RIKSREVISIONEN

RiR 2007:28

Krisberedskap i betalningssystemet

Tekniska hot och risker

ISBN 978 91 7086 130 7
RiR 2007:28
Tryck: Riksdagstryckeriet, Stockholm 2007

Till regeringen
Finansdepartementet
Försvarsdepartementet
Justitiedepartementet
Näringsdepartementet
Socialdepartementet

Datum: 2007-12-10
Dnr: 38-2007-1487

Krisberedskap i betalningssystemet – tekniska hot och risker

Riksrevisionen har granskat regeringens och ansvariga myndigheters insatser för att förebygga och hantera tekniska hot och risker i det centrala betalningssystemet. Resultatet av granskningen redovisas i denna granskningsrapport.

Företrädare för Finansdepartementet och de granskade myndigheterna har fått tillfälle att faktagranska och i övrigt lämna synpunkter på underlag och utkast till slutrapport.

Rapporten överlämnas till regeringen i enlighet med 9 § lagen (2002:1022) om revision av statlig verksamhet m.m. Rapporten överlämnas samtidigt till Riksrevisionens styrelse. Rapporten överlämnas också för kännedom till berörda myndigheter.

Riksrevisor *Eva Lindström* har beslutat i detta ärende. Revisionsdirektör *Eero Marttinen* har varit föredragande. Revisionsdirektör *Claes Isander*, revisionsdirektör *Pierre Gunnarsson* och revisor *Kim Lundmark* har medverkat vid den slutliga handläggningen.

Eva Lindström

Eero Marttinen

För kännedom:
Riksbanken
Finansinspektionen
Riksgälden
Försäkringskassan
Post- och telestyrelsen
Försvarets radioanstalt
Krisberedskapsmyndigheten

Innehåll

Sammanfattning

Utgångspunkter för granskningen

Riksrevisionen har granskat krisberedskapen mot tekniska hot och risker i det centrala betalningssystemet. Vi har utgått från sådana allvarliga el-, tele- och IT-störningar som kan leda till att betalningar inte kan ske och att stora delar av den ekonomiska aktiviteten stannar av.

I granskningen bedömer Riksrevisionen om regeringens och myndigheternas samlade insatser för att förebygga och hantera allvarliga tekniska störningar i betalningssystemet är tillräckliga.

Sannolikheten för att allvarliga tekniska störningar ska inträffa bedöms inte av Riksrevisionen. Hittills har Sverige varit förskonat från en allvarlig störning i det centrala betalningssystemet med svåra konsekvenser för samhället. Betalningssystemet drabbas dock ofta av olika tekniska incidenter.

Riksrevisionens övergripande slutsatser

Riksrevisionen har noterat att den finansiella sektorns aktiviteter när det gäller krisberedskap har utvecklats under senare år. Samtliga granskade myndigheter är engagerade i arbetet och avsätter i varierande omfattning tid och resurser för krishantering. En frivillig samverkan mellan myndigheter och näringsliv har etablerats. Riksrevisionen bedömer dock att statens åtgärder för att förebygga och hantera allvarliga tekniska störningar i betalningssystemet inte är tillräckliga.

Riksrevisionen anser att varken regeringen eller myndigheterna har tillräckliga underlag för att kunna bedöma om vidtagna åtgärder räcker för att *förebygga* allvarliga el-, tele- och IT-störningar i det centrala betalningssystemet. Det finns brister såväl i myndigheternas risk- och sårbarhetsanalyser på området, som i deras tillsyn och uppföljning. Inte heller har man tillräckligt analyserat vad omfattande tekniska störningar skulle kosta samhället. Vidare kan inte regeringen sammanställa en nationell bild av samhällets krishanteringsförmåga, eftersom hanteringen av den information som finns inte är tillräckligt väl organiserad. Nuvarande underlag uppfyller inte heller krisberedskapsförordningens krav. Ett sådant underlag borde bedöma san-

nolikheter för och konsekvenser av tänkbara händelser. Regeringen har inte heller fastställt vilka grundläggande säkerhetskrav som betalningssystemet och dess infrastruktur ska uppfylla eller hur uthålligt systemet måste vara. Regeringen har därför ingen norm att utgå ifrån eller tillräckligt underlag för att bedöma om skyddsåtgärderna och betalningssystemets robusthet är rimliga i förhållande till samhällets kostnader för omfattande betalningsavbrott.

Riksrevisionen bedömer att statens åtgärder inte heller räcker för att *hantera* allvarliga el-, tele- och IT-störningar i betalningssystemet om de inträffar. Granskningen visar att myndigheterna och privata aktörer inte har förberett sig tillräckligt för att kunna begränsa skadorna för medborgare och samhälle av en allvarlig störning. Det finns brister i den krisplanering och de övningar som genomförts. Dessutom är ansvarsfördelningen mellan aktörer för operativ hantering oklar i vissa avseenden. Ingen myndighet har fått ett entydigt övergripande ansvar för att leda, planera, organisera samverkan av och följa upp krisberedskapsåtgärder inom betalningssystemet. Det statliga ansvaret för informationssäkerhet och incidenthantering inom den finansiella sektorn är också uppsplittrat mellan flera myndigheter. Inte heller har regeringen beslutat att funktionen ”Tjänsteman i beredskap” ska finnas inom den finansiella sektorn[1]. En sådan funktion har beslutats inom många andra samhällssektorer där en god förmåga att hantera kriser är av stor vikt.

Riksrevisionen anser därför att regeringen och myndigheterna inte kan bedöma om rimliga åtgärder har vidtagits inom betalningssystemet för att förebygga kriser. Riksrevisionen bedömer av nämnda skäl att förmågan att hantera en allvarlig kris inom detta samhällsviktiga område är bristfällig.

Riksrevisionens särskilda slutsatser och rekommendationer

Regeringens mål och krav är otydliga

Riksrevisionen anser att det finns en otydlighet i målbilden som beror på att regeringen inte fastställt krav på grundläggande säkerhet och uthållighet i betalningssystemet. Detta kan bidra till såväl onödiga investeringar som uteblivna investeringar i säkerhetsåtgärder hos ansvariga myndigheter och företag.

Riksrevisionen rekommenderar därför regeringen att fastställa vilka grundläggande säkerhetskrav som ska gälla för betalningssystemet och dess nödvändiga infrastruktur. Regeringen bör också fastställa hur uthålligt betalningssystemet måste vara.

1 En ”Tjänsteman i beredskap” har enligt krisberedskapsförordningen (2006:942) i uppgift att initiera och samordna det inledande arbetet för att upptäcka, verifiera, larma och informera vid allvarliga kriser.

Ansvarsfördelning och samverkan har svagheter

Staten ansvarar ytterst för att betalningssystemet fungerar vid en kris. Ett dussintal myndigheter inom fem departementsområden samt Riksbanken har ansvar och uppgifter för krisberedskapen inom detta system. Ingen myndighet anser sig ha ett övergripande och samlat ansvar för att leda, planera, organisera samverkan av och följa upp krisberedskapen. Det är oklart om någon myndighet med stöd av lag kan begära ut underlag av alla andra myndigheter som verkar inom betalningssystemet. Dessutom finns inget tydligt utpekat ansvar för samordning av IT-säkerhetsarbete och incidentövervakning. Sekretessproblem försvårar samarbete mellan myndigheter och näringsliv. Myndigheternas samverkan försvåras även av otydliga mål och uppgifter. Dessutom gäller inte krisberedskapsförordningen för Riksbanken. Förordningar gäller bara för myndigheter under regeringen.

Riksrevisionen rekommenderar därför regeringen att fastställa vilken myndighet, exempelvis Finansinspektionen, som har det övergripande krisberedskapsansvaret för betalningssystemet och incidentbevakning samt att föreslå riksdagen i vilka avseenden Riksbanken ska ha ansvar för krisberedskapen. Regeringen bör även precisera samverkansområdenas arbete och sammansättning.

Riksrevisionen vill också fästa riksdagens uppmärksamhet vid behovet av att överväga en ändring av lagen (1988:1385) om Sveriges riksbank i syfte att bestämmelserna i förordningen (2006:942) om krisberedskap och höjd beredskap ska gälla för Riksbanken.

Regeringen och myndigheterna har inte bedömt risker och sårbarheter inom betalningssystemet som helhet

Varken regeringen, Riksbanken eller myndigheterna sammanställer en nationsövergripande analys av hot, sårbarheter och konsekvenser av omfattande tekniska störningar i betalningssystemet. Metoderna för risk- och sårbarhetsanalyser är inte enhetliga, och analyserna uppfyller inte beredskapsförordningens krav. Riksrevisionen anser därför att de förebyggande åtgärder som ansvariga myndigheter och institut har vidtagit inte säkert är tillräckliga för att kunna hindra omfattande skador för medborgare, företag och samhälle.

Riksrevisionen rekommenderar därför regeringen att säkerställa att analyser av risker och sårbarheter i hela det centrala betalningssystemet genomförs och ställs samman. Dessa analyser bör uppfylla krisberedskapsförordningens krav. Regeringen bör också se över sekretessregler och överväga att ge en myndighet föreskriftsrätt över hur risk- och sårbarhetsanalyserna ska utformas och följas upp.

Även granskade myndigheter ska enligt Riksrevisionen i sitt arbete med risk- och sårbarhetsanalyser uppfylla krisberedskapsförordningens krav. Riksgälden ska exempelvis se till att analysen täcker myndighetens ansvarsområde, det vill säga det statliga betalningssystemet i sin helhet.

Regeringens och myndigheternas förberedelser för att hantera en allvarlig störning är inte tillräckliga

En allvarlig teknisk störning i det centrala betalningssystemet kommer att kräva snabba insatser från samtliga granskade myndigheter och från banker och infrastrukturföretag. Det är dock inte säkert att dessa aktörer skulle fungera tillsammans vid en kris. Det finns ingen förberedd ledningsorganisation eller ledningscentral. Inte heller finns funktionen ”Tjänsteman i beredskap” etablerad inom den finansiella sektorn. Ingen av myndigheterna har det ledande ansvaret, och deras krisplaner avser i första hand den egna organisationen. Regeringskansliet har heller aldrig krisövat allvarliga tekniska störningar tillsammans med betalningssystemets aktörer.

Riksrevisionen rekommenderar regeringen att se över hur aktörerna behöver förbereda sig för en akut allvarlig störning i betalningssystemet. Bland annat behöver en långsiktig strategi för gemensamma övningar utarbetas och funktionen ”Tjänsteman i beredskap” etableras inom den finansiella sektorn. Regeringen bör också se över ledningsansvaret för krisförberedelserna och behovet av en förberedd gemensam ledningsorganisation och en central ledningsplats inom sektorn.

Regeringen följer inte upp krisberedskapen

Riksrevisionen kan konstatera att varken regeringen eller myndigheterna gör någon samlad uppföljning av krisberedskapen inom betalningssystemet. Regeringskansliet har heller ingen central mottagare för all krisberedskapsinformation som kan röra betalningssystemet. Det är också oklart i vilken grad Regeringskanslets nya enhet för krishantering kommer att hantera kriser inom betalningssystemet. Dessutom återges sällan väsentliga resultat av tillsynen när myndigheterna rapporterar om risker och sårbarheter. Denna redovisning är också i sig relativt knapphändig. Tillsynsmyndigheterna inspekterar inte heller på plats betalningssystemets underliggande tekniska infrastruktur. Därför kan de inte kontrollera att de finansiella institutionerna har gjort relevanta risk- och sårbarhetsbedömningar eller har fungerande skyddsåtgärder.

Eftersom Regeringskansliet i dag inte samordnar informationen och eftersom tillsynen är begränsad bedömer Riksrevisionen att regering och riksdag har svårt att få en heltäckande bild av beredskapen i det centrala betalningssystemet. Det är också svårt att jämföra myndigheternas skydds-

åtgärder och bedömningar mellan olika år. Om regering och riksdag har en felaktig bild av krisberedskapen inom betalningssystemet riskerar de att prioritera felaktigt, investera ineffektivt i förebyggande åtgärder eller investera för lite i säkerhetsåtgärder.

Riksrevisionen rekommenderar regeringen att se över hur krisberedskapen inom betalningssystemet följs upp. Här ingår att utse en central samordnare för all information om betalningssystemets krisberedskap och att kräva att myndigheterna återrapporterar all väsentlig information. Då blir det möjligt att göra en samlad analys av krisberedskapen inom betalningssystemet. Regeringen bör också se över tillsynen inom detta system. Här ingår att undersöka vilken teknisk kompetens som behövs, om föreskrifter behövs och hur sanktioner ska utövas samt hur myndigheterna bör redovisa resultatet av tillsynen.

Riksrevisionen rekommenderar också Riksbanken, Finansinspektionen och Post- och telestyrelse att via inspektioner på plats och stickprov faktiskt kontrollerar att bankerna och infrastrukturföretagen har infört de skyddsåtgärder man säger sig ha och att kontrollsystemet faktiskt fungerar som det är tänkt. Riksrevisionen anser också att Finansinspektionen bör använda sin föreskriftsrätt och sina sanktionsmöjligheter så att brister i krisberedskapen och regelbrott får konsekvenser för instituten och så att möjligheter skapas att få prövat i domstol hur långt skyldigheten enligt gällande lagar sträcker sig hos bankerna i principiellt viktiga fall.

Konsekvenser av identifierade sårbarheter och brister

Riksrevisionen bedömer att de brister som framkommit i granskningen kan leda till betydligt allvarligare skador för samhälle, företag och medborgare än nödvändigt vid ett eventuellt haveri i betalningssystemet. Det går inte att utesluta att ett avbrott i försörjningen av el, tele och IT till betalningssystemets kärna eller funktionsstörningar i systemet av andra orsaker till exempel kan hindra att stora betalningar mellan bankerna avvecklas. Om inte reservförfaranden hos centrala aktörer fungerar kommer sektorn efter några timmar att uppleva likviditetsstörningar, och deras kunder kommer inte att kunna genomföra normala bankfunktioner såsom att lösa in lån eller göra fastighetsaffärer och företagsköp. Värdepappershandeln kommer också att drabbas och betalningar av utlandskulden eller betalningar som myndigheter behöver göra kan inte ske. Därtill kommer ett antal andra följdverkningar.

En allvarlig el-, tele- eller IT-störning kan också göra det omöjligt för medborgarna att ta ut kontanter, girera eller betala med kort. Om inte betalningar kan göras går det inte heller enligt Riksrevisionen att utesluta att förtroendet för det finansiella systemet skadas. Det kan i sin tur få långsiktiga följdeffekter av allvarlig art.

1 Inledning

Riksrevisionen har granskat krisberedskapen mot tekniska hot och risker i det centrala betalningssystemet. Resultatet av granskningen presenteras i denna rapport.

1.2 Motiv för granskningen

Det svenska betalningssystemet omsätter 1 290 miljarder kronor varje dag[2]. De allra flesta betalningar sker numera genom elektroniska överföringar, som är starkt beroende av att den tekniska infrastrukturen (el, tele och IT) fungerar väl. Om inte de elektroniska överföringarna fungerar stannar stora delar av den ekonomiska aktiviteten av.

Allvarliga tekniska fel kommer ofta plötsligt och kan sprida sig snabbt eftersom olika aktörer och tekniska delsystem är beroende av varandra. Det gör att inblandade parter inte alltid hinner skydda sig tillräckligt. Den teknologiska utvecklingen har dessutom gått snabbt och antalet aktörer har ökat. Betalningssystemet har blivit alltmer beroende av en teknik som också är öppen för storskalig manipulation på ett helt annat sätt än under tidigare decennier. Samtidigt kvarstår risken för allvarliga olyckor, till exempel kabelbrott och datorhaverier. Den nya tekniken kan alltså genom spridnings- och kaskadeffekter snabbt leda till betydande skador och förluster för företag och konsumenter. Ytterst kan det bli kaos i samhället om ingen kan betala.

Betalningssystemet drabbas ofta av olika tekniska incidenter. Hittills har Sverige varit förskonat från en riktigt allvarlig störning. Hur en sådan störning kan se ut beskriver vi i avsnitt 1.6.

2 Värdepappershandeln står för 500 miljarder, kort och gireringar 30 miljarder, valutahandel 390 miljarder, betalningar mellan banker 360 miljarder och kontantbetalningar 10 miljarder kronor. Källa: Riksbanken. Eva Srejber, 2006. *Sårbarheter i det moderna betalningsväsendet.*

1.2 Frågeställningar

Syftet med granskningen är att bedöma om beredskapen för tekniska hot och risker i det centrala betalningssystemet är tillfredsställande. Revisionsfrågan som ska besvaras är följande:

Är statens åtgärder tillräckliga för att allvarliga tekniska störningar inom det centrala betalningssystemet kan förebyggas eller hanteras om de inträffar?

Vi har ställt följande delfrågor:

1. Har riksdagen och regeringen lagt fast tydliga och enhetliga mål för krisberedskapens inriktning och ambitionsnivå?
2. Är ansvarsfördelningen och samverkan så utformade att samhället på ett ändamålsenligt sätt kan förebygga eller hantera allvarliga störningar i det centrala betalningssystemet?
3. Har berörda samverkansmyndigheter säkerställt att de själva och de finansiella företagen har en tillräcklig förmåga att hantera kriser?
4. Har ansvariga myndigheter genomfört en tillfredsställande tillsyn och uppföljning?

1.3 Avgränsningar

Granskningen avgränsas till statliga insatser som gör att det centrala betalningssystemet fungerar även vid allvarliga el-, tele- och IT-störningar. Vi riktar främst intresset mot de verksamheter där allvarliga störningar kan få stora konsekvenser för samhälle, företag och medborgare.

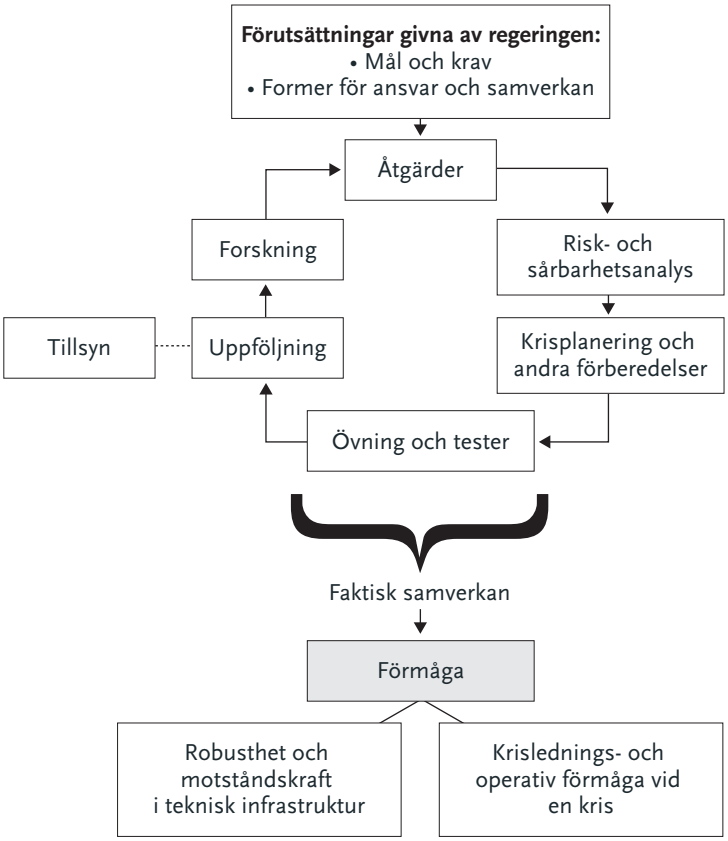
Berörda departement är Finans-, Social-, Närings-, Justitie- och Försvarsdepartementen. Myndigheter som vi i första hand granskar är Finansinspektionen, Försäkringskassan, Riksgälden, Post- och telestyrelsen samt Krisberedskapsmyndigheten. Dessutom granskar vi Riksbanken och samverkansorgan mellan stat och privat sektor. Tullverket och Skatteverket har en mer perifer roll inom betalningssystemet och ingår därför inte i granskningen. Den granskade tidsperioden är år 2003–september 2007.

