga utbetalningar av ålderspension, är kraven på denna kritiska infrastruktur därför mycket hög, något som inte minst bör reflekteras i exempelvis leveransavtal med elleverantören. Det lokala bankkontoret kan också internt genomföra åtgärder för att bli mindre sårbara vid ett elavbrott, t.ex. investera i reservkraftskapacitet och utveckla rutiner för att möjliggöra utnyttjandet av denna.



Figur 8. Med en maximalt tolerabel avbrottsstid på 30 minuter för saldokontrollen respektive att det centrala datasystemet måste ha en återhämtningstid vid avbrott på mindre än 20 minuter, ställs hårda krav på den kritiska infrastrukturen, i vårt exempel elförsörjningen.

## *Metodsteg 2 - Riskvärdering*

I riskvärderingen identifieras, analyseras och utvärderas olika händelser som kan störa kontinuiteten hos kritiska aktiviteter. Fokus ligger på de kritiska resurserna, det vill säga de resurser som krävs för att leverera den kritiska aktiviteten. Dessa har identifierats i samhällskonsekvensanalysen. Händelser som kan störa kontinuiteten hos kritiska resurser kan vara externa eller interna. De kan exempelvis röra sig om elavbrott, sjukdom, tekniska eller mänskliga fel, sabotage, IT-attacker eller naturkatastrofer. I vissa fall finns sådana händelser beskrivna och värderade i organisationens hotbilda-beskrivning.

### **Fokus på kritiska resurser**

Vid riskvärderingen i detta sammanhang bedöms inte sannolikheten av en enskild händelse utan fokus ligger på en analys av sannolikheten att en kritisk resurs inte kan användas. Det är med andra ord kontinuiteten hos kritiska resurser som står i fokus, allt från extrema oväder till epidemier kan till exempel påverka leveranserna av kritiska komponenter från en underleverantör.

### **Riskvärderingens olika moment**

Riskvärderingen omfattar följande moment:

- Identifiering: Identifiera händelser som kan påverka kontinuiteten hos de kritiska resurser som stöder de kritiska aktiviteterna.
- Analys: Analysera konsekvenser och sannolikhet. Konsekvensen bedöms med hänsyn tagen till kraven på återhämtningstider för varje kritisk resurs som definierats i samhällskonsekvensanalysen. Sannolikheten att händelsen orsakar denna konsekvens ger besked om befintlig robusthet och återhämtningsförmåga vid en viss typ av händelse.

- Aggregering: Efter att riskanalyser genomförts för samtliga kritiska resurser kan resultaten aggregeras i syfte att skapa kunskap om vilka händelser som orsakar de största riskerna för kontinuiteten hos den samhällsviktiga funktionen. Sammanställningen skapar således information om var det finns de största behoven av robusthöjande åtgärder.
- Bedömning: Bedöm vilka risker som inte kan accepteras samt var det finns behov av åtgärder för att reducera dessa risker. Resultatet från riskvärderingen ska tjäna som grund för utformandet av kontinuitetsstrategier (se nästa avsnitt).