1.4 Bedömningsgrunder

Bedömningsgrunder för granskningen är främst krav i krisberedskapsförordningen (2006:942) och andra författningar[3] samt uttalanden från riksdagen och regeringen. Vi använder också bedömningskriterier och berättigade krav som i övrigt kan ställas på en väl fungerande krisberedskap inom det centrala betalningssystemet. Bedömningen görs utifrån modellen i figur 1.1.

3 Bet. 1999/2000:FiU 13, rskr. 1999/2000:106.

Figur 1:1 Riksrevisionens utgångspunkter för att bedöma förmåga



Först granskar vi om regeringens mål och krav för krisberedskapen inom betalningssystemet är tydliga, och om de vägleder myndigheternas arbete och ökar förutsättningarna för en god samlad förmåga *(kap. 3)*. Vi bedömer här om målen är så preciserade att de kan följas upp och ligga till grund för överväganden om åtgärder, vilket riksdagen önskat[4].

Därefter bedömer vi om ansvarsfördelningen mellan myndigheterna är tydlig eller om det finns risk för att uppgifter faller mellan stolarna[5] *(kap. 4)*. Vidare bedömer vi i vilken grad myndigheterna samverkar när de utför sina uppgifter. Vi bedömer också om rätt parter deltar och om deltagarna är motiverade att samverka. Vid denna bedömning stöder vi oss på Krisberedskapsmyndighetens analyser av fungerande samverkan, som vi anser vara rimliga.

För det tredje går vi in på varje myndighets krisberedskapsarbete *(kap. 5)*. Arbetet bedöms i första hand utifrån krisberedskapsförordningens krav och regeringens uttalade krav på förmåga. I andra hand utgår vi från kriterier som Krisberedskapsmyndigheten föreslagit och som vi bedömer är rimliga.

4 Bet. 1999/2000:FiU13, rskr, 1999/2000:106.
5 För perioden före år 2007 hänvisar vi till verksförordningen (1995:1322) där det ställs krav på effektiv verksamhet. Därefter gäller en ny förordning (2007:515). I övrigt tillämpas här rimlighetsbedömningar.

Myndigheterna ska enligt krisberedskapsförordningen analysera risker och sårbarheter inom sina ansvarsområden och föreslå åtgärder som kan göra betalningssystemet mer motståndskraftigt. Myndigheterna ska också göra krisplaner och på andra sätt förbereda sig för att kunna hantera en allvarlig störning om den inträffar. Dessutom ska de öva sin krisberedskap. Incidenter ska rapporteras och analyseras. Det är också rimligt att betalningssystemets IT-miljö regelbundet prövas med penetrationstester. Några av myndigheterna har också fått i uppgift att stödja forskning för att täcka in kunskapsluckor inom ansvarsområdet.

I ett fjärde och sista steg utvärderar vi i vilken grad uppföljning och tillsyn fungerar väl *(kap. 6)*. För att beredskapsarbetet ska vara effektivt måste man följa upp och ta vara på erfarenheter och låta dem påverka det fortsatta arbetet[6]. Tillsynsmyndigheterna ska kontrollera att skyddsåtgärder genomförs av företag som har en central funktion i betalningssystemet. Här granskar vi om svenska tillsynsmyndigheter följer svenskt regelverk och internationella överenskommelser.

När Riksrevisionen bedömer den samlade förmågan hos regering och myndigheter att förebygga och hantera allvarliga störningar i betalningssystemet använder vi regeringens och KBM:s klassificeringar: god, god men vissa briser, bristfällig och mycket bristfällig. Den samlade bedömningen görs utifrån vilka brister som konstaterats i de enskilda grundförutsättningar som redovisats ovan.

Mer preciserade bedömningsgrunder redovisar vi i början av varje kapitel och i bilaga 1.

1.5 Metod och genomförande

Granskningen bygger på studier av dokument såsom författningar, utredningar, utskottsbetänkanden, budgetpropositioner och regleringsbrev. Vi har också granskat myndigheternas risk- och sårbarhetsanalyser och planer för beredskap för allvarligare störningar inom betalningssystemet, underlag och utvärderingar av totalövningar samt mötesprotokoll och dokumentation från olika samverkansforum.

För att komplettera dokumentstudierna har vi gjort ett femtiotal intervjuer. Vi har intervjuat enhetschefer och handläggare vid Finansdepartementet och enheten för beredskap och analys (EBA) vid Statsrådsberedningen. Vi har också intervjuat flera personer vid samtliga myndigheter som har ett uttalat ansvar för beredskapen inom betalningssystemet. Dessutom har vi intervjuat företrädare för bland annat Bankföreningen, storbankerna samt Värdepapperscentralen (VPC) och Bankgirocentralen (BGC).

6 Se not 3 ovan.

Professor Roland Heickerö från Totalförsvarets forskningsinstitut (FOI) har anlitats för att analysera hot, risker och sårbarheter inom betalningssystemet. Fil dr Johannes Malminen från samma institut har analyserat hur departement och ansvariga myndigheter förberett sig för att akut hantera en kris. För kvalitetssäkring har vi anlitat två experter: fil dr Peter Stenkula vid KTH och professor Lars Jonung vid EG-kommissionen.

1.6 Vad kan allvarligt störa betalningssystemet och få stora skadeverkningar? – ett exempel

Ett stort antal händelseförlopp kan leda till allvarliga störningar inom det centrala betalningssystemet. Enligt krisberedskapsförordningen[7] ska myndigheterna kunna hantera även allvarliga händelser som är mindre troliga, men som skulle få omfattande konsekvenser. Ett sådant händelseförlopp som enligt några av de granskade myndigheterna kan inträffa, är om till exempel ett elavbrott allvarligt påverkar kontantförsörjningen[8].

Allmänhet och företag kan i huvudsak betala på tre sätt: med kontanter, betalkort eller via girering. Kontanterna tar konsumenten ut från bankkontor eller uttagsautomat. Men uttagsautomaterna fungerar inte utan el. Eftersom inte heller datorer, larm och andra viktiga system fungerar utan el är det sannolikt att bankkontoren skulle stänga vid ett omfattande elavbrott. Dessutom blir också betalkorten i stor utsträckning obrukbara utan el eftersom terminalerna kräver el, och enligt Svenska bankföreningen sker 59 procent av alla betalningar med kort. Tidigare har handeln använt manuella kortdragare, men detta har i stort sett upphört. Utan elektricitet är det också omöjligt att betala räkningar via girering. Alla tre huvudsakliga betalningsvägar är således beroende av el.

Ett större elavbrott vid fel tidpunkt i månaden kan därför innebära att stora delar av befolkningen och näringslivet inte hinner betala sina räkningar i tid. Många företag och personer riskerar därmed att stå utan likvida medel.

Ett omfattande elavbrott orsakat av exempelvis ett kabelbrott eller en översvämning[9] i Gamla stan skulle alltså kunna få allvarliga konsekvenser för hela Stockholmsregionen och därmed även det svenska samhället.

De flesta myndigheter och institut har tillgång till reservkraft, men under en begränsad tid. Det är därför inte säkert att konsumenterna omedelbart påverkas av ett elavbrott. Är elavbrottet längre än två eller tre dagar kan följderna däremot bli problematiska. Om ingen kan betala avstannar de

7 Förordningen (2006:942) om krisberedskap och höjd beredskap.

8 Ett elavbrott kan också påverka andra delar av betalningssystemet, till exempel möjligheten att föra över stora betalningssummor mellan de centrala aktörerna i betalningssystemet. Det skulle i sin tur förstärka problemen med kontantförsörjning. Denna komplikation beskrivs inte här.

9 En vattenhöjning i Mälaren kan leda till en översvämning i Gamla stan, vilket kan leda till att systemet med försörjningstunnlar för bland annat vatten, el, värme, tele och datakommunikation under Stockholm vattenfylls. Stora delar av teletrafiken mellan olika delar av landet passerar också via kablar i dessa tunnlar.

ekonomiska transaktionerna och butikerna stänger. Ytterst kan det enligt Eva Srejber[10], före detta vice riksbankschef, innebära ett kristillstånd, liknande det som inträffade under krisen i Argentina under år 2003, då nästan bara byteshandel fungerade.

När tillgången till kontanter är slut kan nya betalningssätt komma att utvecklas, till exempel skuldbevis. Dessa är dock beroende av trovärdigheten hos de personer eller företag som utfärdar dem. De som inte har denna trovärdighet kan få problem.

1.7 Några centrala begrepp i rapporten

I rapporten används ett antal fackuttryck och begrepp. De mest använda begreppen har följande betydelser.

- Hot: Faror som kan vålla skador på personer eller egendom. Antagonistiska hot uppstår på grund av mänskligt agerande med en medveten intention.
- Det centrala betalningssystemet[11]: De tekniska och administrativa system som gör det möjligt att betala för varor och tjänster i samhället.
- Risk: Den fara som en oönskad händelse innebär för människor, miljö och materiella värden. Risk är en sammanvägning mellan sannolikhet och konsekvens.
- Sannolikhet: Hur ofta en händelse bedöms inträffa.
- Konsekvens: Den negativa följden av en oönskad händelse.
- Sårbarhet: Ett systems (bristande) förmåga att fungera när det utsätts för påfrestningar.
- Operativ risk: Risken för förluster till följd av icke ändamålsenliga eller inte fungerande interna förfaranden, mänskliga fel, system eller yttre händelser.
- Teknisk risk: Operativa risker i teknisk infrastruktur, såsom data- och IT-system, el- och teletransmission, energiförsörjning och infrastrukturens skalskydd.
- Robusthet: Förmåga att fungera och uppnå syften vid påfrestning.
- Förebyggande åtgärd: Åtgärd som begränsar sannolikheten för en oönskad händelse.
- Förberedande åtgärd: Åtgärd som begränsar konsekvensen av en oönskad händelse.
- Förmåga: Den robusthet och beredskap som finns i samhället.
- Krishanteringsförmåga: Förmåga att leda, samordna och informera vid svår påfrestning.
- Operativ förmåga: Förmåga att motverka eller lindra skador *under* en kris.
- Samhällsviktig verksamhet: verksamhet som det blir kris om den stannar eller som är väsentlig för att en kris i samhället ska kunna hanteras.

10 Riksbanken. Eva Srejber, 2006. *Sårbarheter i det moderna betalningsväsendet*.
11 I rapporten används som en kortare version också betalningssystemet, i stället för att alltid upprepa *det centrala* betalningssystemet.

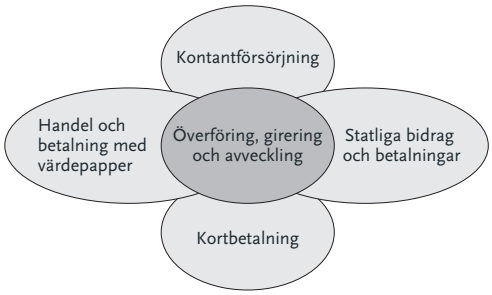
2 Det centrala betalningssystemet

I detta kapitel ger vi en kort översikt över betalningssystemet, dess kärnverksamheter och inbördes beroenden samt ansvariga aktörer. Beskrivningarna är huvudsakligen hämtade från Riksbanken och Krisberedskapsmyndigheten.

2.1 Vad är det centrala betalningssystemet?

Det centrala betalningssystemet består av de tekniska och administrativa system som gör det möjligt att betala för varor och tjänster i samhället. Bankerna är här de centrala företagen. Mindre betalningar sker ofta med sedlar och mynt. Andra sätt att betala är med kort eller genom överföringar och gireringar. Överföringar mellan olika bankkonton används vid stora betalningar. Staten har ett delvis eget betalningssystem för att kunna betala ut bidrag och löner. Värdepapper måste kunna betalas och användas som säkerheter för betalningar. Att dessa centrala delar av betalningssystemet fungerar är av stor vikt för samhället. Det centrala betalningssystemet innehåller alltså flera delvis inbördes beroende och delvis oberoende samhällsviktiga kärnverksamheter. Detta illustreras i figuren nedan.

Figur 2.1 Kärnverksamheter inom betalningssystemet



Kontantförsörjning

Kontanter används för att säljare och köpare ska kunna mötas fysiskt och byta varor mot pengar. Ofta rör det sig om relativt låga belopp. Kontantbetalningarna står fortfarande för en stor del av antalet transaktioner, även om andelen har minskat på senare år till förmån för kortbetalning och elektroniska överföringar. Ur ett krisperspektiv är det enligt Krisberedskapsmyndigheten viktigt att de som behöver får tillgång till kontanter i sitt närområde; detta för att kunna betala varor och tjänster kontant.

Kortbetalning

När vi betalar med kort överförs pengar mellan två konton hos någon eller några banker. Många kort fungerar som både uttags- och betalkort. I Sverige sker sex av tio betalningar med kort. Både de delar av betalkortssystemet som finns inom banker och de som finns inom säljföretag, liksom kontantförsörjningen, är beroende av fungerande el och telekommunikationer. Ur ett krisperspektiv är det därför viktigt att kortinnehavare faktiskt kan betala nödvändiga varor och tjänster med kort.

Överföring, girering och avveckling

Överföring, girering och avveckling är navet i det finansiella systemet. Vid överföring flyttas ett tillgodohavande från en kontoinnehavare till en annan. Man kan föra över pengar genom att besöka ett bankkontor, ringa, skicka ett brev eller ett fax till bankkontoret eller genom att registrera sin överföring själv via internet.

En girobetalning är en särskild sorts överföring som utnyttjar ett bestämt nummer (bankgiro) för att identifiera betalningsavsändare och betalningsmottagare. Det så kallade RIX-systemet sköter avveckling av stora betalningar mellan bankerna. Ur ett krisperspektiv är det viktigt att nödvändiga transaktioner mellan konton och kontohavare kan göras inom förväntade tidsramar.

Statliga bidrag och betalningar

Det statliga betalningssystemet består av de regelverk, avtal, system och rutiner som gör det möjligt för myndigheter, medborgare och företag att betala varandra. Själva utbetalningarna görs av bankerna. Staten har ramavtal med tre banker, och det är Riksgälden som förhandlar om dessa avtal. År 2003 genomförde 270 myndigheter cirka 100 miljoner betalningstransaktioner för totalt 4 000 miljarder kronor. Myndigheterna har tillgång till medel på statsverkets checkräkning i Riksbanken (SCR). Riksgälden sätter upp regler för hur staten ska betala ut löner och bidrag.

Bidragen från socialförsäkringssystemet har särskilt stor betydelse för såväl enskilda som för samhällsekonomin i stort. Av 100 kronor som används för privat konsumtion kommer cirka 25 kronor från socialförsäkringen. Den svenska socialförsäkringen (cirka 50 olika förmåner och bidrag) betalade år 2005 sammanlagt ut 399 miljarder kronor. Av dessa pengar går 80 procent till utsatta grupper, som sjuka, handikappade och pensionärer.

Ur ett krisperspektiv är det viktigt att dessa grupper får tillräckligt stor ersättning för att klara de nödvändigaste utgifterna. Det är också viktigt att statliga myndigheter kan betala ut löner. Dessutom måste det statliga betalningssystemet vara så säkert att det inte kan utnyttjas i brottsliga syften.

Handel, clearing och avveckling i finansiella instrument

Av all handel med finansiella instrument[12] är räntehandeln viktigast för samhället på kort sikt. Här ingår dels den kortsiktiga handeln mellan bankerna, dels penningmarknads- och obligationshandeln. Det viktiga är att alla inblandade har beredskap (likviditet) för kommande in- och utbetalningar. Korta placeringar måste vara enkla att omvandla till likvida medel när betalningarna sker eller tillgångar belånas.

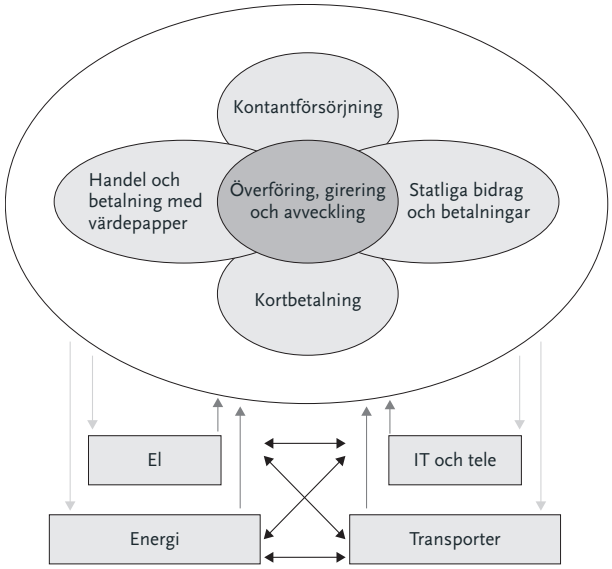
Parterna i systemet måste kunna lita på att motparten betalar enligt överenskommelse. Utan detta förtroende riskerar likviditetsskapande verksamhet att stanna av. Det kan räcka med ett rykte för att skada förtroendet för en motpart.

I ett krisperspektiv är det viktigt att det går att handla med finansiella instrument i sådan omfattning att betalningssystemet fungerar. Staten måste också kunna ta nya lån samt avveckla och betala redan upptagna lån.

2.2 Infrastrukturen för betalningssystemet

De olika kärnverksamheterna i betalningssystemet är beroende av en underliggande infrastruktur i form av bland annat el, tele, energi och transporter (se figur 2.2 nedan). Störningar i dessa verksamheter kan påverka en enskild eller all kärnverksamhet, och verksamheterna kan även påverka varandra.

Figur 2.2 Beroendeförhållanden



12 Gränsdragningen mellan handel i finansiella instrument och avvecklingsdelen i kärnverksamheten *överföring, girering och avveckling* är inte helt tydlig. En aktivitet som tas upp under den ena kärnverksamheten också kan betraktas som en del i den andra kärnverksamheten.

Elförsörjning

Den finansiella sektorn är mycket beroende av el. Banker, bankomater, kortsystem och central avveckling behöver alla el. De mest betydande finansiella aktörernas huvudkontor och centrala datasystem finns inom en liten yta i centrala Stockholm, och tre av fyra storbankers huvudkontor försörjs med el från Fortum. Även pumpar på bränslestationer och telekommunikation är mycket beroende av el. Ett omfattande elavbrott kan alltså också innebära att diesel inte kan fyllas på i reservelaggregaten, om inte snabbt tillräckliga lager byggts upp.

Telekommunikationer

All finansiell verksamhet är beroende av telekommunikationer. El är i sin tur en grundförutsättning för elektronisk kommunikation. Ett längre elbortfall gör därför att även telekommunikationerna störs.

Energileveranser

Alla aggregat för reservel drivs med diesel. Bränslepumpar vid oljedepåer och bensinstationer är beroende av el. Transporter behöver olja, diesel och bensin. Därför kan energibrist leda till att all regional elförsörjning liksom telekommunikationer mellan exempelvis Riksbanken och bankerna slås ut.

Transporter

Kontantförsörjningen liksom myndigheternas och bankernas reservelaggregat är – som nämnts ovan – även beroende av att transporterna fungerar. Då behövs även tillgång till diesel för transporterna.

2.3 Vilka är de ansvariga aktörerna?

I kapitel 4 beskriver vi mer ingående vilket ansvar olika aktörer har inom det centrala betalningssystemet. Här nedan redovisas endast vilka offentliga och privata aktörer som huvudsakligen har ett ansvar inom det centrala betalningssystemet respektive ansvar för underliggande infrastruktur.

2.3.1 *Ansvar inom det centrala betalningssystemet*

Offentliga aktörer

Riksbanken
Finansinspektionen (FI)
Riksgäldskontoret (Riksgälden)
Försäkringskassan
Skatteverket (granskas ej)

Privata aktörer

Systemviktiga banker som SEB, Nordea, SHB och Swedbank
Börser, auktoriserade marknadsplatser och clearingorganisationer (Stockholmsbörsen, Bankgirocentralen och Värdepapperscentralen)

2.3.2 *Ansvar för underliggande infrastruktur (el, tele, energi, transporter och informationssäkerhet)*

Offentliga aktörer

Post- och telestyrelsen (tele, IT)
Energimyndigheten (el, energi)
Svenska Kraftnät AB (el)
Försvarets radioanstalt och Totalförsvarets forskningsinstitut (informationssäkerhet)

Privata leverantörer av infrastruktur

Regionala och lokala elföretag
Teleoperatörer
Oljebolag, transportföretag med flera
Mjukvaruleverantörer, reparatörer med flera

2.3.3 *Generellt beredskapsansvariga myndigheter och stödmyndigheter*

Krisberedskapsmyndigheten (KBM)
Försvarsmakten
Rikspolisen, Säkerhetspolisen (Säpo)
Länsstyrelserna

2.3.4 *Samverkansorgan*

Samverkansområdet för ekonomisk säkerhet (SOES)
Finansiella sektorns privat–offentliga samverkansprojekt (FSPOS)
Andra samverkansorgan vid KBM, Riksbanken och Post- och telestyrelsen med flera.

2.3.5 *Regeringskansliet med ansvariga departement*

Finansdepartementet
Försvarsdepartementet
Näringsdepartementet
Socialdepartementet
Justitiedepartementet

3 Mål och krav från regering och riksdag

Revisionsfrågan i detta kapitel är:
Har riksdagen och regeringen lagt fast tydliga och enhetliga mål för krisberedskapens inriktning och ambitionsnivå när det gäller betalningssystemet?

3.1 Bedömningsgrunder

Mål måste enligt riksdagen vara välformulerade, mätbara och uppföljningsbara för att resultatstyrning ska bli meningsfull[13]. Mål för samhällets krisberedskapsåtgärder som kanaliseras via olika departement bör också vara rimligt entydiga och ligga i linje med varandra. Med mål och krav menas här ett framtida tillstånd som samhället önskar.

3.2 Vilka uttalanden har riksdagen gjort?

3.2.1 Mål för den generella krisberedskapen

Målen för vår säkerhet bör enligt riksdagen[14] vara att värna

- befolkningens liv och hälsa
- samhällets funktionalitet
- förmågan att upprätthålla våra grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter.

Enligt riksdagen är ett fungerande samhälle beroende av ett antal samhällsviktiga verksamheter, vilka inte får bryta samman. En av dessa verksamheter är betalningsväsendet.

3.2.2 Mål för politikområden och i lagar

Mål för politikområdet Finansiella system och tillsyn

Det finansiella systemet ska enligt riksdagen vara effektivt och tillgodose såväl samhällets krav på stabilitet som konsumenternas intresse av ett gott skydd. Tillsynen ska bedrivas effektivt.

13 *Utvecklingen av den ekonomiska styrningen* bet. 1999/2000 FiU13, rskr. 1999/2000:106.
14 Samverkan vid kris – för ett säkrare samhälle prop. 2005/06:133, bet. 2005/06:FöU9.

Mål och krav i rörelselagar

En bank ska enligt banklagen drivas på ett sådant sätt att den inte äventyrar sin förmåga att fullgöra sina förpliktelser[15]. Bankerna ska identifiera, mäta, styra och ha kontroll över de risker verksamheten är förknippad med. Bankernas ställning ska kunna överblickas och i övrigt vara sund. Lagen kräver också att bankerna har styrdokument för operativa risker, riskhanteringsprocesser, styrning och kontroll[16]. Finansinspektionen ska se till att bankerna följer lagarna. Om Finansinspektionen bedömer att en bank bryter mot lagen kan den gripa in med sanktioner. Ytterst kan banken förlora sitt tillstånd att bedriva bankrörelse.

Mål i riksbankslagen

Enligt riksbankslagen[17] ska Riksbanken se till att betalningsväsendet fungerar säkert och effektivt. Riksbanken ska också försörja landet med sedlar och mynt. När Riksbanken planerar och genomför sin verksamhet i fred ska den beakta de krav som totalförsvaret ställer.

Mål i ellagen

Ett elavbrott får vara högst 24 timmar långt, enligt ett krav i ellagen. Kravet gäller nätbolagen på regional och lokal nivå, och ska vara uppfyllt senast den 1 januari 2011. Det beslutade riksdagen i december 2005.

Ellagens krav är formulerat som funktionskrav. Det innebär att varje nätbolag själv kan avgöra hur kravet ska nås. Antingen kan bolagen se till att deras nät är robusta eller att de snabbt kan reparera näten vid ett elavbrott. Det är också möjligt att ställa strängare krav än funktionskravet.

Mål i lagen om elektronisk kommunikation

Teleoperatörer ska uppfylla rimliga krav på att telekommunikationerna fungerar väl och är tekniskt säkra. Telekommunikationerna måste vara uthålliga och tillgängliga vid extraordinära händelser i fredstid[18]. Regeringen eller den myndighet som regeringen utser får meddela teleoperatörerna hur de ska leva upp till denna skyldighet och om undantag från skyldigheterna[19].

15 Lagen (2004:297) om bank- och finansieringsrörelse.
16 Lagen (2006:1371) om kapitaltäckning och stora exponeringar.
17 Lagen (1988:1385) om Sveriges riksbank.
18 Lagen (2003 389) om elektronisk kommunikation.
19 Lagen (2005:240) om ändring i lagen (2003:389) om elektronisk kommunikation.

3.3 Internationella standarder och krav på betalningsväsendet

Det svenska betalningsväsendet är en del av det globala betalningssystemet. Centralbankernas gemensamma intresse för betalningsväsendet har lett till att de i dag samarbetar på ett omfattande och institutionaliserat sätt. Riksbanken medverkar till exempel i grupper som arbetar med kontinuitets- och krisfrågor inom Centralbankernas bank (BIS) och inom Europeiska centralbankssamarbetet (ECBS). Riksbanken deltar också i det EU-samarbete som sker inom ramen för Ecofin[20] och inom den nordiska sfären av centralbanker.

Riksbanken utvärderar finansiella system och aktörer enligt CPSS[21] och Ioscos[22] normer. CPSS är en del av Bank of International Settlement (BIS). I två rapporter[23] anger CPSS riktlinjer för ett säkert centralt betalningssystem och hur man effektivt bör övervaka detta system. Ett viktigt mål är att all central avveckling mellan systemviktiga banker och infrastrukturföretag bör ske senast samma dag. Finansinspektionen och Post- och telestyrelsen arbetar på samma sätt som Riksbanken i många internationella sammanhang.

3.4 Riksbankens mål enligt bankens egen instruktion

Riksbanken agerar i två roller för att främja betalningsväsendet. Det skriver direktionen inom Riksbanken, som består av riksbankschefen och vice riksbankschefer, i Riksbankens instruktion. Den ena rollen innebär att se till att kontantförmedlingen och övrig betalningsförmedling fungerar. Den andra rollen innebär att förebygga och hantera kriser inom det finansiella systemet.

Mer konkret ger Riksbanken ut sedlar och mynt. Banken ansvarar också för och övervakar RIX-systemet, som genomför stora betalningar mellan bankerna och dess deltagare. Dessutom ska Riksbanken låna ut pengar under dagen.

20 EU:s ministerråd när finansministrarna möts.
21 CPSS är ett forum för G 10-ländernas centralbanker som ska stärka finansmarknadernas infrastruktur genom effektiva och ändamålsenliga betalningssystem. Committee on Payment and Settlement Systems (CPSS) har formulerat standarder för effektiva betalnings- och värdepappersflöden, och sedan 1999 finns ”Core Principles for Systematically Important Payment Systems”. IMF använder denna standard som utgångspunkt för sina krav på olika länders betalningssystem.
22 International Organization of Securities Commissions (Iosco) är en internationell organisation där över 100 tillsynsmyndigheter samarbetar om att ta fram gemensamma regler för värdepappersmarknadens aktörer.
23 *Core principles for systematically important payment systems* från år 2001 och *Central bank oversight of payment and settlement systems från* år 2005, Bank for International Settlements.

3.5 Regeringens mål och krav på myndigheterna

3.5.1 Krisberedskapsförordningens[24] mål och krav

Statliga myndigheter ska arbeta för att göra samhället mindre sårbart. De ska också kunna hantera sina uppgifter väl vid kriser i fredstid och vid höjd beredskap. Detta är effektmålen i krisberedskapsförordningen. Övriga krav i förordningen är inte effektmål, utan krav på aktiviteter som myndigheterna ska utföra, till exempel samverka eller göra en risk- och sårbarhetsanalys med ett antal angivna moment.

3.5.2 Regeringens mål och krav för enskilda myndigheter i instruktioner och regleringsbrev

Ett dussin myndigheter ansvarar för olika typer av statliga insatser som berör krisberedskapen mot tekniska hot och risker inom betalningssystemet. Dessa myndigheters insatser regleras och styrs från fem departement.

1. Försvarsdepartementet: Krisberedskapsmyndigheten, Försvarets radioanstalt och övriga myndigheter
2. Finansdepartementet: Finansinspektionen, Riksgälden, Skatteverket och länsstyrelserna
3. Socialdepartementet: Försäkringskassan
4. Näringsdepartementet: Post- och telestyrelsen, Svenska kraftnät AB och Energimyndigheten
5. Justitiedepartementet: Säkerhetspolisen, Rikspolisstyrelsen

3.6 Iakttagelser

Regeringen styr krisberedskapen för att betalningssystemet ska kunna fungera under allvarliga störningar via fem departement och genom mål som formuleras i ett dussin ansvariga myndigheters regleringsbrev. Riksbanken styrs av riksbankslagen och internationella åtaganden.

Målen är allmänt hållna

Regeringens mål och krav är allmänt uttryckta. Oklara formuleringar dominerar, som till exempel ”minska risken för olyckor och svåra påfrestningar”, ”bidra till ett stabilt system”, ”verka för att samhällets sårbarheter minskar”,

24 Krav på myndigheterna att hantera kriser finns i krisberedskapsförordningen (2006:942) som trädde i kraft den 1 september 2006. Denna förordning ersatte en tidigare krisberedskapsförordning (2002:472).

”bidra till ett väl fungerande samhälle för medborgare och näringsliv”, ”ett hållbart informationssamhälle för alla”, ”öka driftsäkerhet och tillgänglighet” och ”öka robustheten i samhällsviktiga system och infrastrukturer”.

I vissa fall antyder regeringen att det finns mer preciserade krav på säkerhet, men regeringen anger inte vilka dessa krav är eller vem som ska ställa dem. Exempel på sådana formuleringar är ”tillgodose statsmakternas uttalade krav på ... säkerhet”, ”tillgodose samhällets krav på stabilitet”. Målen är också i många fall uttryckta i åtgärdstermer som ”verka för”, ”bidra till”, ”motverka”, inte i termer av slutresultat och önskade effekter.

Även Riksbankens mål i riksbankslagen är allmänt hållet. Riksbanken ska ”främja” ett säkert betalningsväsende.

Målen är inte enhetliga

Regeringens mål för krisberedskap är inte enhetliga. Särskilt skiljer sig mål och krav formulerade utifrån krisberedskapsförordningen från de mål och krav om tillsyn och övervakning som gäller bankernas och infrastrukturföretagens riskhantering.

I det förra fallet är de centrala begreppen ”hot, risker och sårbarheter” och målen rör politikområdet ”Skydd och beredskap mot olyckor och svåra påfrestningar”.

I det senare fallet är begreppen ”stabilitet” och ”finansiella och operativa risker” centrala. Regeringen reglerar här tydligare hur bankerna ska ta fram underlag och kräver att bankerna hänvisar till internationella standarder som till exempel Basel II-regler och CPSS-normer[25].

Inga krav på uthållighet från regeringen

Regeringen har inte preciserat något mål för hur uthålligt betalningssystemet ska vara. Ett sådant mål eller uttalande om uthållighet kan baseras på i vilken utsträckning samhället kan undvara en viss finansiell tjänst, aktivitet eller funktion utan allvarliga olägenheter eller spridningseffekter (timmar eller dagar). Målet kan även tala om hur länge (i dagar) samhället ska kunna hantera en kris och upprätthålla en viss funktion eller tjänst med förberedda beredskapsåtgärder. Finansinspektionen och andra samverkansansvariga myndigheter har efterfrågat tydligare mål för uthållighet. Alltför hög uthållighet kostar pengar, menar man, medan alltför låg uthållighet kan kosta samhället mycket vid en kris.

25 Se avsnitt 3.3.

Uttalanden om uthållighet skiljer sig mellan aktörer och sektorer

Samverkansansvariga myndigheter bör enligt Krisberedskapsmyndigheten vid en kris i fredstid kunna agera i sina roller med en uthållighet i minst en vecka. Detta gäller i förekommande fall även verksamhetskritiska delar av respektive sektor[26]. Vilka de samverkansansvariga myndigheterna är utpekar krisberedskapsförordningen.

Flera intervjuade tolkar dock inte detta mål som ett tidsmål för hela det centrala betalningssystemet (så att det även skulle gälla de privata aktörer som ansvarar för delar av systemet). De tolkar i stället målet snävare, så att det enbart avser krisberedskapen inom den egna myndigheten eller hur de åtgärder som finansieras av Krisberedskapsmyndigheten ska planeras. Enligt Finansinspektionen skulle dock ett avbrott i centrala funktioner hos storbankerna som varar i mer än två till tre dagar bli svårt att hantera. Regeringen har inte tagit ställning i denna fråga.

Tjänster, målgrupper och företag prioriteras inte

Vid en kris kan inte alla finansiella tjänster fungera. I praktiken kan man behöva välja vilka tjänster som mest akut måste fungera och vilka målgrupper som är mest utsatta i krisläget. Sådana prioriteringar har regeringen inte analyserat, förberett eller fastställt.

Grundläggande krav på leverantörer av infrastruktur har inte formulerats annat än på elområdet

Regeringen har inte formulerat grundläggande krav som samhället och den finansiella sektorn bör ställa på leverantörer av infrastruktur som till exempel tele och IT när det gäller det centrala betalningssystemet.

3.7 Bedömning av mål och krav

Riksrevisionen bedömer att de mål och krav regeringen lagt fast för krisberedskapen inom det centrala betalningssystemet inte är tillräckligt tydliga. Regeringen har inte formulerat mål som det går att följa upp eller utöva tillsyn emot. Regeringen har inte uttalat hur lång uthålligheten ska vara i betalningssystemet eller angivit vilka finansiella tjänster och målgrupper som ska prioriteras vid en kris.

26 KBM (2005), *Samhällets krisberedskap – Inriktning för verksamheten 2007.*

Regeringen har inte heller fastställt vilken grundläggande funktionalitet som ska finnas och vilka säkerhetskrav som kan ställas på leverantörer av telekommunikationer, energi och IT.

Regeringskansliet menar att tydliga mål och krav kan vara kostnadsdrivande. Riksrevisionen menar att det bara är fallet om åtgärder beslutas utan att tillräckliga analyser görs av konsekvenser och kostnader.

Några myndighetsrepresentanter menar att preciserade mål och krav kan hämma teknikutvecklingen på så att alla aktörer anpassar sig till en viss lägsta nivå. Riksrevisionen anser dock att väl formulerade krav även kan stimulera teknikutvecklingen och bidra till höjda säkerhetsnivåer.

Om målen inte är tydliga och enhetliga blir det svårare att följa upp resultat av skyddsåtgärderna, värdera effekter av åtgärderna och få en samlad lägesbild. Otydliga mål försvårar därmed möjligheterna för myndigheterna att kunna förbereda och inrikta beredskapsåtgärder på ett effektivt sätt.

4 Myndigheternas ansvar och samverkan

Revisionsfrågan i detta kapitel är följande:
Är ansvarsfördelningen och samverkan utformade så att samhället på ett ändamålsenligt sätt kan förebygga eller hantera allvarliga störningar i det centrala betalningssystemet?

4.1 Bedömningsgrunder

Ansvarsfördelning och skyldigheter att samverka för myndigheter under regeringen regleras i krisberedskapsförordningen från år 2006[27], i riksbankslagen och i myndigheternas instruktioner och regleringsbrev. Dessa dokument anger vilka myndigheter som har ansvar för bland annat planering, samordning, risk- och sårbarhetsanalyser, bidrag till skyddsåtgärder, samverkan, övningar, normgivning, uppföljning och tillsyn.

Våra bedömningsgrunder för ansvarsfördelning är följande:

- Ansvaret för dessa uppgifter bör vara tydligt fördelat mellan de granskade myndigheterna. Samhället bör inte riskera att uppgifter faller mellan stolarna.
- Myndigheterna bör ta ansvar för de uppgifter de fått i regleringsbrev och instruktioner.

Vi använder också följande normer från Krisberedskapsmyndighetens rapporter om vad som krävs för att samverkan ska fungera[28] och som vi anser vara rimliga:

- Myndigheter bör samverka när det behövs.
- Om inte samverkan fungerar bör någon leda samverkan.
- De parter som samverkar bör ha förtroende för varandra.
- De parter som är beroende av varandra bör vara med i samverkan.
- Deltagarna bör vara motiverade att samverka.
- Det bör finnas tydliga mål, mandat och resurser för samverkan.

27 Förordning (2006:942) om krisberedskap och höjd beredskap.
28 KBM (2006) *Privat-offentlig samverkan – från idé till fungerande praktik.*

4.2 Ansvarsfördelning enligt riksdag och regering

Den ansvarsfördelning som enligt riksdagen ska gälla för krisberedskapen slogs fast i propositionen *Samverkan vid kris – för ett säkrare samhälle*[29]. Utöver målen för krisberedskapen lade man där fast vissa grundläggande principer för det generella krisberedskapsarbetet, där ekonomisk säkerhet ingår.

- *Ansvarsprincipen* innebär att den som normalt har ansvar för en verksamhet också ska ha ansvaret vid en kris.
- *Närhetsprincipen* innebär att en kris ska hanteras där den inträffar av dem som är närmast berörda och ansvariga.
- *Likhetsprincipen* innebär att en verksamhet inte ska förändra sin organisation och lokalisering mer än vad som krävs vid en kris.

Samhällets krishantering ska bygga på samverkan mellan aktörer på lokal, regional och nationell nivå samt inom och mellan enskilda sektorer. Med utgångspunkt i sektorsspecifika författningar agerar varje aktör utifrån sin roll, sin uppgift och sina befogenheter. Agerandet sker samtidigt, och aktörerna är ofta starkt beroende av varandra. Det är därför viktigt att de samordnar arbetet.

4.2.1 Riksbankens ansvar

De riksdagsbeslut som fattats under 2000-talet om krisberedskap behandlar inte Riksbankens ansvar. Ett skäl är att riksdagen flyttade ansvaret för beredskapsplaneringen inom det finansiella området från Riksbanken till Finansinspektionen redan år 1995[30, 31]. Det beslutades då att Riksbanken skulle behålla beredskapsansvaret för den egna verksamheten – bland annat för sedlar, mynt, valutareserv och för en eventuell valuta- och kreditreglering. I övrigt ska Finansinspektionen svara för att planera beredskapen. Riksbanken ska dock samråda med Finansinspektionen i frågor om finansiella tjänster.