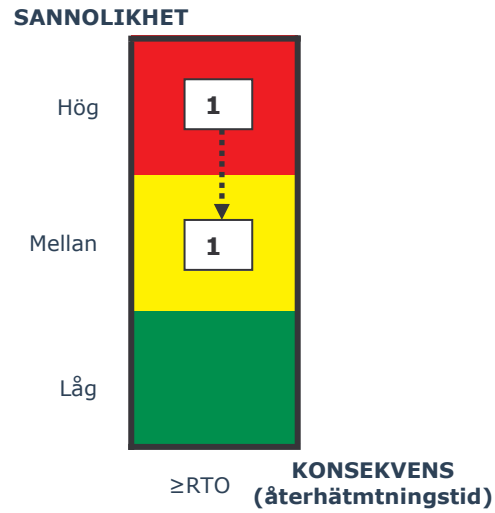
## Genomförande

Då den möjliga konsekvensen av en händelse analyseras ska resultatet från samhällskonsekvensanalysen beaktas. Om konsekvensen innebär att en kritisk resurs, t.ex. ett system, inte fungerar så påverkas en kritisk aktivitet. och att ett avbrott i en kritisk aktivitet efter en viss tid får en icke-tolerabel påverkan på en samhällskritisk funktion. I exemplet ovan medför ett avbrott på mer än 30 minuter i saldokontrollen konsekvenser för utbetalningen av ålderspension. Om t.ex. ett elavbrott med betydande sannolikhet orsakar ett avbrott hos en kritisk resurs, i det här fallet det centrala datasystemet, bör systemets förmåga att återhämta sig inom 20 minuter bedömas. Om bedömningen är den att det t.ex. finns en effektiv lösning för reservkraft på plats och en övergång till denna reservdrift kan ske inom tidsrymden kanske sannolikheten för ett avbrott i det centrala datasystemet som är längre än kravet på återhämtningstid (RTO) är låg. Om det däremot saknas redundans är denna sannolikhet högre och det kan därmed finnas behov att identifiera robusthöjande åtgärder för att reducera risken.

En styrka med denna metod är att efter genomförd riskvärdering kunna visa på de konsekvenser ett avbrott i infrastrukturen får för ett antal samhällsviktiga funktioner. Genom att systematiskt värdera de kritiska resurserna, såsom personal, system, tjänster, leverantörer, etc., utifrån en eller flera händelser, kan besked om robustheten hos en samhällsviktig funktion fås. I exemplet ovan kan det visa sig att ett avbrott i

elförsörjningen redan efter 20 minuter kan medföra ett avbrott i utbetalningen av ålderspension om reservsystem och/eller reservrutiner saknas hos institutet som drabbas.

Vid genomförandet av riskvärderingen kan en riskmodell, som illustreras i figur 10 nedan, användas. Ett ekonomisystem som körs i det centrala datasystemet kan exempelvis vara en kritisk resurs för en samhällsviktig funktion som identifierats med hjälp av samhällskonsekvensanalysen. Systemet kan inte köras utan el. I vårt exempel har kravet på återhämtningstiden för systemet satts till 4 timmar. Institutet har sedan tidigare investerat mycket pengar för att skapa redundans i systemet och det kan vid ett elavbrott drivas med reservkraft som startar momentant vid ett avbrott i den ordinarie elförsörjningen. Tack vare reservkraften är sannolikheten låg för att ett elavbrott ska resultera i ett avbrott som överstiger 4 timmar hos ekonomisystemet. I ett annat exempel kanske det centrala datasystemet (1) saknar reservkraft. Avbrott som vida överstiger kravet på återhämtningstiden för systemet bedöms i det fallet ha en hög sannolikhet och åtgärder bör vidtas förändra situationen, se figur 10.



Figur 10. Om (1) är det centrala datasystemet i exemplet ovan, behöver sannolikheten reduceras och risken "förflyttas" åtminstone från rött till gult område. Detta kan göras genom att initiera olika former av åtgärder, eller "kontinuitetslösningar".

### *Metodsteg 3 - Utveckling av kontinuitetsstrategier*

En strategi bör utformas för att en organisation inom ramen för privatoffentlig samverkan på ett effektivt sätt kan investera i åtgärder för att öka robustheten hos en samhällsviktig funktion, se nästa avsnitt "Behov av kontinuitetsstrategi på samhällsnivå". Åtgärder för att reducera risken exponerad mot det centrala datasystemet (1) i exemplet ovan bör initieras, vilket i matrisen ovan illustreras av en flytt från "rött" till "gult" område. Viktigt är dock att riskvärderingar för den kritiska resursen genomförts för samtliga händelser som kan tänkas påverkas dess kontinuitet innan olika kontinuitetsåtgärder kan beslutas.

#### **Behov av kontinuitetsstrategi på samhällsnivå**

Samhällskonsekvensanalysen och riskvärderingen genererar viktig kunskap om vad som är kritiskt hos de aktörer som har ett ansvar kopplat till leveransen av en samhällskritisk funktion och vilka risker aktörerna är exponerade mot. Information om hur kritisk t.ex. olika infrastrukturer är för den samhällsviktiga funktionen kan systematiskt identifieras. Denna kunskap omsätts i lämpliga strategier för att öka robustheten avseende leveransen av en samhällsviktig funktion.