Enligt riksbankslagen ska Riksbanken främja ett säkert och effektivt betalningsväsende samt övervaka dess stabilitet. Lagen preciserar inte närmare Riksbankens ansvar i dessa avseenden, och det gör inte heller bankens arbetsordning. Riksbanken övervakar främst de stora, i huvudsak finansiella, betalningarna mellan banker och andra finansiella institut. Övervakningen sker enligt bankens instruktion och enligt andra uttalanden från direktionen.

29 Prop. 2005/06:133, bet. 2005/06:FöU9.
30 *Riksbankens och Finansinspektionens beredskapsansvar,* bet. 1994/95:FiU3.
31 Lagen (1988:1385) om Sveriges riksbank trädde i kraft den 1 januari 1989. I förarbetena (prop. 1986/87:143 s. 73) uttalas att ”Paragrafen har utformats efter förebild av vad som gäller för vissa affärsverk som har planeringsansvar inom totalförsvarets ram ... Bestämmelserna ansluter sig till den roll inom de civila delarna av totalförsvaret som riksbanken får genom riksdagens beslut.” I den ursprungliga bestämmelsen stod uttryckligen också att ”Det åligger riksbanken att ansvara för beredskapsplaneringen på bank- och betalningsväsendets område”.

Riksbanken har valt att låta bankerna använda RIX-systemet för att utföra betalningar till varandra. Systemen för bankomat- och kortbetalningar har Riksbanken däremot undantagit från sitt primära ansvarsområde. Kontanthanteringen har Riksbanken i praktiken lagt ut på privata företag[32]. Ansvaret för kontantförsörjningen har man begränsat till att ge ut och makulera sedlar och mynt. Intervjuade personer hos Riksbanken anser inte att banken ansvarar för att till exempel belysa risker och sårbarheter i kontantförsörjningen i dess helhet eller för att göra förberedelser som kan lindra skadorna om försörjningen med kontanter havererar.

Rent formellt gäller inte krisberedskapsförordningen för Riksbanken. Förordningar gäller bara för myndigheter under regeringen. Riksbanken brukar dock i regel följa även förordningar[33]. Riksbanken har inom finansiella sektorns privat-offentliga samverkansprojekt (FSPOS) bidragit med såväl resurser som underlag för att följa upp och bedöma förmågan[34].

Riksbankens stabilitetsrapport bedömer förmågan hos några centrala aktörer inom betalningssystemet, men inte samlat och årligen vilka operativa och tekniska risker som finns i alla delar av det centrala betalningssystemet.

4.2.2 Myndigheter under regeringen

Alla myndigheter under regeringen har ett ansvar för krisberedskapen inom sina respektive ansvarsområden och ska varje år göra risk-, hot- och sårbarhetsanalyser. Myndigheterna ska också redovisa åtgärder och behov samt hur de ska hantera konsekvenserna av en kris till Regeringskansliet och Krisberedskapsmyndigheten[35].

Myndigheterna ska enligt krisberedskapsförordningen planera övningar inför kommande kriser. Vidare ska de informera andra aktörer, medier och allmänheten vid allvarliga kriser. De samverkansansvariga myndigheterna ska dessutom utveckla samarbetet med näringslivet och föra en kontinuerlig dialog med dess företrädare. Detta ska, om möjligt, leda till att parterna får en gemensam syn på förhållanden och sårbarheter i samhället samt en uppfattning om ömsesidigt ansvar.

De samverkansansvariga myndigheter som omfattas av granskningen är Finansinspektionen, Riksgälden, Försäkringskassan, Svenska kraftnät AB, Energimyndigheten och Post- och telestyrelsen. Dessa myndigheter har alla vidtagit åtgärder på de områden som utpekas i krisberedskapsförordningen.

32 Distributionen av kontanter sköts sedan år 2005 av privata företag. Då avvecklade Riksbanken sitt bolag Pengar i Sverige AB.
33 Brev från Riksbanken till Riksrevisionen, daterat den 27 oktober 2007.
34 Riksbanken är adjungerad medlem i SOES och FSPOS. Riksbanken är också en av de ursprungliga initiativtagarna till FSPOS.
35 Förordning (2006:942) om krisberedskap och höjd beredskap.

Finansinspektionen

Finansinspektionen är central förvaltningsmyndighet för tillsyn, regler och tillstånd vad gäller finansiella företag. Finansinspektionen ska följa och analysera utvecklingen inom verksamhetsområdet samt rapportera till regeringen om instabilitet i finanssektorn riskerar att skada det finansiella systemet. Inspektionen ska också utföra uppgifter enligt krisberedskapsförordningen och samarbeta internationellt inom sitt verksamhetsområde.

Finansinspektionen ska varje år lämna en rapport till regeringen som bedömer hur stabilt det finansiella området är. Inspektionen ska också samråda med Riksbanken i frågor om betalningssystemets stabilitet eller frågor som berör Riksbankens ansvar för betalningsväsendet och beredskapsplaneringen enligt riksbankslagen.

Riksgälden

En av Riksgäldens huvuduppgifter är att vara statens internbank. I den rollen har Riksgälden fått ansvaret för att det statliga betalningssystemet tillgodoser statsmakternas krav på kostnadseffektivitet, säkerhet, information och valfrihet. Riksgälden ska tillgodose det grundläggande behovet av ekonomisk säkerhet och minimera riskerna för störningar. Riksgälden ska aktivt samverka med andra för att stärka samhällsviktiga system och infrastrukturer samt samhällets förmåga att leda kriser.

Riksgälden har också ansvar för det statliga betalningssystemet. Riksgälden har här möjlighet att ställa krav på säkerhet och berdskap i de avropsavtal som man har slutit med storbankerna om att hantera statens utbetalningar.

Länsstyrelserna

Länsstyrelserna ansvarar enligt krisberedskapsförordningen för geografisk samordning. De ska samordna arbetet mellan kommuner, landsting och myndigheter[36]. I storstadsregionerna, särskilt i Stockholm, finns många viktiga aktörer samlade.

Krisberedskapsmyndigheten

Krisberedskapsmyndigheten[37] ansvarar för att minska risken för och konsekvenserna av olyckor och svåra påfrestningar på samhället i fred. Ansvaret

36 *Förordningen (2006:942) om krisberedskap och höjd beredskap.*

37 Krisberedskapsmyndigheten, som bildades år 2002, är en tvärsektoriell myndighet med begränsat operativt ledningsansvar och fokus på utbildning, koordinering, övning, metodstöd och utarbetande av beslutsunderlag till Försvarsdepartementet. Ett utredningsförsvar som lades i maj 2007 föreslår att KBM, Räddningsverket och Styrelsen för psykologiskt försvar slås samman.

koncentreras främst till den förberedande och förebyggande krisfasen. Krisberedskapsmyndigheten ska främja samverkan och samordning[38]. Myndigheten ska utveckla metoder samt sammanställa och analysera myndigheternas risk- och sårbarhetsanalyser.

Krisberedskapsmyndigheten får inte sätta standarder för krisberedskap och säkerhet. Man saknar ett förordningsansvar. Myndigheten bevakar dock att grundläggande säkerhetskrav ställs då andra skaffar nya system med myndighetens medel. Man kan också lyfta fram goda exempel.

Krisberedskapsmyndigheten har inget ansvar i operativ krishantering, men ska vid en kris ställa samman lägesbilder för regeringen på en nationell nivå[39]. Krisberedskapsmyndigheten ska också hålla samman arbetet med samhällets informationssäkerhet och varje år ge regeringen en samlad bild av informationssäkerheten i landet.

Myndigheter ansvariga för teknisk infrastruktur

Post- och telestyrelsen ansvarar för elektroniska kommunikationer. Inom Post- och telestyrelsen finns Sveriges IT-incidentcentrum (Sitic). Sitic samverkar med bland annat Rikspolisstyrelsen, Säkerhetspolisen och Verva i arbetet med att bevaka incidenter.

Energimyndigheten är central förvaltningsmyndighet för användning och tillförsel av energi, däribland el. Ansvaret inkluderar inte att förebygga eller operativt hantera elavbrott. Vid Energimyndigheten finns också Energimarknadsinspektionen. Inspektionen är nätmyndighet enligt ellagen och bedriver tillsyn över nätbolagen.

Svenska kraftnät AB ska verka för en robust elförsörjning.

Övriga myndigheter

Försvarsmakten[40] ska kunna genomföra underrättelse- och säkerhetsoperationer för att möta hot eller insatser mot civila mål. Försvarsmakten ska även hjälpa andra myndigheter att skydda prioriterade samhällsfunktioner och infrastrukturer. Myndigheten ska med tillgängliga resurser kunna bidra till samhällets samlade förmåga att hantera svåra påfrestningar i fred.

Försvarets materielverk utvärderar och certifierar IT-säkerhets-produkter.

Försvarets radioanstalt ska[41] öka samhällets förmåga att stå emot IT-relaterade hot genom att[42] stödja insatser vid kriser med IT-inslag, vara med och identifiera inblandade aktörer vid hot mot samhällsviktiga system och göra

38 KBM:s Regleringsbrev, år 2007.
39 Intervju, KBM, 2006-11-30.
40 Försvarsmaktens regleringsbrev, år 2007.
41 Försvarets radioanstalts regleringsbrev, år 2007.
42 Förordning (1994:714) med instruktion för Försvarets radioanstalt.

IT-säkerhetsanalyser. Anstalten har i särskilt uppdrag att göra penetrationstester, vilket man gjort för bland annat Riksbankens räkning.

Säkerhetspolisen (Säpo) ingår i *Rikspolisstyrelsen*. Säpo har en enhet för finansiell säkerhet.

Rikskriminalpolisen, som också är en del av Rikspolisstyrelsen, har en IT-brottssektion. Denna sektion utvecklar teknik och metoder samt är med och utreder IT-kriminalitet.

Ansvarsfördelning inom myndigheterna

Inom Finansinspektionen och Riksbanken är ansvaret för krisförberedande uppgifter som rör konventionella kriser respektive finansiella kriser skilda åt i organisationen. Säkerhets- och IT-avdelningarna förbereder för och förebygger tekniska hot och risker, medan andra avdelningar sköter tillsyn och övervakning av finansiella risker som hotar stabiliteten i det finansiella systemet. Dessa avdelningar samverkar. De har dock olika utgångspunkter för arbetet, och därför skiljer sig deras synsätt och de begrepp som används en del från varandra, liksom kraven på säkerhetsåtgärder.

4.3 Samverkan

4.3.1 Allmänt

Starka ömsesidiga beroenden inom betalningssystemet ställer stora krav på samverkan i krisplaneringen. Ett antal samverkansorgan och samverkansprojekt har därför initierats för bl.a. informations- och erfarenhetsutbyte. Myndigheterna samverkar framför allt inom Samverkansområdet för ekonomisk säkerhet (SOES). Samverkan mellan myndigheter och näringslivet sker inom den Finansiella sektorns privat-offentliga samverkansprojekt[43] (FSPOS). Post- och telestyrelsen har ett eget organ för samverkan med bl.a. teleoperatörer.

Riksbanken driver ”Referensgruppen för betalningssystemfrågor” med representanter från VPC, Bankgirocentralen, Stockholmsbörsen, Bankföreningen, Riksgäldskontoret och de fyra stora bankerna. Dessutom finns sedan länge ett samarbete mellan Regeringskansliet, Finansinspektionen och Riksbanken[44].

43 Här ingår bl.a. Riksbanken, Finansinspektionen, Bankföreningen, VPC, BGC, storbankerna och några försäkringsbolag.

44 **Memorandum of understanding on co-operation between the Banking Supervisors, central Bank and Finance Ministries of the** European Union in Financial Crisis situations.

4.3.2 *Myndighetssamverkan*

Samverkansområdet ekonomisk säkerhet

Sex samverkansområden har organiserats med stöd av krisberedskapsförordningen: teknisk infrastruktur, transporter, farliga ämnen, ekonomisk säkerhet, skydd, undsättning och vård samt geografiskt områdesansvar. Krisberedskapsmyndigheten anser att arbetet i samverkansområdena överlag fungerar väl och att ingående myndigheter generellt sett är aktiva och intresserade av samarbetet. Emellertid konstateras också att arbetsformerna behöver utvecklas[45] bl.a. när det gäller framtidsinriktning av krisberedskapen, privat-offentlig samverkan, den internationella dimensionen och forskning och utveckling.

Krisberedskapsmyndigheten rapporterar varje år om arbetet inom samverkansområdena till regeringen. Myndigheten organiserar också samverkansmötena och är sekreterare, men har inget uttalat ledningsansvar.

Samverkansområdet för ekonomisk säkerhet (SOES) omfattar enligt den nya krisberedskapsförordningen från år 2006 förutom Krisberedskapsmyndigheten numera fem myndigheter. Dessa är Riksgäldskontoret, Finansinspektionen, Tullverket, Skatteverket och Försäkringskassan. Det är hälften så många som tidigare. Ändå har Tullverket och Skatteverket skrivit till regeringen för att få dra sig ur samarbetet, men fått avslag. Riksbanken och länsstyrelser är adjungerade deltagare i SOES. Utifrån den tidigare krisberedskapsförordningen från år 2002 ställdes år 2005 ett antal mål upp för SOES verksamhet. Dessa är:

- Leda och samordna insatser så att samhällsviktiga ekonomiska system fungerar vid svåra påfrestningar.
- Motståndskraft i den elektroniska kommunikationen.
- Tillgodose samhällets behov av bränslen och drivmedel.

Privat-offentlig samverkan

På regeringens uppdrag tillsattes år 2003 en nationell styrgrupp för privat-offentlig samverkan. Styrgruppens slutsats blev att avtalsbaserad privat-offentlig samverkan (POS) bör integreras i det nya krishanteringssystemet. Det nya samverkanssystemet ”bör bygga på en öppen organisationsstruktur med lokala, regionala samverkansstrukturer och en gemensam central POS-funktion samt kvalitetssäkrade arbetsprocesser och frivilligt deltagande för den privata sektorn”. Styrgruppen föreslog att det år 2007 skulle finnas en organisationsstruktur, lagstöd och arbetsprocess för privat-offentlig samverkan.

45 KBM (2007) *Verksamheten i samverkansområdena under perioden den 1 september–31 december 2006.*

Vid ett möte med företrädare för den finansiella sektorn år 2005 startade Finansinspektionen ett privat-offentligt samverkansprojekt inom den offentliga sektorn (FSPOS). Projektets mål var att till juni 2006 utarbeta ett förslag på uppgifter, arbetsformer, mandat och syfte med ett permanent privat-offentligt samverkansorgan när det gäller sårbarhet inom den finansiella sektorn. FSPOS finansieras av Krisberedskapsmyndighetens medel via Finansinspektionen. I samarbetet deltar bland annat Finansinspektionen, Bankföreningen, Bankgirocentralen, Försäkringskassan, Fondhandlareföreningen, Försäkringsförbundet, Krisberedskapsmyndigheten, Riksbanken, Riksgäldskontoret, Sparbankernas riksförbund, Stockholmsbörsen och Värdepapperscentralen. Samarbetet vilar på ett samarbetsavtal.

4.4 Iakttagelser

4.4.1 Iakttagelser om ansvarsfördelning

Oklar ansvarsfördelning mellan Finansinspektionen och Riksbanken

Finansinspektionen och Riksbanken har enligt sina uppdragsbeskrivningar delvis samma mål – att främja det finansiella systemets stabilitet och effektivitet – men olika medel för att uppnå sina mål. Det gemensamma målet gör att överlappande verksamhet i viss mån är oundviklig. Finansinspektionen ska bedriva tillsyn över finansiella företag, i synnerhet över dem som har störst betydelse för systemets stabilitet. Riksbanken ska övervaka de stora bankerna och infrastrukturföretagen. Båda myndigheterna bildar sig löpande en uppfattning om tillståndet i den finansiella sektorn och om vilka finansiella hot som kan leda till en finansiell kris.

Även när det gäller att analysera hot och risker är ansvarsförhållandena delvis oklara. Å ena sidan ska Finansinspektionen göra en risk- och sårbarhetsanalys som omfattar hela den finansiella sektorn, inklusive det centrala betalningssystemet. Å andra sidan har Riksbanken genom sitt mer fokuserade uppdrag att främja betalningssystemet också denna uppgift. Riksbanken leder dessutom en referensgrupp med de främsta deltagarna i RIX-systemet. Riksbanken anser dock att Finansinspektionen formellt fått ansvar[46] för krisberedskap och krisplanering inom det centrala betalningssystemet. Finansinspektionen anser å sin sida att Riksbanken också ansvarar för att det centrala betalningssystemet fungerar även vid allvarliga störningar.

Varken Riksbanken eller Finansinspektionen anser sig enligt våra intervjuer[47] ha ett huvudsakligt ansvar för att *leda* samverkan och övningar mellan

46 Brev från Riksbanken till Riksrevisionen, 2007-10-25. I brevet hänvisar Riksbanken till det utskottsuttalande som gjordes i betänkandet 1994/95:FiU3 där det framgår att ”Utskottet tillstyrker regeringens förslag i prop. 1994/95:47 att ansvaret för beredskapsplaneringen inom det finansiella området flyttas från Riksbanken till Finansinspektionen.

47 Intervju, Finansinspektionen, 2007-10-02. Intervju, Riksbanken, 2007-09-19.

myndigheter samt mellan myndigheter och det privata näringslivet. Inte heller anser de sig ansvara för att lämna en *samlad* uppföljning och rapportering av krisberedskapen inom det centrala betalningssystemet. Finansinspektionen och Riksbanken har inget formellt mandat att begära ut uppgifter om allvarliga sårbarheter inom sina respektive ansvarsområden från till exempel Riksgälden eller Försäkringskassan.

Samtliga nämnda myndigheter deltar dock i de samverkansorgan som finns. Deltagarna i SOES respektive FSPOS anser sig inte vara skyldiga att lämna ut fördjupade risk- och sårbarhetsanalyser till övriga deltagare. Så har inte heller skett. Finansinspektionen har till exempel inte fått tillgång till de risk- och sårbarhetsanalyser som gjorts inom FSPOS arbetsgrupp Kritisk infrastruktur eller dess arbetsgrupp Betalningsförmedling.

Ansvaret för nationell informationssäkerhet och sammanställning av IT-incidenter är oklart vad avser betalningssystemet

För närvarande hanterar sju myndigheter under fyra departement frågor om informationssäkerhet. Bankerna och andra företag ska formellt sett rapportera incidenter inom betalningssystemet till Finansinspektionen, Riksbanken, Sitic och Krisberedskapsmyndigheten. Ingen samordnar dock denna rapportering. Ingen myndighet har tagit ett samlat ansvar för att övervaka IT-säkerheten inom det centrala betalningssystemet.

Riksgälden har begränsat sitt ansvar

Enligt Riksgäldens regleringsbrev ska myndigheten lämna en risk- och sårbarhetsanalys för hela det egna ansvarsområdet, inte enbart för den egna myndigheten. Riksgälden ansvarar för att statens betalningssystem är säkert. Men myndigheten har inte redovisat någon analys av risker och sårbarheter i hela den statliga betalningskedjan från myndighet till företag och medborgare.

Ansvaret för riskhantering är uppsplittrat inom myndigheterna

Det är olika avdelningar inom Finansinspektionen och Riksbanken som förbereder för hantering av konventionella respektive finansiella risker och kriser. De tillämpar delvis skilda synsätt, begrepp och krav på säkerhetsåtgärder. Företrädare för de olika traditionerna bedömer både risker och samband mellan olika risker på olika sätt. Till exempel kan en teknisk incident enligt flera bedömare inom krisberedskapstraditionen mycket väl gå över i en finansiell systemkris. Ansvariga för finansiella kriser är däremot något skeptiska

till möjligheterna att tekniska hot och risker kan gå över i en finansiell kris. Dessa grupper har därför olika uppfattning om vilken beredskap och vilka krisåtgärder som då behöver vidtas.