Det är i första hand den enskilda organisationens ansvar att gardera sig för de risker som föreligger. Det kan göras genom att i avtal med leverantörer ställa krav på tillgänglighet och ersättning vid brister, genom att undvika att göra sig beroende av ständigt fungerande telekommunikationer, genom att anskaffa reservalternativ, genom att anskaffa lokalt skydd mot såväl som fysiskt intrång, dataintrång, etc. Andra alternativ organisationen kan välja kan vara att utveckla alternativa processer eller organisationslösningar.

Strategier som kan beslutas av organisationer inom ramen för privatoffentlig samverkan, eller för ett sektorsövergripande samarbete, kan vara att med samlad kraft verka för att ställa ökade krav på leverantörer av kritisk infrastruktur, t.ex. el och telekommunikation, avseende leveransförmåga och återhämtningstider vid avbrott. Andra strategier kan vara att samordna och hitta gemensamma lösningar för att stärka återhämtningsförmågan hos de organisationer som levererar kritiska aktiviteter för en samhällsviktig funktion. Sådana strategier kan t.ex. vara att hålla gemensamma lokaler för reservdrift, gemensamma ramavtal avseende inköp av reservkraftsaggregat som klarar nödvändig försörjning av prioriterade kritiska resurser, gemensam planering avseende dieselförsörjning vid längre avbrott, harmoniserade reserv- och återgångsrutiner, etc.

### **Hög robusthet genom redundans och flexibilitet**

En kontinuitetsstrategi beskriver i regel hur en organisation avser uppnå kontinuitet inom de för verksamheten viktigaste områdena. En hög robusthet avseende leveranser av kritiska aktiviteter kan fås såväl genom ökad flexibilitet som ökad redundans.

Redundans innebär att det finns reservalternativ för kritiska resurser. Dessa kan användas i händelse av ett avbrott. Vanliga former av redundans är att ha flera datasystem som reserv, reservkraftsaggregat för elförsörjning, lagerbuffertar av kritiska komponenter, utnyttjande av multipla leverantörer av kritiska tjänster och produkter, etc. Sådana lösningar kan vara nödvändiga och framgångsrika i en viss utsträckning. Dock medför investeringar i redundans ofta kostnader utan tydlig avkastningspotential bortsett från vid ett eventuellt avbrott hos kritiska resurser. Det kan därför vara svårt att motivera sådana investeringar i extra kapacitet hos organisationen som drivs av att kontinuerligt öka kvaliteten, effektiviteten och lönsamheten i verksamheten. Det kan i bästa fall ses som ett "nödvändigt ont", en

riskförsäkring.<sup>14</sup> Det är därför viktigt att kunna motivera nödvändiga investeringar i redundanta lösningar genom att analysera den effekt en lösning har för återhämtningstiden hos en kritisk resurs och att kunna visa på den reducering av kostnader som lösningen skulle innebära vid ett avbrott. Här kan organisationer inom ramen för privatoffentlig samverkan spela en viktig roll. Investeringar som bedöms vara nödvändiga för att öka robustheten hos en samhällsviktig funktion, men som av skäl som beskrivits ovan inte en enskild organisation har förmåga att fatta beslut om, kan legitimeras utifrån de mål som den gemensamma organisationen för privatoffentlig samverkan arbetar mot.

Operativ flexibilitet kan också öka robustheten och förmågan hos aktörer att snabbt agera i händelse av ett avbrott i verksamheten. Här handlar det om att utveckla företagets skicklighet snarare än kapacitet, vilket kan vara svårare än att ordna extra lager, fler leverantörer, eller extra IT-kapacitet. Åtgärder för att öka flexibiliteten kan innebära fundamentala förändringar för hela verksamheten och relationer med leverantörer. Åtgärderna kan involvera nära partnerskap med leverantörer som kan kallas in för att hjälpa till vid ett avbrott i verksamheten och flexibla kontrakt som tillåter snabba ändringar avseende kvantitet och leveranstider. Det kan också handla om att en organisation t ex rekryterar personer med bred kompetens eller utvecklar en sådan hos befintlig personal. Sådana åtgärder gör det möjligt för organisationen att snabbt kunna förflytta en person från en arbetsuppgift till en annan.