På Riksbanken finns två krisledningsgrupper. Beroende på krisens art kan alltså dessa grupper komma att arbeta parallellt. Riksbanken skriver själv i en promemoria[48] att ett sådant delat ansvar kan ”ge passivitet i pressade situationer, alternativt tidsödande beslutsprocesser där olika incitament ger olika uppfattningar om hur man ska gå tillväga”.

Direktionen förväntas inom kort besluta om ett antal ändringar i instruktionen som bl.a. berör krisorganisationen[49]. Ledningsgruppen för konventionella kriser, LKK, kommer enligt förslaget att avskaffas och dess uppgifter övertas av Riksbankens ledningsgrupp. Ledningsgruppen består av bankens avdelningschefer, vilket enligt banken innebär att krisledningen tydligare blir ett ansvar för bankens dagliga ledning.

Även inom Finansinspektionen analyserar och övervakar skilda avdelningar tekniska hot och risker inom det finansiella området. Säkerhetsavdelningen ska till exempel följa krisberedskapsförordningens krav, medan tillsynsavdelningarna följer Basel II-reglerna.

4.4.2 Iakttagelser om samverkan

Allmänna brister i samverkansområdena

De olika samverkansområdena arbetar på olika sätt: genom undergrupper, arbetsgrupper eller främst genom seminarier. Det finns ingen gemensam eller särskild utbildnings- eller uppföljningsplan för arbetet inom de olika samverkansområdena. Varje myndighet ansvarar också för att välja egna representanter i de olika samverkansområdena. Detta har medfört att ledamöterna representerar olika befattningsnivåer. Dessutom är instruktionerna för arbetet olika tydliga, och därmed varierar representanternas mandat, åsikter och rätt att delegera.

Myndigheternas samverkan inom SOES har gått trögt

I SOES ingår inte myndigheter som representerar den underliggande infrastrukturen som el, tele och energi eller myndigheter som är experter på informationssäkerhet. Riksbanken är dock adjungerad medlem. Krisberedskapsmyndigheten är endast sammankallande, och ordförandeskapet roterar bland de övriga deltagarna.

48 Riksbanken (2006) *Ansvar och samverkan för kontinuitets- och krisplanering i det finansiella systemet.*
49 Brev från Riksbanken till Riksrevisionen, 2007-11-01.

SOES har liksom andra samverkansområden tidvis haft problem med att finna konkreta arbetsuppgifter. SOES har emellertid utarbetat en verksamhetsplan som fram till våren år 2007 innehöll effektmål och leveransmål. En följd av detta är en gemensam skrivbordsövning och en studie av hur myndigheterna är beroende av varandra. SOES har också kartlagt flödet av till exempel girobetalningar- och pensionsutbetalningar.

Granskningen visar också att deltagarna i SOES efter fem år ännu inte enats om hur olika begrepp ska tolkas. De har inte heller lyckats uppdatera någon gemensam risk- och sårbarhetsanalys i enlighet med den nya krisberedskapsförordningen eller kunnat ge en gemensam och samlad bild av samhällets förmåga. Företrädare för flera myndigheter har framfört att SOES inte producerar något effektivt resultat och i SOES egna protokoll konstateras till exempel att samverkansområdet måste planera sin verksamhet mer aktivt, att deltagarna måste engagera sig aktivt även mellan mötena och att man behöver ett tydligare operativt fokus. I protokollen kritiseras också Krisberedskapsmyndighetens kommunikation som anses vara ”envägs med kort svarstid och med bristande lyhördhet för korrektion av faktafel”. Protokollen visar även att SOES avgränsat sitt arbete från centrala ämnesområden som uttryckligen utpekas i Krisberedskapsförordningens § 11, nämligen EU-frågor samt forskning och näringslivssamverkan. SOES har visserligen lämnat förslag på forskningsinsatser, men ett stort antal scenarier är inte kartlagda. Inte heller har SOES eller någon aktör på det finansiella beredskapsområdet initierat forskning om hot och risker samt långsiktiga effekter av att betalningssystemet står stilla.

Medan lagen och Krisberedskapsmyndigheten sätter SOES agenda, sätter medlemmarna själva agendan i FSPOS. SOES ställning i förhållande till FSPOS är oklar. Vissa aktörer ser FSPOS som ett komplement eller rent av som en arbetsgrupp under SOES, medan andra menar att FSPOS ersatt SOES eller att FSPOS och SOES behöver integreras. Även om FSPOS arbete redovisas på SOES möten, behandlar man inte underliggande dokument[50].

Krisberedskapsmyndighetens representanter känner till det arbete som pågår inom olika samverkansområden. På så sätt samordnas områdena till viss del, men vissa anser att samarbetet kan behöva stärkas.

Den privat-offentliga samverkan inom FSPOS har trots hög aktivitet allvarliga sekretess-, insyns- och kontinuitetsproblem

Finansinspektionen har tagit initiativ till att samverka med privata företag för att stärka den finansiella sektorns robusthet och förmåga att hantera kriser. Samverkan påbörjades år 2000 med en plan för arbetet som sträcker sig

50 Intervju. Försäkringskassan. 2007-03-02.

fram till år 2010. Finansinspektionen har själv bestämt hur arbetet ska gå till och stämt av arbetet och upplägget med Krisberedskapsmyndigheten.

Finansinspektionen anser att privat-offentlig samverkan ska vara frivillig, inte minst när den omfattar störningar av samhällelig art. Enligt Finansinspektionen behöver samverkan också planeras noggrant, och man måste sakta bygga upp förtroende.

Näringslivet har i första hand ett ekonomiskt intresse av att samverka. Ägarna måste förstå nyttan av investeringar och åtgärder om dessa ska kunna genomföras. Inspektionen anser att ägarna kan vara misstänksamma mot myndigheterna och rädda för att fel och brister ska avslöjas.

I FSPOS medverkar näringslivsrepresentanter aktivt i arbetet, såväl i sessioner som i särskilt inrättade mindre arbetsgrupper. Riksrevisionen har inte kunnat ta del av samtliga rapporter från arbetsgrupperna eftersom deltagarna inom FSPOS kommit överens om att inte lämna ut resultat från de privat drivna arbetsgrupperna till myndigheterna, inklusive Finansinspektionen. Denna typ av sekretess hindrar även olika arbetsgrupper inom FSPOS att rapportera till varandra. Myndighetsföreträdare får en övergripande muntlig rapport, men får inte ta del av underlagen på grund av bland annat banksekretess. Arbetsgruppen Kritisk infrastruktur har till exempel destruerat sina skriftliga dokument efter att översiktligt ha presenterat resultatet.

Arbetet har hittills lett till planer på en gemensam internetplattform, en kriskontaktlista, en kartläggning av betalningsströmmar, definitioner av samhällsviktiga och branschviktiga tjänster, prioriteringar av tidskritiska tjänster samt krav på redundans.

FSPOS leds av en beslutsgrupp med Finansinspektionen som ordförande. FSPOS har inte gjort någon gemensam analys av hotbilden som utgångspunkt för arbetet. Det saknas tydliga mål, men FSPOS arbetar ändå enligt Finansinspektionen effektivt, målinriktat och prestigelöst. FSPOS arbetar utifrån de risker och sårbarheter som identifierats vid Finansinspektionens scenarie- och krisledningsövningar.

FSPOS saknar också anknytning till Regeringskansliet. Gruppen fattar endast konsensusbeslut och saknar egna resurser. FSPOS är ett projekt, utan juridisk status, vilket har medfört problem, bland annat med sekretess, insyn och kontinuitet. FSPOS saknar också en arbetsgrupp för IT-hot. Man anser att IT-hot ska hanteras i andra projekt eller organ. Arbetsgruppen för omvärldsbevakning har kommit att handla mer om informationsdelning än om omvärldsbevakning, som är ett vidare fält och kräver mer resurser. Projektet har hittills administrerats med hjälp av konsulter. FSPOS har också initierat en av de största övningarna som genomförts inom den finansiella sektorn i Sverige.

4.5 Bedömning av ansvar och samverkan

Riksrevisionen bedömer att ansvarsfördelning och samverkan inte är utformade så att samhället på ett ändamålsenligt sätt kan förebygga och hantera allvarliga störningar i det centrala betalningssystemet.

Myndigheter och näringsliv samarbetar på ett konstruktivt sätt för att stärka den tekniska krisberedskapen i betalsystemet. De avgränsningar som finns i ansvarsfördelningen mellan centrala myndigheter medför dock att väsentliga sakområden inte behandlas på ett systematiskt sätt i beredskapsarbetet. Ett sådant sakområde är beredskapen mot tekniska hot och risker i betalsystemet, där ingen myndighet har ett uttalat krisledningsansvar eller tillgång till all samlad information. Därmed kan ingen samlad analys utföras av en centralt bemyndigad aktör med överblick över den samlade förmågan att hantera ett krisförlopp.

Riksrevisionen bedömer att en sådan centralt ansvarig aktör behöver utses och att det då är nödvändigt att betryggande former för överföring av sekretessbelagd information säkerställs. Inte heller de samverkansforum som ska få till stånd ett gemensamt arbete har tillgång till alla beslutsunderlag. I samverkansforum ingår inte alla de aktörer som Riksrevisionen bedömer vara av central betydelse för krisberedskapen i det centrala betalsystemet, exempelvis länsstyrelsen i Stockholm och Riksbanken, medan aktörer som ter sig mindre väsentliga i sammanhanget, till exempel tullen och Skatteverket, deltar.

Riksrevisionen bedömer att målsättningarna för samverkansarbetet är oklara, att krisberedskapsförordningen inte utvecklar vilket innehåll samverkansarbetet ska ha och att den inte knyter an till de övriga former för myndighetssamverkan, näringslivskontakter, regeringskontakter och forskarutbyte som uppstått eller behövs.

5 Förmåga att förebygga och hantera kriser

Revisionsfrågan i detta kapitel är följande:
Har berörda samverkansmyndigheter säkerställt att de själva och de finansiella företagen har en tillräcklig förmåga att förebygga och hantera kriser?

I detta asvnitt granskar vi sex väsentliga moment som den samlade förmågan byggs upp av:

1. *Risk- och sårbarhetsanalyser* som innehåller bedömningar av risker och konsekvenser samt analyser och förslag till åtgärder för ökad robusthet *(förebyggande åtgärder)*.
2. *Förberedelser för att kunna hantera kriser när den väl inträffar* (förberedande åtgärder för att uppnå krisledningsförmåga och operativ förmåga).
3. *Övningar* (som verifierar om förberedelser för att hantera kriser varit tillräckliga).
4. *Penetrationstester* (som kan verifiera robustheten i IT-systemen och upptäcka sårbarheter i dessa system).
5. *Incidentrapportering och incidentanalyser* (är viktiga för att kunna larma snabbt, lära av tidigare händelser och utveckla arbetet).
6. *Forskning* (för att täcka in kunskapsluckor, utveckla området och utforma nya metoder).

I bilaga 1 redovisas preciserade bedömningsgrunder för dessa åtgärder.

5.1 Genomförda risk- och sårbarhetsanalyser under åren 2003–2007

5.1.1 Vilka risk- och sårbarhetsanalyser har granskats?

Vi begränsar vår genomgång till de risk- och sårbarhetsanalyser som granskade myndigheter enligt krisberedskapsförordningen ska lämna till regeringen. I bilaga 1 redovisas vilka krav krisberedskapsförordningen respektive internationella standarder ställer på analyserna. Vad avser betalningssystemet är följande myndigheter intressanta: Finansinspektionen, Försäkringskassan, Riksgälden, Post- och telestyrelsen, Svensk kraftnät AB och Energimyndigheten.

För Riksbanken och samverkansorganen granskas de risk- och sårbarhetsanalyser som avser betalningssystemet. Rent formellt gäller inte krisberedskapsförordningen för Riksbanken eftersom förordningar bara gäller för myndigheter under regeringen. Riksbanken bedöms i stället efter de internationella standarder banken kommit överens om att följa.

Statskontoret har på regeringens uppdrag granskat de analyser som görs av myndigheter under Finansdepartementet. Riksrevisionen har låtit Roland Heickerö, FOI, bedöma de risk- och sårbarhetsanalyser som gjorts av granskade myndigheter.

5.1.2 Iakttagelser om risk- och sårbarhetsanalyser

Riksbanken har ingen samlad risk- och sårbarhetsanalys

Riksbanken började år 2002 avdelningsvis analysera och kartlägga kritiska system och processer inom den egna verksamheten[51]. Analyserna gjordes av personal inom Riksbanken. Riksbanken tillämpar den brittiska standarden för kontinuitetsplanering[52]. Detta innebär bland annat att banken genomför så kallade Buisiness Impact Analysis (BIA) och risk- och sårbarhetsanalyser utifrån ett sådant synsätt. En utgångspunkt i dessa analyser är de hot som har stora eller oacceptabla konsekvenser för verksamheten, även om hoten är mindre sannolika eller helt osannolika. I dagligt tal kallas detta ”Worst-Case-Scenarios”. Riksbanken menar dock att det inte är fruktbart att ta upp alla de hot och risker som kan drabba verksamheten, eftersom dessa inte ens alltid är möjliga att föreställa sig[53]. Riksbanken har därför i stället identifierat ett antal huvudkonsekvenser som bankens kontinuitetsplanering bygger på.

Riksbankens möjlighet att förebygga störningar i banksystemet och i infrastrukturen bygger i huvudsak på bankens förmåga att identifiera risker och påverka de aktörer som är viktiga för stabiliteten i det finansiella systemet, det vill säga banker och systemviktig infrastruktur. Riksbanken har operativt ansvar för RIX och för detta system utför banken särskilda säkerhetsanalyser. Under senare år har det etablerats ett antal internationella standards och normer med minimikrav för betalnings- och avvecklingssystem. Sedan år 2002/03 utvärderar Riksbanken Bankgirocentralen, Värdepapperscentralen och Stockholmsbörsen enligt dessa krav. Det är dock företagen som själva ansvarar för riskanalyser inom den egna organisationen. Avsikten är att Riksbanken framöver ska göra uppföljningar av utvärderingarna. Riksbanken deltar även i utvärderingen av vissa internationella system.

---

51 Riksbanken, *Sammanställning av resultatet av Verksamhetsberoendeanalyser och Hot- och riskanalyser, år 2002 och 2003.*

52 **British Standards. BS 25999** *Business Continuity assessment Online,* spring 2007.

53 Dessa konsekvenser täcker enligt Riksbanken in de flesta hot och risker som kan medföra de uppräknade konsekvenserna och som behöver någon form av teknisk, administrativ eller organisatorisk kontinuitetslösning. Riksbanken gör även risk- och sårbarhetsanalyser samt riskhantering löpande. Dessa analyser är i första hand till för att identifiera de skyddsåtgärder som krävs för att möta identifierade risker inom ramen för den aktuella analysen.

Riksbanken har också under ett par års tid aktivt verkat i olika sammanhang för att sprida information om hur betalningssystemet fungerar och hur enskilda aktörers ställningstaganden inom kontinuitets- och krisplaneringen påverkar helheten. Diskussionerna har bland annat förts inom samverkansgrupperna SOES och FSPOS. I dessa sammanhang har kartläggningar av flödet av betalningstjänster genomförts för att identifiera beroenden och för att kunna diskutera vilket ansvar varje organisation har i händelse av kris. Diskussionerna har ökat medvetenheten om att alla inblandade måste ha en rimlig nivå på sin kontinuitets- och krisplanering och att samverkan behövs för att säkerställa gemensamma intressen som exempelvis tillgången till grundförutsättningar som el, tele, bränsle och vatten. Analysresultaten har dock inte dokumenterats i en samlad rapport. De finns beskrivna i presentationsmaterial, i ett internt PM och i ett tal som hölls av vice riksbankschefen Eva Srejber på Sveriges Säkerhetsting år 2006.

Två penetrationstester har utförts av Försvarets radioanstalt vid Riksbanken under år 2004. Det ena testet avsåg det externa datorverket och det andra det interna datornätverket. Resultatet av dessa tester redovisas i en sekretessbelagd bilaga till denna rapport.

Riksbanken har sammanfattningsvis inte ställt samman en risk- och sårbarhetsanalys för det centrala betalningssystemet och kontantförsörjningen i sin helhet. Riksbankens riskanalyser är spridda över olika avdelningar, dokument och aktiviteter. Europeiska centralbanken kommer framöver att kräva att krisplaner ska finnas hos finansiella företag inklusive centralbanker som innefattar ett brett urval av tänkbara scenarier, till exempel naturkatastrofer, olika typer av avbrott och terroristattacker. Riksbankens analyser har inte haft en sådan ansats. Riksbankens verksamhetsanalyser under åren 2002-04 avsåg huvudsakligen konsekvenserna av att en enhet eller funktion inte fungerar inom Riksbanken, inte sannolikheter för att något ska inträffa som kan leda till att det centrala betalningssystemet i sin helhet inte fungerar. Konsekvenserna för samhället i andra och tredje led har inte belysts i dessa analyser. Däremot har de analyser som sker inom FSPOS haft denna ambition.

Risk- och sårbarhetsanalyser hos myndigheter under regeringen har betydande brister

Statskontoret konstaterar i sin genomgång att sårbarheter ofta är bristfälligt analyserade. Exempelvis är följdeffekterna i samhället ofta dåligt belysta i myndigheternas redovisningar. Detsamma gäller analyser av var gränserna går för samhällets förmåga. Analyser av resursbehov vid mer allvarliga händelser saknas också.

Riksrevisionens egen granskning av myndigheternas risk- och sårbarhetsanalyser[54] bekräftar bilden från Statskontorets analyser. Av sammanställ-

54 Följande myndigheters risk- och sårbarhetsanalyser har granskats av Riksrevisionen: Finansinspektionen, Riksgälden, Försäkringskassan och Post- och telestyrelsen.

ningen i tabell 5.1 framgår också att analyserna ofta utelämnar vissa typer av risker och hot. Antagonistiska hot samt risker och sårbarheter som gör att systemen kan manipuleras behandlas sällan, inte heller möjligheterna till insiderproblem och risker för utpressning. Det saknas även bedömningar av sannolikheter för att hoten ska realiseras, liksom i många fall vad konsekvenserna kan bli av dessa hot. Hot, risker och sårbarheter är sällan så specificerade att det går att bedöma lämpliga åtgärder. I flera fall framgår inte heller åtgärder för att hantera identifierad risk eller sårbarhet. Ofta beaktas inte andra myndigheters identifierade risker och åtgärder. Kostnaderna för åtgärder uppskattas nästan aldrig. Underlagen är ofta löst hållna och oprecisa till sin karaktär. Tekniska analyser saknas i allmänhet, liksom ingående beskrivningar av vilka typer av hot som kan förekomma och med vilka medel eller på vilka vägar dessa hot kan realiseras. I en sekretessbelagd bilaga, H1, redovisas exempel på risker och sårbarheter som inte återfinns i Försäkringskassans och Riksgäldens risk- och sårbarhetsanalyser, men som myndigheterna i andra sammanhang har identifierat.