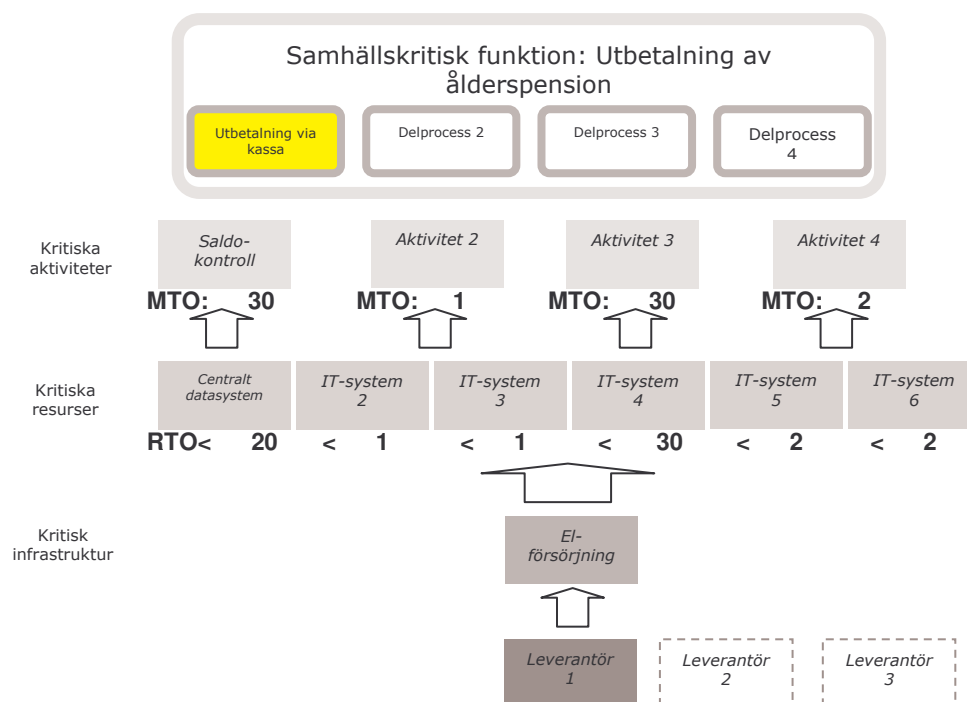
### **Åtgärder inom ramen för privatoffentlig samverkan**

I det tidigare exemplet visar det sig att alla fyra delprocesser som stöder utbetalningen av ålderspension är kritiskt beroende av elförsörjning. Återhämtningstiderna (RTO) som definierats i samhällskonsekvensanalysen för de kritiska resurserna - det centrala datasystemet och fem andra IT-system - varierar mellan 20 minuter och 2 timmar. De finansiella instituten som ansvarar för de

---

<sup>14</sup> Se även Yossi Sheffi, *The Resilient Enterprise*, 2005.

kritiska resurserna använder kanske samma elleverantör, vars kapacitet i samband med en störning inte räcker till. Effekten kan då bli att de maximala tolerabla avbrottstiderna överskrids, se figur 12 nedan. I en sådan situation kan en privat-offentlig strategi vara att förmå parterna att välja olika elleverantörer.



Figur 12. De kritiska resurser som stödjer utbetalningen av ålderspension är samtliga beroende av en och samma elleverantör. En strategi kan vara att öka redundansen genom att välja olika leverantörer som klarar att försörja resurserna med el utifrån de krav som ställs på återhämtningstider (RTO).

Kunskaper från samhällskonsekvensanalysen och riskvärderingen skapar förutsättningar att utveckla, optimera och tydliggöra en kontinuitetsstrategi. Resultatet från riskvärderingen kan t.ex. visa att de verkliga riskerna mot en samhällsviktig funktion handlar om bristen på viktig kompetens. En strategi med fokus på att skapa redundant försörjning från kritisk infrastruktur, t.ex. elförsörjning, kommer inte att hantera denna risk. Istället kanske fokus bör ligga på att underlätta kompetensförsörjningen hos olika aktörer och att skapa gemensamma rutiner för att undvika eller hantera personalbortfall vid t.ex. en epidemi.

Åtgärder för att öka förmågan hos aktörer att leverera aktiviteter i syfte att öka kontinuiteten hos samhällskritiska funktioner behöver inte komma till stånd på rent kommersiella grunder. Ambitionen kan vara att genom partnerskap nå uppgörelser om t ex samfinansiering mellan staten och enskilda aktörer om åtgärder av värde för samhällssäkerheten.

## Bilaga 1 Processkarta

Bifogad processkarta användes av projektet "Testpiloten"