Tabell 5.1 Risk- och sårbarhetsanalyser utifrån beredskapsförordningens krav

	Krav enligt beredskapsförordningen m.m.	**Enskilda myndigheters RSA**
1	Årligen genomfört RSA år 2003–2006.	Görs inte alltid
2	RSA bör ha ett samhällsperspektiv. Ej endast avse egen verksamhet.	Görs inte alltid
3	Hot, risker och sårbarheter bör vara identifierade och hållas isär.	Görs inte alltid
4	Möjlighet att bedöma sannolikheten för att risk/hot ska realiseras bör framgå.	Framgår sällan
5	Konsekvenser av realiserade hot och risker bör framgå.	Framgår sällan
6	Metod för analysernas genomförande bör framgå eller hänvisas till.	Framgår sällan
7	Hot, risker och sårbarheter specificerade att det går att bedöma lämpliga åtgärder.	Framgår sällan
8	Åtgärder för att hantera identifierad risk och sårbarhet bör framgå.	Framgår sällan
9	Behovet av ytterligare åtgärder bör anges.	Görs inte alltid
10	Åtgärder relaterade till identifierad hot, risk eller sårbarhet och konsekvenser.	Görs inte alltid
11	Åtgärder identifierade av andra myndigheter och organisationer bör analyseras.	Görs sällan
12	Kostnaderna för åtgärder bör uppskattas och relateras till ev. skadekostnader.	Görs nästan aldrig

Samverkansorganens risk- och sårbarhetsanalyser är begränsade

För att skapa en gemensam syn på risk- och sårbarhetsanalyser har man inom SOES[55] genomfört en s.k. morfologisk analys[56]. Analysen gjordes med stöd av FOI. Avsikten var att skapa en gemensam begreppsapparat och hotbild. Avsikten var också att göra beroendena mellan myndigheterna och omvärlden tydliga.

Analysen visade att ett antal samverkande faktorer måste beaktas när risker för skador värderas. Det gäller till exempel faktorer som tid, drabbade aktörer och system, reservalternativ, beroenden av system och organisationer, geografisk omfattning och komplexitet. Flera olika typer av hot och konsekvenser omnämns, men bara allmänt. Överlag uppfattades denna analys som alltför teoretisk.

Ska vara Deltagarnai SOES anser inte att de analyser som hittills gjorts inom samverkansområdet uppfyller kraven på en gemensam risk- och sårbarhetsanalys[57]. Behovet av att skapa gemensamma metoder och synsätt för samtliga samverkansområden påpekades också.

Det huvudsakliga arbetet inom FSPOS har bedrivits i särskilda arbetsgrupper under våren och hösten år 2007. Bland annat har arbetsgruppen Kritisk Infrastruktur gått igenom kritiska beroenden av el, tele och vatten. En rapport har ställts samman under våren. Rapporten har dock inte lämnats till andra utanför arbetsgruppen. Arbetsgruppen har bestått av representanter från privata företag.

Dessutom har en så kallad avbrottskonsekvensanalys genomförts i två steg inom arbetsgruppen Betalningsförmedling. Analysens mål är att utreda konsekvenserna vid utslagning av kritiska aktörer i betalningsväsendet. Analysen ska också identifiera och föreslå konkreta förbättringsåtgärder. I den första delen av analysen får deltagarna ge synpunkter på konsekvenser för organisationen och samhället i stort av ett längre avbrott hos deltagarna. Den andra delen genomförs en tid senare och ska identifiera åtgärder som kan minska sårbarheten inom det centrala betalningssystemet. Delar av åtgärderna som föreslagits har prövats i en övning den 27 september år 2007. En viktig del i det framtida arbetet är att kartlägga hur systemrisken påverkas av att många aktörer har samma leverantörer.

55 I dokumentet *Sammanställning av RSA-arbetet inom SOES, 2005,* finns en summering av SOES arbete med att ta fram risk- och sårbarhetsanalyser.
56 En morfologisk analys syftar till att bringa reda i – ge form åt – komplexa sammanhang där många faktorer samspelar med varandra på ett svåröverskådligt sätt.
57 SOES (2005) *Sammanställning av RSA-arbetet inom SOES.*

5.1.3 *Bedömning av risk- och sårbarhetsanalyser*

Riksrevisionen kan konstatera att det finns betydande brister i myndigheternas analyser av risker och sårbarheter i det centrala betalningssystemet. En heltäckande analys av tillräcklig kvalitet är en förutsättning för att regering och myndigheter ska kunna bedöma vilka förebyggande åtgärder som måste vidtas för att betalningssystemet ska bli tillräckligt robust och motståndskraftigt. Därmed är också förmågan att vidta förebyggande åtgärder enligt vår bedömning bristfällig. Skälen till denna bedömning är följande.

- En samlad bild saknas. Det finns i dag ingen samlad bild av hot, risker, sårbarheter inom det samhällsviktiga betalningssystemet och vilka konsekvenser detta kan få i olika händelseförlopp. De risk- och sårbarhetsanalyser som hittills tagits fram av myndigheter, Riksbanken och samverkansorganen[58] kan utgöra delar i ett underlag till en sådan sammanställd bild, men dessa analyser är antingen mycket summariska eller tar inte med resultat från analyser som gjorts av andra myndigheter och finansiella institut eller utelämnar väsentliga delar av betalningssystemet. Det saknas också en sammanställning och analys av möjliga åtgärder samt kostnader och effekter för dessa.

- Analyserna är överlag löst hållna och allmänna till sin karaktär. Tekniska analyser saknas ofta, liksom fylliga beskrivningar av vilken typ av hot som kan inträffa, av vem eller av vad hotet kan utlösas och med vilka medel eller på vilka vägar. Sårbarheter och risker för manipulation av systemen behandlas sällan i analyserna. Inte heller möjligheter till en insiderproblematik och risker för utpressning. Vilken typ av skada skulle till exempel en initierad individ eller grupp kunna ställa till med i ett samhällsviktigt system samt vilka effekter och konsekvenser skulle kunna uppstå? Inte heller diskuteras vilka möjligheter som i dag finns att skydda informationssystemen från antagonistiska angrepp. Flera av Krisberedskapsmyndighetens hotscenarier analyseras inte alls eller i begränsad utsträckning. Det gäller t.ex. terroristhot med EMP-vapen[59], översvämningsscenariot i Stockholms innerstad, mera omfattande datahaverier och Internetkrascher. I någon mån gäller det också säkerhetsbrister i informationssystemen.

  Bristen på analyser av el- och teleberoendet i betalningssystemet påtalas ofta i intervjuer. I de risk- och sårbarhetsanalyser som Energimyndigheten och Svenska Kraftnät AB lämnat saknas en analys av sårbarheter i regionala och lokala nät. Det gäller också det ömsesidiga

58 Det har varit anledningen till att vissa analyser genomförts inom ramen av FSPOS och SOES, dvs. syftet har delvis varit att skapa en sådan bild, ett arbete som alltså har initierats av Finansinspektionen och Riksbanken.
59 EMP står för Elektromagnetisk puls.

beroendet mellan el- och teleförsörjningen och vilka konsekvenser det kan få inom samhällsviktiga områden som t.ex. betalningssystemet.

Konsekvenser av realiserade hot och risker beskrivs ofta endast mycket översiktligt. Det gör det svårt att identifiera vilka skadeverkningar som kan komma att inträffa och vilka åtgärder som kan behöva vidtas. Sårbarheter, hot och risker samt åtgärder identifierade av andra myndigheter och organisationer analyseras sällan. Kostnader finns sällan med i analyserna.

- Risk- och sårbarhetsanalyser som görs i privat-offentlig samverkan har flera begränsningar. Finansinspektionen och Riksbanken menar att den privat-offentliga samverkan som sker inom FSPOS kommer att bidra till att identifiera risker, hot och sårbarheter. Bankerna och infrastrukturföretagen avser dock inte att lämna ut sina risk- och sårbarhetsanalyser till myndighetsrepresentanterna. Det betyder att staten sannolikt inte kan förvänta sig att det inom FSPOS kommer fram en tillräckligt inträngande bild av sårbarheter i det centrala betalningssystemet. Finansinspektionen menar dock att sekretessfrågan är avgörande och att en utredning pågår för att undanröja problemen med sekretess. Finansinspektionens hoppfulla slutsats motsägs av flera av våra intervjuade från både myndigheter och privata institut. Dessa personer hävdar bestämt att de inte kommer att lämna ut några mer ingående tekniska risk- och sårbarhetsanalyser till andra aktörer. Risken är då påtaglig att analyserna blir begränsade till sitt innehåll; sannolikt utesluts de avgörande sårbarheterna i dessa analyser. Sådana begränsade analyser kan snarast vara till nackdel om de accepteras som fullödiga och kompletta.

- Osäkerheten i analyser och bedömningar redovisas sällan. Många av de analyser som myndigheterna redovisar bygger alltså på begränsade underlag och på oprecisa analyser. Hur man gått till väga för att komma fram till slutsatser och bedömningar framgår ofta inte, inte heller om underlag, information och kunskaper egentligen saknas för att kunna göra bra analyser.
  Inslaget av externa och oberoende utvärderingar är litet. De externa tester av sårbarheter som gjorts av utomstående har främst förekommit på området informationssäkerhet. Resultatet av testerna redovisas i en hemlig bilaga. I de fall konsulter har anlitats har myndigheterna ofta använt samma konsultföretag.

5.2 Förberedelser för att kunna hantera kriser

5.2.1 Finansdepartementets och myndigheternas förberedelser

Vilka förberedelser som myndigheter enligt regeringens beslut ska göra för att snabbt hantera en kris framgår av bilaga 1. I samma bilaga finns också angivet vilka bedömningskriterier som Riksrevisionen använt i granskningen av operativ krishanteringsförmåga. De myndigheter som granskats är Finansinspektionen, Försäkringskassan, Riksgälden och Riksbanken. Dessutom har vi granskat Finansdepartementets förberedelser enligt samma kriterier. Förberedelserna har granskats via dokumentationen i krishanteringspärmar och manualer m.m. samt genom de analyser och bedömningar myndigheterna själva har gjort av dessa förberedelser[60]. Genomgången av dokument har kompletterats med intervjuer på myndigheterna. Fil. dr Johannes Malminen vid FOI har på uppdrag av Riksrevisionen analyserat det framtagna underlaget. Av analysen framgår följande.

5.2.2 Iakttagelser om förberedelser för att akut hantera en kris

Krisplaner har inte uppdaterats

De krisplaner som för närvarande gäller vid granskade myndigheter är beslutade två till tre år tillbaka i tiden. Vid övningar som myndigheterna genomfört har flera allvarliga brister i planerna uppmärksammats. I flertalet fall har myndigheterna fattat beslut att uppdatera planerna. Ingen ny plan är dock slutgiltigt fastställd och beslutad av myndigheterna. Samtliga myndigheter uppger i intervjuer att deras planer har eller ska uppdateras. Skälet till att de nya planerna ännu inte har beslutats är att vissa åtgärder ännu saknas. Vid flera av de övningar som genomförts av myndigheterna har deltagarna haft problem med vilken plan som egentligen gäller. Äldre planer beslutade har funnits tillsammans med uppdaterade, men inte beslutade planer. Det har skapat en oklarhet om vilken planering som egentligen gäller.

Ingen ”Tjänsteman i beredskap” som uppfyller regeringens krav

Ett snabbt sätt att komma i gång med krishanteringsarbetet är att ha en ”Tjänsteman i beredskap” (TIB)[61]. Regeringen har beslutat att 40 myndigheter ska ha en ”Tjänsteman i beredskap”, dock ingen myndighet inom den

60 Förmågeredovisningar som regeringen har efterfrågat i regleringsbrev och som även skickats till och ställts samman av KBM.
61 Krisberedskapsmyndigheten har på uppdrag av regeringen definierat hur en sådan funktion ska vara utformad och föreslagit vilka myndigheter som ska ha en sådan funktion. Regeringen har därefter fattat beslut om vilka myndigheter som ska ha en ”Tjänsteman i beredskap”.

finansiella sektorn. Ingen av de granskade myndigheterna har heller på eget initiativ inrättat en ”Tjänsteman i beredskap” som uppfyller kraven på en sådan tjänsteman. Därmed saknas i viss mån en förmåga att snabbt fatta beslut om åtgärder och möjligheter att i ett tidigt skede svara för myndighetens initiala uppfattning. De störningar inom betalningssystemet som kan inträffa kan dock ha ett mycket hastigt förlopp. I vissa fall handlar det om timmar eller enstaka dygn innan en allvarlig kris kan vara för handen.

Kontakterna med underrättelseväsendet inte formaliserade

Det finns också brister i myndigheternas kontakter med underrättelseväsendet. Det borde ligga i både finanssektorns och underrättelsemyndigheternas intresse att upprätta formaliserade kanaler för utbyte av information. Finansinspektionen har ställt denna fråga vid flera tillfällen, men responsen från underrättelsemyndigheterna har dock uteblivit.

Brister i delegerings- och ersättningsordning samt rollfördelning

En tydlig delegerings- och ersättningsordning är viktig för att öva rätt personer och mentalt förbereda personalen i övrigt på vad som kan komma att begäras i en krissituation. Det finns i vissa fall brister i utformningen av delegerings- och ersättningsordningen i myndigheternas krisledningar och övriga krisorganisation. Ibland är till exempel inte ersättare utsedd och man kan därmed ifrågasätta både uthålligheten och förberedelserna hos personalen i organisationen. Vid flera av de övningar som genomförts har rollfördelningen inom krisorganisationerna varit oklar.

Ledningsfunktion saknas inom sektorn

Krisberedskapsmyndigheten ska årligen lämna förslag till vilka myndigheter som har ansvar och skyldighet att ha förmåga att vid en kris omgående kunna upprätta en ledningsfunktion för bland annat samordning och information. Förslaget skall lämnas till regeringskansliet vid samma tidpunkt som årsredovisningen. Krisberedskapsmyndigheten har inte föreslagit att någon myndighet inom den finansiella sektorn ska ha en sådan funktion.

Dubbla krisorganisationer

En viss brist i Riksbankens ledningskompetens, men också i bankens generella krishanteringsupplägg, ligger i att instruktionen skapat två krisledningsorganisationer. Det finns ingen tydlig information om hur Ledningsgruppen för konventionella kriser (LKK) och Ledningsgruppen för störningar i det finansiella systemet (LSF) ska förhålla sig till varandra i den fastställda LSF-planen. I LKK:s plan står det att frågor som inte kan hanteras genom samråd mellan grupperna avgörs av riksbankschefen eller dennes ställföreträdare. Direktionsmedlemmar uppger i en intervju att de två krisledningsorganisationerna inte ska uppfattas som stuprör, utan att båda aspekterna måste samarbeta för att hantera kriser som spiller över organisationsgränsen.

Risken är dock, medger Riksbanken i en promemoria, att det ”blir konflikter, mandatproblematik och för mycket folk inblandade för att snabbt kunna fatta effektiva beslut i en oklar krissituation som har både konventionella och finansiella ingredienser”[62]. Även resultat från två övningar som Riksbanken genomfört under de senaste två åren visar att så kan bli fallet.

Oklara rutiner för att skapa en gemensam lägesbild för myndigheterna

En av de viktigaste uppgifterna vid en akut kris är att myndigheterna tillsammans med branschen snabbt skapar sig en god bild av läget. Det nämns förhållandevis lite i myndigheternas planer om hur det ska gå till att skapa en sådan gemensam lägesbild. Riksbanken nämner knappast något i sin LKK-plan om vilka rutiner för att snabbt skapa och upprätthålla en lägesbild. Otydligheten med ledningsorganisationen som redovisats ovan gör det extra viktigt för Riksbanken att ange principer och processer för hur en lägebild ska tas fram och av vem i både LKK och LSF. Myndigheternas lägesbild är viktig både för att organisationen internt ska förstå beslut som fattas, men framför allt för hur sektorn sammantaget ska kunna hantera läget på ett tillfredställande sätt. Hur en gemensam lägesbild ska tas fram har förberetts i mindre utsträckning.

Få förberedelser för samverkan utanför finanssfären

Flera av myndigheterna har inte förberett samverkan med myndigheter utanför den direkta finanssfären. I några fall pågår arbete - som ännu inte är klart - med att åstadkomma sådana föreberedelser, till exempel inom Finansinspektionen och FSPOS.

62 Riksbanken (2006). *Ansvar och samverkan för kontinuitets- och krisplanering i det finansiella systemet.*

Eftersom samtliga myndigheter särskilt påpekar behovet av fungerade el- och teleförbindelser för att upprätthålla den egna verksamheten och det centrala betalningssystemet förefaller det väsentligt att förberedelser för samverkan borde ha genomförts med myndigheter och företag utanför finanssektorn, till exempel Post- och telestyrelsen, Svenska kraftnät AB, Energimyndigheten och Fortum. Myndigheterna förlitar sig visserligen på sina egna reservrutiner, men utan samverkan blir det svårare att påverka aktörer, vars verksamhet kan komma att ha direkt påverkan på myndigheternas egen förmåga att upprätthålla sina prioriterade funktioner.

Visserligen behöver inte samverkan ske fysiskt utan kan i många fall skötas via telefon eller liknande. Om fysiska möten krävs, menar några av myndigheterna att platsen kommer att avgöras när väl en kris inträffat. För den egna organisationens förberedelser anges alltid vikten av att ha en plats, ett förberett rum där krisledningen samlas. Det kan förfalla viktigt att det också finns en sådan förberedd mötesplats för de samverkande parterna. För närvarande finns inte sådana utsedda.

Samverkan försvåras också av att uppdaterade kontaktlistor på samverkansparter inte finns med i krismanualerna förutom på Finansdepartementet[63]. Några myndigheter uppger dock att man lagt kontaktlistor hos ansvariga i stället.

Alternativa arbetsplatser alltför nära varandra

Samtliga alternativa arbetsplatser hos granskade myndigheter ligger förhållandevis nära befintliga lokaler. Riksbanken följer som tidigare nämnts internationella standarder som rekommenderats av CPSS[64]. CPSS - och framöver även Europeiska centralbanken - rekommenderar att viktiga aktörer inom betalningssystemen ska ha ett andra arbetsställe och att detta arbetsställe inte ska vara beroende av samma kritiska infrastruktur som det primära arbetsstället nyttjar. Dessa krav uppfyller i dag inte centrala myndigheter och finansiella företag i Stockholm.

Myndigheterna har inte heller systematiskt undersökt vilka möjligheter som finns att kommunicera mellan finansiella aktörer och institutioner på ett alternativt sätt och från alternativa arbetsplatser vid störningar i telesystemet eller övat sådana situationer. Finansinspektionen uppger dock att detta delvis har övats i FSKLÖ[65], då en kurir gick mellan företag och myndigheter för att lämna underlag och utbyta information.

63 Riksbanken har dock vid faktagranskning meddelat att respektive verksamhetsdel ansvarar för sina kontaktuppgifter. Detta gör Riksbanken för att slippa en centraliserad administration.
64 Se not 18.
65 *Intervju, Finansinspektionen, 2007-10-24.*

Förberedelser för att sprida gemensam information kan behöva förbättras

Det finns brister i förberedelserna för att sprida gemensam information till omvärlden. I flera fall ingår inte i planläggningen att till exempel ha förberett ansvar och rutiner för gemensamma inforamtionsinsatser. Så elementära ting som adressuppgifter saknas ofta eller är inte uppdaterade.

När det gäller satellittelefoner som alternativ kommunikationsväg finns sådana telefoner endast i mycket begränsad omfattning. Om el- och telekommunikationer skulle slås ut förefaller sektorns informationsspridning vara sårbar. Centraliseringen av finanssektorns aktörer gör i och för sig att man kan mötas öga mot öga, men samtidigt kan en lokalt begränsad, men kraftig störning slå ut kommunikationerna med den globala finansmarknaden, som också är viktig när det gäller informationsspridning.

Förberedelserna har fokus på den egna myndigheten och inte på allmänheten

Vad gäller förberedelser för att minska skadeverkningar och återställa funktioner har dessa främst fokuserat på åtgärder inom den egna myndigheten, i mindre utsträckning på den gemensamma infrastrukturen och att minska skadeverkningarna för allmänheten. De åtgärder som anges i krisplanerna handlar ofta till exempel om att höja skalskydd kring byggnader och datoranläggningar i en krissituation. I vissa fall finns reservrutiner förberedda. Försäkringskassan har till exempel kommit överens med bankerna om att använda förra månadens uppgifter för utbetalningar av bidrag. Riksbanken har bland annat manuella reservrutiner att tillgå, ifall RIX-systemet inte fungerar.

Få förberedelser av brist på kontanter

Riksbanken har också ett strategiskt beredskapslager av kontanter att tillgå om det skulle bli problem i kontantförsörjningen. Dock saknar staten i dag ett reservsystem för att distribuera kontanter till allmänheten om de ordinarie distributionskanalerna – banker och bankomater – är utslagna; det vill säga om de privata företagens reservåtgärder inte har räckt till. Riksbanken anser att det är dess uppgift att försörja landet med sedlar och mynt (grossistfunktion), inte distribuera dem (detaljistfunktion). Det föreligger således en problematisk situation om till exempel el-, tele- och IT-förbindelserna är utslagna under en längre period. Ingendera av Riksbanken eller Finansinspektionen vidkänner ett ansvar för att utreda vilka möjligheter som står till buds och vilka åtgärder som kan behöva förberedas innan en kris i kontant-

försörjningen inträffar. De förberedelser som skulle behöva göras handlar om att analysera risker, sårbarheter och konsekvenser av en sådan störning samt möjliga reservåtgärder. Vare sig Riksbanken eller Finansinspektionen har således utrett möjligheterna att upprätthålla kontantförsörjningen vid ett omfattande elavbrott. En sådan utredning eller analys skulle framför allt behöva klargöra vad som skulle kunna underlätta medborgarnas kontant- och betalningsproblem på olika sätt. Till exempel skulle äldre system med manuella kortdragare kunna användas som reservrutin eller medborgarna kunna få anstånd med betalningar som har förfallit och få möjligheter till krediter vid köp av livsnödvändigheter etcetera. Det torde finnas stora möjligheter att göra långtgående förberedelser för att upprätthålla kontantförsörjningen och att ha gjort klart vem som distribuerar till vilken plats och på vilka villkor. När tillgången till kontanter är slut kan också nya betalningssätt utvecklas, till exempel skuldbevis. Dessa är dock beroende av trovärdigheten hos de personer eller företag som utfärdar dem. De som inte har denna trovärdighet kan få problem. Även ordande former skuldbevis och av anstånd med betalningar kommer att behövas, vilket också torde behöva förberedas.

5.2.3 Bedömning av förberedelser att hantera kriser

Enligt Riksrevisionens bedömning är det i dag inte säkerställt att aktörernas krisledningar fungerar väl tillsammans när en kris inträffar. Krisplaner som både är beslutade och uppdaterade har saknats. Det saknas också en ”Tjänsteman i beredskap” och en ledningsfunktion inom sektorn. Aktörerna har inte förberett sig tillräckligt tillsammans på händelseförlopp som kan få allvarliga skadeverkningar för samhället, till exempel på att ta fram en gemensam lägesbild eller samverka med aktörer utanför den finansiella sfären. De saknas också förberedelser för den händelse att brist på kontanter uppstår.

Om genomtänkta förberedelser saknas riskeras omfattande skadliga konsekvenser. Risker för konflikter och att för många personer eller personer med otillräcklig kompetens ska hantera en oklar krissituation ökar också. Bortfall av centrala delar av betalningssystemet kan snabbt få långtgående konsekvenser för samhället. Då ställs stora krav på ett snabbt och genomtänkt agerande.

5.3 Övningar inom det finansiella systemet

5.3.1 Granskade övningar

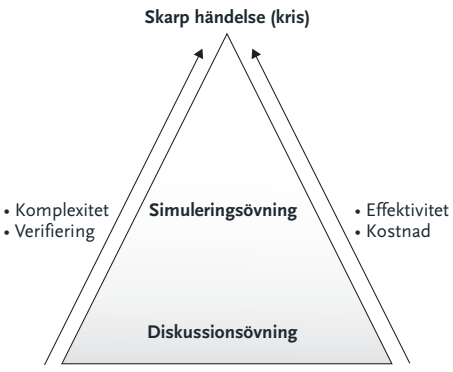
Denna kartläggning har avgränsats till övningar som behandlat tekniska hot och risker inom det finansiella systemet mellan januari år 2003 och oktober år 2007[66]. Kartläggningen innefattar övningar där någon av myndigheterna från det finansiella systemet övat eller varit med och arrangerat övningen. Avgränsningarna innebär att vi har kartlagt och analyserat 30 övningar[67]. Det är viktigt att påpeka att övningar som av olika skäl inte ingår i denna analys, också har en positiv inverkan på beredskapen.

Övningarna kan delas in efter olika aspekter och kategorier beroende på vad som ska belysas. Vi har valt att dela in och analysera övningarna efter form, syfte, omfattning, kontinuitet, moment som övats samt erfarenheter och återkoppling. För att ge en så tydlig bild som möjligt av övningsverksamheten har vi valt att använda oss av följande två begrepp.

Under en *diskussionsövning* samlas deltagarna för att diskutera hur myndigheten kommer att agera utifrån ett givet scenario. Övningsformen används för att i grupp teoretiskt analysera olika problemställningar och diskutera fram lösningar utan tidspress.[68] En del myndigheter kallar detta scenarioövning, ”table top”-övning, seminarieövning och skrivbordsövning.

En *simuleringsövning* är, till skillnad från en diskussionsövning, mer lik en kris genom att de övade agerar som om det vore en kris. En simuleringsövning innehåller motspel av exempelvis massmedier. En simuleringsövning är främst lämplig om målet är att pröva funktioner, organisation, samverkansformer med mera.[69] Denna form av övning kallas även för krisledningsövning och skarp övning.

Bild 5.1 Olika typer av övningar inom det finansiella systemet



Bilden är en omarbetning av 4 C Strategies beskrivning av olika typer av övningar.

66 Det innebär att övningar som skett i samspel, men handlar om en renodlad finansiell kris inte ingår i kartläggningen.
67 Övningarna fördelar sig mellan ansvariga enligt följande: Finansinspektionen = 7st (här räknas alla bankövningar under ett år som en övning då övergripande scenario varit detsamma. Endast storbankerna, VPC, BGC och Stockholmsbörsen räknas med här). Försäkringskassan = 6st, Krisberedskapsmyndigheten = 0st, Post- och telestyrelsen = 2 st, Riksbanken= 9 st, Riksgäldskontoret = 4 st, SOES = 1st och FSPOS =1 st.
68 Krisberedskapsmyndigheten (2007) *Öva krishantering.* s. 33.
69 Krisberedskapsmyndigheten (2007) *Öva krishantering.* s. 34.

Det finns alltså olika sätt att använda sig av övningar. Flertalet av de övningar som kartlagts är simuleringsövningar[70]. På vissa av dessa övningar har övningsledningen agerat motspel till de övade. Övningsledningen har då agerat så som exempelvis berörda myndigheter eller massmedia torde agera under en kris. På andra övningar har berörda aktörer själva agerat motspel. Det har exempelvis Finansinspektionen gjort vid flera övningar. De övade får då information så som vid en kris, men den myndighet som agerar motspel över inte sin krisledning. Generellt sett har övningarna syftat till att stärka förmågan att hantera kriser. Syftet med övningarna som Finansinspektionen arrangerat för banker, VPC, BGC och Stockholmsbörsen skiljer sig från andra övningar. Under dessa övningar var syftet primärt att verifiera förmågan. Det sekundära syftet med övningen är utgöra underlag för deltagarnas arbete med att stärka sin beredskap.

5.3.2 Riksrevisionens iakttagelser om övningar

Övningarnas omfattning är begränsad

Tabell 5.2 Övningarnas omfattning

Antal övningar	Övningens omfattning
0	Alla väsentliga aktörer deltar (dvs. Regeringskansliet, operatörer, myndigheter och institutioner).
1[70]	Stor övning med flera aktörer. Övningen omfattar störningar i flera tekniska system som övas samtidigt.*
3[71]	Stor övning med flera aktörer där övningen sker vid samma tillfälle och omfattar ett tekniskt system.
1[72]	En eller två myndigheter/institutioner övar ett förlopp eller del av ett förlopp
25	En myndighet/institution övar egen verksamhet vid kris.

** Med tekniska system avses här bl.a. RIX, kortbetalningssystem och system för betalning av värdepapper.*

Tabellen ovan visar att majoriteten av övningarna sker enskilt på myndigheten eller institutionen. Regeringskansliet har inte övat störningar i betalningssystemet tillsammans med operatörer, myndigheter och institutioner. Övningsverksamheten kan därför liknas vid ett antal öar där övningen och resultaten från övningen är isolerade från övriga aktörer inom det finansiella systemet. Det är inte heller alltid hela krisledningen som övas.

70 Diskussionsövningar (exkl. bankerna): 5 st + majoriteten av Finansinspektionens övningar år 2006. Simuleringsövningar (exkl. bankerna): 15 st + sista dagen på Finansinspektionens övning år 2006. Inklusive bankerna (om ett års övning räknas som en övning) är motsvarande antal för diskussionsövningar 7 st och simuleringsövningar 17 st.

71 FSPOS övning, FSKLÖ, i september år 2007. Här simulerades bl.a. att RIX inte fungerade och att dubbla betalningar registrerats av Bankgirocentralen.

72 Försäkringskassan övade tillsammans med fyra storbanker och Säpo i oktober år 2007. Då simulerades bl.a. att delar av det offentliga betalningssystemet inte fungerade. SOES genomförde år 2005 en diskussionsövning, där det simulerades bl.a. stora störningar i Internettrafiken p.g.a. virus. Krisledningsövningen år 2004 (arrangerad av Finansinspektionen) simulerade att SWIFT inte fungerade.

73 Försäkringskassans övning tillsammans med Nordea år 2007 avsåg också betalningssystemet.

Det finns dock exempel på samverkansövningar med flera aktörer och deras krisledningar. En sådan övning har arrangerats av FSPOS år 2007 och en av Finansinspektionen år 2004. Övningen som arrangerades i september år 2007 är den största övning som hittills genomförts inom den finansiella sektorn. Krisberedskapsmyndigheten har också för avsikt att anordna en samverkansövning[74] år 2008. Scenariot för den övningen är bland annat omfattande logiska IT-attacker mot det finansiella systemet. Enligt uppgift kommer Regeringskansliet, myndigheter och privata aktörer inom det finansiella området att delta i den övningen.[75]

Varierande intensitet mellan övningarna

Övningsintensiteten och regelbundenheten beträffande övningar varierar mellan myndigheterna. Exempelvis har Försäkringskassan[76] och Riksgälden[77] haft högre ambition beträffande övningsverksamhetens intensitet än de mäktat med. Riksgälden har exempelvis som mål under perioden 2002-2007 att genomföra en scenarioövning med hela beredskapsorganisationen var 18:e månad. Riksgälden har under perioden genomfört sex övningar, varav fyra under år 2007. Kartläggningen visar samtidigt att övningar av varierande omfattning genomförs.

Det akuta läget under en kris övas mest

Vilka moment som övats varierar mellan övningarna och mellan myndigheterna. Moment som ledning och hantering av information till massmedier är relativt vanligt förekommande. Övning av ledning har varit en del i samtliga övningar. Andra moment som att tidigt upptäcka en händelse samt att återställa hela betalningstjänstfunktioner övas däremot mycket sällan[78]. Endast enstaka övningar har varit oförberedda för de övande.

Ytterligare ett moment som övas sällan är samverkan. Det finns dock exempel där samverkan varit en stor del av övningen. Under Finansinspektionens regi övade Riksbanken, banker, försäkringsbolag, VPC, BGC och Stockholmsbörsen tillsammans. Ytterligare ett exempel är Försäkringskassans övning tillsammans med Nordea år 2007 och FSPOS samverkansövning år 2007.

74 SamÖ-08.
75 Seminarium, FSPOS, 2007-11-27.
76 Enligt Försäkringskassans riktlinjer för krisberedskap ska huvudkontoret öva varje halvår. Huvudkontoret övade senast i november år 2005, övningen dessförinnan ägde rum i april år 2004.
77 Enligt beredskapsplanen för perioden 2002-2007 skulle Riksgälden genomföra en utrymningsövning årligen och var 18:e månad genomföra en scenarioövning med hela beredskapsorganisationen samt en övning av beslutsprocesser vid driftstörningar.
78 Enskilda myndigheter och enskilda moment, t.ex. återgång till ordinarie arbetsplats efter byte till den alternativa arbetsplatsen, övas mera frekvent.

Flera identifierade hot- och riskscenarier övas inte

Försäkringskassan har övat några identifierade riskscenarier, men långt ifrån alla väsentliga scenarier. Finansinspektionen har med sin krisorganisation endast övat ett fåtal av de hot- och riskscenarier man själv identifierat i sin risk- och sårbarhetsanalys[79]. Inspektionen har inte deltagit med hela sin krisorganisation i någon samverkansövning, utan endast deltagit som motspelare etc. Inte heller Riksgälden har övat alla de risk- och hotscenarier man identifierat som väsentliga. Riksbanken gör inte regelrätta hot- och riskscenarier av samma typ som övriga myndigheter.

Erfarenhet och återkoppling

Hur erfarenheter av en övning återförs varierar mellan myndigheterna. Rapporter från de övningar vi kartlagt och analyserat finns om än av varierande kvalitet. De myndigheter[80] som anlitat konsultbolaget 4 C Strategies har alla likartade processer för återkoppling. Efter övningen samlas erfarenheter i institutionsspecifika rapporter. Dessa rapporter har sedan utgjort underlag för en övergripande rapport från övningen. Den övergripande rapporten är avidentifierad och generell. Rapporten handlar i vissa fall mer om övningens utformning än resultat från övningen.

Återföringen av erfarenheterna från övningar bland personalen varierar mellan myndigheterna. Riksgäldskontoret menar att all information inte bör spridas bland personalen eftersom resultaten kan vara känsliga och spridning kan medföra komplikationer i arbetet.[81] Finansinspektionen redovisar däremot resultatet av övningarna på möten där hela myndigheten är samlad. Vidare informeras också de anställda via intranätet.[82] Riksbankens övningsrapporter riktas till berörda chefer som har ansvaret för att vidta identifierade åtgärder.

5.3.3 Bedömning av övningar

Riksrevisionen kan konstatera att alla myndigheter som är ansvariga för betalningssystemet inklusive regeringen hittills inte har övat sina krisorganisationer tillsammans och spritt erfarenheter av övningarna. Myndigheternas övningsverksamhet speglar inte heller i tillräcklig omfattning de omvärldsförhållanden som kan förväntas råda i samband med omfattande tekniska störningar i betalningssystemet. Riksrevisionen bedömer därför att förmågan hos myndigheterna att hantera en allvarlig störning inte är säkerställd. Bedömningen baseras på följande argument.

79 Finansinspektionen menar att inte alla identifierade risker ska övas, utan ett viktigt moment i övningen är att krisledningen kan bedöma effekter och vidta åtgärder, inte öva alla specifika risker.
80 Gäller i detta fall Finansinspektionen samt Post- och telestyrelsen.
81 Intervju, Riksgäldskontoret, 2007-09-07.
82 Intervju, Finansinspektionen 2007-10-08.

- Majoriteten av övningarna sker myndighetsvis. Övningsverksamheten inom den finansiella sektorn har under de senaste åren utvecklats från att vara diskussionsövningar till att alltmer likna verkliga förhållanden under en kris. Flera aktörer övar också oftare tillsammans än tidigare. Riksrevisionen kan dock konstatera att det hittills inte genomförts någon övning där Regeringskansliet, leverantörer, myndigheter och banker övat tillsammans och vid ett och samma tillfälle. Majoriteten av de övningar som genomförts kan liknas vid öar eller små grupper av öar där varje aktör övar sin egen organisation eller tillsammans med någon eller några andra aktörer eller motspelare. Vid en kris är samarbete mellan regelrätta krisorganisationer av central betydelse för att pröva om de förberedelser som gjorts verkligen är tillräckliga och fungerar. Att enbart öva det akuta skedet vid en kris och att öva aktörsvis eller mot enstaka motspelare innebär att väsentliga delar i beredskapsarbetet inte testats. Finansinspektionen har dock inte alls övat sin krisorganisation tillsammans med någon annan aktör. Riksbanken har gjort detta i övningen i september år 2007. Dessförinnan har endast enstaka personer från banken deltagit i så kallade skrivbordsövningar.

  Det är också viktigt att Regeringskansliet är med och övar eftersom myndigheterna inte har befogenhet att vidta flera typer av åtgärder som kan bli aktuella vid en allvarlig kris, till exempel frågor kring extraordinära katastrofbidrag eller att regelverk tillfälligt behöver upphävas.

- Identifierade hot och händelseförlopp har inte övats. Riksrevisionen kan också konstatera att flera av de hot och riskscenarier som identifierats i myndigheternas risk- och sårbarhetsanalyser inte övats.

- Erfarenheter av övningar sprids inte tillräckligt. För att en övning ska resultera i en ökad förmåga att hantera kriser är hanteringen av de brister som framkommit i övningen viktig. En övning i sig ökar förmågan att hantera en kris inom närtid, medan omhändertagande av erfarenheterna ökar den långsiktiga förmågan. För att öka den operativa förmågan i krishanteringsarbetet är spridning av erfarenheter mellan aktörerna väsentligt, så att inte misstag upprepas. Riksrevisionen kan konstatera att erfarenheterna vanligtvis hålls inom den enskilda myndigheten eller institutet. Det beror till stora delar på att övningarna görs enskilt. Vid de övningar där privata aktörer medverkat ser vi en risk att erfarenheterna inte sprids. De privata aktörernas ovilja att dela med sig av identifierade brister kan bero på konkurrens, risken att bristerna blir offentliga då de når en myndighet eller att uppgifterna kan användas i syfte att utöva tillsyn. Oavsett orsak kan ovilja att dela med sig av erfarenheter aktörer emellan försvåra arbetet med att uppnå en god beredskap för finansiella kriser.

5.4 Incidentrapportering och incidentanalyser

5.4.1 Allmänt

Banker och andra finansiella företag ska formellt sett rapportera incidenter inom betalningssystemet till Finansinspektionen, Riksbanken, Sitic och i vissa fall till Krisberedskapsmyndigheten. Finansinspektionens incidentrapportering gäller händelser av väsentlig betydelse[83]. Sitic ska förmedla information om IT-incidenter mellan samhällets organisationer och sprida information om nya problem som kan störa IT-system. Riksbankens incidentrapportering avser deltagarna i RIX-samarbetet. Rapporteringen av incidenter till Krisberedskapsmyndigheten är mer allmänt inriktad och avser situationsbaserad uppföljning av större katastrofer.

5.4.2 Iakttagelser

Incidentrapporteringen brister

Sitic har enligt uppgift aldrig fått någon rapport om incidenter från banker, däremot har Sitic ibland ingripit på eget initiativ[84]. Sitic, finans- och teleföretag deltar också i olika konstellationer[85] för att tidigt varna inför störningar och utbyta förebyggande säkerhetsinformation på informell grund[86]. Finansinspektionens tillsynsenhet har ingen kontakt med Säpo, FOI, Försvarets radioanstalt eller Sitic ifråga om incidentrapportering. Även om incidenterna ökar bedömer Finansinspektionen att säkerheten är god och att bankerna har bra system[87]. Polisen har gjort en motsatt bedömning, den omfattande mediala rapporteringen om olika typer av störningar i samtliga storbankers IT-verksamhet[88] avspeglar sig inte i Finansinspektionens incidentrapportering. Finansinspektionens incidentrapportering har inte heller utformats. Finansinspektionens incidentrapportering har inte heller utformats för att fungera i ett akut läge. Då minskar sannolikt möjligheterna att tidigt varna och samordnat hantera tidskritiska störningar. En fungerande incidentbevakning ställer krav på snabb upptäckt och att informationen når rätt mottagare så att snabba åtgärder kan vidtas[89]. Eftersom incidentrapporteringen är uppsplittrad försvagas möjligheterna i samhället som helhet att snabbt upptäcka och åtgärda incidenter inom betalningssystemet.

83 Finansinspektionen (1999:7) Allmänna råd om rapportering av händelser av väsentlig betydelse.
84 Computer Sweden. 2005-10-05. Sitic stängde koreanska sajten - inte polisen.
85 S.k. CERT-computer emergency response teams.
86 PTS (2004) Uppbyggnaden av Sveriges IT-incidentcentrum.
87 Intervju, Finansinspektionen, 2007-04-03.
88 SR, 2007-01-02.
89 Mandia, K & Prosise, K, (2001) *Incident reports.*

5.4.3 *Bedömning*

En fungerande incidentbevakning ställer enligt Riksrevisionen krav på snabb upptäckt och att informationen når rätt mottagare så att snabba åtgärder kan vidtas. Eftersom incidentrapporteringen är uppsplittrad försvagas möjligheterna i samhället som helhet att snabbt upptäcka och åtgärda incidenter inom betalningssystemet.

5.5 Penetrationstester

5.5.1 *Vad är penetrationstester?*

Penetrationstester är en form av aktiv teknisk kontroll som klargör behovet av informationssäkerhet. Sådana tester görs både av privata företag och myndigheter. I staten har Försvarets radioanstalt regeringens uppdrag att utföra sådana tester. Radioanstaltens uppdrag är avgiftsfinansierade och kontrollen görs efter myndigheternas begäran. Två penetrationstester har utförts av Försvarets radioanstalt vid Riksbanken under år 2004. Det ena testet avsåg det externa datorverket och det andra det interna datornätverket. Inom Försäkringskassan och Riksgälden har penetrationstester gjorts av privata företag under åren 2005-06.

5.5.2 *Iakttagelser*

Penetrationstester görs inte systematiskt och regelbundet

Penetrationstester görs inte systematiskt och regelbundet av myndigheterna. Riksrevisionens iakttagelser om de penetrationstester som genomförts av granskade myndigheter har påverkat Riksrevisionens slutsatser. Dessa iakttagelser redovisas i en sekretessbelagd bilaga (Bilaga H1).

Utkontraktering ökar krav på penetrationstester och personkontroller

Riksrevisionen konstaterar att en omfattande utkontraktering av IT-stöd förekommer inom myndigheterna. Många underleverantörer har därmed tillträde till det centrala betalningssystemets IT-miljöer. Kontrollen av myndigheternas egen IT-personal är inte alltid regelbunden. Det saknas i vissa fall även rutiner för säkerhetskontroll av konsultföretag. Samtidigt har både drift och underhåll placerats utomlands för vissa centrala system.

Försvarets radioanstalt anlitas endast undantagsvis

Försvarets radioanstalt används endast undantagsvis av granskade myndigheter. En orsak är att radioanstaltens analyser uppfattas som dyra. En annan orsak är att små myndigheter inte förmår identifiera behovet av analyser.

5.5.3 Bedömning av penetrationsanalyser

Riksrevisionen kan konstatera att penetrationsanalyser inte görs systematiskt och regelbundet inom granskade myndigheter. Relativt få penetrationstester har också gjorts av dessa myndigheter. Dessa tester har inte följts upp med nya tester. Därmed är det inte säkert att vidtagna åtgärder varit tillräckliga.

5.6 Forskning

5.6.1 Vilken forskning bedrivs?

Krisberedskapsmyndigheten finansierar i dagsläget inget forskningsprojekt inom området tekniska hot och risker i betalningssystemet[90]. Av cirka 65[91] pågående forskningsprojekt är det ett som direkt berör betalningssystemet. Det är projektet "Global finance as a threat: Post-crisis threat perception and policy development in Sweden". Det finns också fyra[92] projekt som indirekt berör betalningssystemet. På uppdrag av Krisberedskapsmyndigheten bedrev Totalförsvarets forskningsinstitut (FOI) forskningsprogrammet "Säkring av viktig infrastruktur" mellan åren 2000 och 2003 och ett visst underlag om IT-relaterade hot mot finansiella system ställdes samman inom programmet.[93]

Riksbanken bedriver ingen forskning som direkt rör tekniska hot och risker inom betalningssystemet.[94] Tre av tolv anställda på Riksbankens forskaravdelning har dock en forskningsprofil som rör operativ risk. Det finns även Riksbanksstudier som indirekt berört tekniska hot och risker i betalningssystemet bland annat spridningsrisker.[95]

90 Vid ett seminarium år 2007 konstaterades bland annat att nästan ingen forskning existerar på området teknisk risker i betalningssystemet. (Morten Bech, New York Fed "Systemic Risk in the Interbank Payment System due to Wide-Scale Disruptions").
91 Enligt uppgift på Krisberedskapsmyndighetens hemsida 2007-11-19 stöder Krisberedskapsmyndigheten idag ca 40 pågående forskningsprojekt samt ca 25 andra projekt fördelat på ramforskning, postdoktoralt stöd samt miljöstöd.
92 "Upplösta gränser mellan det privata och det offentliga - ett mångvetenskapligt forskningsprojekt om privatoffentlig samverkan" där fallstudier görs i bl.a. finansiella sektorn. "Utveckling av riskbegrepp och riskhanteringsstrategier för minskad sårbarhet i tekniska system". "Vulnerability och Complex Infrastructure". KBM har också av regeringen fått i uppdrag att - i samverkan med berörda samhällsaktörer - identifiera och analysera kritiska beroendeförhållanden mellan samhällsviktiga verksamheter som kan medverka till att en händelse leder till en allvarlig kris för samhället. Syftet är att ta fram förslag till konkreta åtgärder för att hantera beroendena. Arbetet genomförs inom ramen för projektet "Samhällskritiska beroenden".
93 FOI, underlagsrapport, 2005. s. 82-93 samt 109-114.
94 Telefonsamtal, Riksbanken, 2007-10-31.
95 Genomgång av forskaravdelningen utifrån den inriktning som anges på Riksbankens hemsida.

5.6.2 *Iakttagelser om forskning*

Ingen forskning om tekniska sårbarheter i betalningsystemet har initerats

Varken Krisberedskapsmyndigheten eller Riksbanken har tagit initiativ till att systematiskt täcka avgörande kunskapsluckor. Ett systematiskt uppbyggt och genomfört forskningsprogram för att få fram ny kunskap om tekniska sårbarheter i betalningssystemet saknas alltså. Riksrevisionen har identifierat kunskapsluckor till exempel om vad som händer om en systemviktig aktör inte kan fullgöra sina åtaganden på grund av tekniska störningar och om de nya typer av beroenden som teknikutvecklingen skapar. Det gäller också frågan om hur sårbara informationssystemen är för manipulation av insider och antagonister. Det finns ingen akademisk institution i Sverige med en tydlig forskningsprofil som rör tekniska risker i betalningssystemet.

5.6.3 *Bedömning av forskning*

Forskning är viktig för att samhället ska kunna möta de framtida tekniska hoten mot betalningssystemet. Riksrevisionen kan dock konstatera att vare sig Krisberedskapsmyndigheten eller Riksbanken stöder sådan forskning för närvarande.

5.7 Bedömning av förmåga

Riksrevisionen bedömer att vare sig regeringen eller myndigheterna har tillräckliga underlag för att kunna bedöma om vidtagna åtgärder räcker för att förebygga allvarliga tekniska störningar i det centrala betalningssystemet. Nuvarande underlag uppfyller inte krisberedskapsförordningens krav. Ett sådant underlag bör innehålla bedömningar av sannolikheter för och konsekvenser av tänkbara händelser samt analyser av samhällets kostnader för omfattande avbrott i betalningssystemet. Regeringen och myndigheterna har därmed inte tillräckligt underlag för att kunna bedöma skyddsåtgärdernas omfattning och betalningssystemets robusthet i dag i förhållande till samhällets kostnader vid omfattande avbrott i betalningarna. Riksrevisionen anser därför att regeringen saknar de nödvändiga förutsättningarna för att kunna bedöma om det vidtagits rimliga skyddsåtgärder inom betalningssystemet.

Riksrevisionen bedömer också att statens åtgärder inte heller ger tillräckliga förutsättningar för att hantera allvarliga tekniska störningar i betalningssystemet när de väl inträffar. Granskningen visar att myndigheterna och privata aktörer inte har förberett sig tillräckligt genom krisplanering och övningar så att skadeverkningarna för medborgare och samhälle kan begrän-

sas när en allvarlig störning inträffar. Myndigheternas övningsverksamhet speglar enligt Riksrevisionen inte i tillräcklig utsträckning de omvärldsförhållanden som kan förväntas råda i samband med omfattande tekniska störningar i betalningssystemet. Det har inte genomförts övningar där hela branschen inklusive Regeringskansliet övar tillsammans. Det finns inte någon utsedd ”Tjänsteman i beredskap” hos granskade myndigheter som uppfyller regeringens definition av en sådan tjänsteman. Regeringen har inte utsett en myndighet som ska leda samverkan i kris eller en gemensam plats för akut krishantering förberetts.

Vidare är incidentrapporteringen uppsplittrad. Därmed försvagas enligt Riksrevisionen möjligheterna att snabbt upptäcka och åtgärda incidenter inom betalningssystemet. Penetrationsanalyser görs inte heller systematiskt och regelbundet inom granskade myndigheter. Därmed är det inte säkert att vidtagna skyddsåtgärder är tillräckliga. Riksrevisionen har slutligen identifierat flera betydande kunskapsluckor inom området betalningssystem.

Riksrevisionen kan sammanfattningsvis konstatera att myndigheterna under de senaste åren intensifierat sitt gemensamma arbete för att förebygga och hantera kriser i betalningssystemet, men att det också finns brister i alla de sex grundläggande förutsättningar för förmåga som identifierats i granskningen. Därtill kommer brister i mål, ansvarsfördelning samt uppföljning och tillsyn som behandlas i andra kapitel. Även om de grundläggande förutsättningar som Riksrevisionen identifierat saknas och många brister finns i de förberedelser som myndigheter vidtagit kan man inte utesluta att det finns förmåga inom sektorn att hantera en allvarlig störning om den skulle inträffa. Eftersom en allvarlig störning ännu inte inträffat måste en bedömning av förmåga baseras på de förberedelser som gjorts i ett antal grundläggande avseenden. Riksrevisionen bedömer således att förmågan att förebygga och hantera allvarliga störningar inom det centrala betalningssystemet är bristfällig.

6 Uppföljning och tillsyn

Revisionsfrågan i detta kapitel är:
Har ansvariga myndigheter genomfört en tillfredsställande uppföljning och tillsyn?

6.1 Bedömningsgrunder

Syftet med en *uppföljning* är att leverera en lägesbild till riksdagen och till inblandade aktörer. Uppföljningen ska innehålla en bedömning av huruvida myndigheten uppnått målet eller inte. Om målet inte uppnåtts bör en redogörelse av alternativa vägar för att uppnå målet finnas med i uppföljningen. Vidare ska resultatet av uppföljningen kunna ställas emot kostnaderna.[96]

Vad gäller *tillsyn* bedömer vi i vilken grad den är inriktad på inspektioner av de delar i betalningssystemet där risker och konsekvenser av allvarliga tekniska störningar kan antas vara störst och om tillsynen under senare år faktiskt kontrollerat bankernas och el-, tele- och IT-operatörernas bedömningar av tekniska risker samt de skyddsåtgärder som vidtagits. Slutligen har vi också granskat om tillsynsmyndigheterna utnyttjat sin föreskriftsrätt och möjligheter att utdela sanktioner så att regelbrott får efterverkningar.

6.2 Uppföljning

6.2.1 Hur ser uppföljningssystemet ut?

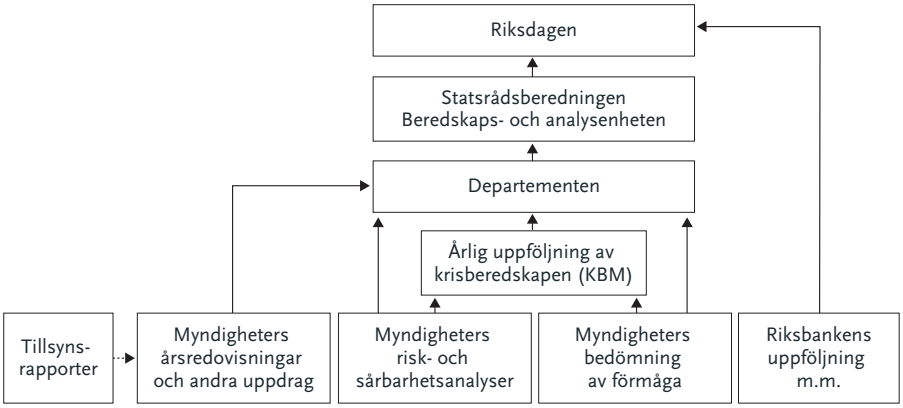
Som framgår av figur 6.1 består den uppföljning som görs av flera olika delar. Myndigheternas årsredovisningar och andra uppdrag redovisas direkt till respektive departement. Myndigheternas risk- och sårbarhetsanalyser[97] liksom myndigheternas bedömning av förmåga redovisas till Krisberedskapsmyndigheten och till respektive departement. Riksbanken, som är en myndighet under riksdagen, redovisar sin uppföljning direkt till riksdagen. Tillsynsresultat redovisas översiktligt i myndigheternas årsredovisningar. Resultat från tillsynsrapporter redovisas ofta i myndigheternas årsredovisningar.

Krisberedskapsmyndigheten är centralt placerad för att samordna myndigheternas uppföljning. Krisberedskapsmyndigheten redovisar nämligen

96 Utvecklingen av den ekonomiska styrningen, bet. 1999/2000 FiU13, rskr 1999/2000:16.
97 Risk- och sårbarhetsanalyserna behandlas i avsnitt 5.1.

i sin tur en årlig uppföljning till sitt departement. Informationen går sedan via departementen till Statsrådsberedningen för att slutligen nå riksdagen. I denna årliga rapport följer Krisberedskapsmyndigheten upp den verksamhet som myndigheterna genomfört med anslag 7:5[98]. Till skillnad från myndigheternas årsredovisningar ska den årliga uppföljningen av krisberedskapen ge en samlad bild av aktörernas förmåga och av den beredskapsverksamhet som finansierats via anslag. Den årliga uppföljningen ska även visa hur mål, uppgifter och resurser relaterar till förmåga och vidtagna åtgärder under året. Vidare ska den årliga uppföljningen påpeka om något behöver förändras.[99]

Figur 6.1. Uppföljningens organisation



Myndigheternas årsredovisningar och andra uppdrag[100]

Myndigheternas årsredovisningar skrivs utifrån respektive departements krav på återrapportering. De olika myndigheterna har i stort sett haft samma krav, med undantag för några krav som är specifika för en viss myndighet. Åren 2005 och 2006 var de gemensamma[101] återrapporteringskraven bland annat att redovisa förhållanden eller gränssättande faktorer inom myndighetens ansvarsområde som allvarligt begränsar samhällets förmåga vid svåra påfrestningar i fred och hur dessa faktorer kan elimineras.[102]

Finansinspektionens stabilitetsrapport publiceras en gång om året. I granskningen har vi gått igenom rapporterna från åren 2005 och 2006. Rapporterna beskriver hur den finansiella marknaden utvecklas och vilka hot och risker som finns mot finansiell stabilitet.

98 Anslag 7:5 är de medel som avsatts för krisberedskap i statsbudgeten. Anslaget var 1444 miljoner kronor år 2006.
99 KBM (2003) *Metodutveckling av den årliga uppföljningen*, s.11.
100 Granskningen avser årsredovisningarna för åren 2004-2006. Fokus är rapporteringen av myndighetens krisberedskap.
101 För att ett återrapporteringskrav ska räknas som gemensamt ska minst två av myndigheterna ha kravet i sitt regleringsbrev.
102 Bl.a. Finansinspektionens årsredovisning för år 2006 s.34.

Myndigheternas förmågebedömningar

Varje år begär regeringen en bedömning av förmåga från de myndigheter som ges ett särskilt ansvar i krisberedskapsförordningen. Hur redovisningen gått till och vilka kategorier som använts har ändrats över tiden[103]. Myndigheternas bedömningar av förmåga görs numera utifrån scenarier som Krisberedskapsmyndigheten tagit fram och värderas enligt en fyrgradig[104] skala. Under år 2007 har Krisberedskapsmyndigheten, efter uppdrag i regleringsbrevet, utvecklat indikatorer på krisberedskapsförmåga och försvarsförmåga. Indikatorerna ska vara generella och gemensamma och användas när myndigheterna gör sina bedömningar av förmåga. Myndigheternas bedömning av förmåga utgör den huvudsakliga grunden för den samlade bedömningen av samhällets förmåga att hantera kriser som Krisberedskapsmyndigheten årligen lämnar till regeringen.

Krisberedskapsmyndigheten bedömde att samhällets förmåga att hantera svåra påfrestningar inom Samverkansområdet ekonomisk säkerhet under åren 2002-2004[105] var ”icke godtagbar”. Motsvarande bedömning av förmåga för två områden som det centrala betalningssystemet är starkt beroende av, elektroniska kommunikationer och elsäkerhet, var också under åren 2002-2005 ”icke godtagbar”. År 2006 ändrar Krisberedskapsmyndigheten uppföljningen och redovisar endast om åtgärder förbättrat förmågan. Vissa, men inga avgörande förbättringar redovisas inom området ekonomisk säkerhet. Någon sammanfattande bedömning av området gjordes inte heller under år 2007. Krisberedskapsmyndigheten bedömer dock att det finns allvarliga brister i samhällets förmåga att hantera konsekvenserna av långvariga elavbrott och långvariga avbrott i de elektroniska kommunikationerna. Beträffande kriser som berör flera samhällsfaktorer anser Krisberedskapsmyndigheten att samhällets förmåga är bristfällig[106].

Krisberedskapsmyndighetens årliga uppföljning

Under åren 2003–2006 har den årliga uppföljningen bestått av tre delar: en redovisning av det gångna årets verksamhet, en ekonomisk redovisning av anslaget samt en bedömning av förmåga. Krisberedskapsmyndighetens ambition är att koncentrera uppföljningen till den ekonomiska redovisningen. Bedömningen av förmåga ska så småningom bli en egen rapport[107].

---

103 Under åren 2003 och 2004 bestod bedömningen av förmåga av tre olika delar: grundförmåga, förmåga inom fem år och förmåga inom tio år. År 2005 delar man däremot in förmågan i tre andra delar: krishanteringsförmåga, operativ förmåga och förmåga att stå emot störningar i samhällsviktig verksamhet. Denna förändring gjordes för att myndigheternas tidigare bedömningar inte varit jämförbara.

104 Förmågan bedöms utifrån följande fyra steg. God förmåga, i huvudsak god förmåga men med vissa brister, viss men bristfällig förmåga samt ingen/mycket bristfällig förmåga.

105 År 2005 gjorde Krisberedskapsmyndigheten ingen bedömning av området Ekonomisk säkerhet.

106 Krisberedskapsmyndigheten. *Samhällets krisberedskapsförmåga 2006/2007.*

107 Intervju, Krisberedskapsmyndigheten, 2007-08-28.

Myndigheternas risk- och sårbarhetsanalyser

Statliga myndigheter[108] ska – som nämnts i kapitel 5 - årligen ta fram en risk- och sårbarhetsanalys inom sitt ansvarsområde.[109] Det är både den egna myndigheten och samhällets krisberedskap som ska behandlas i risk- och sårbarhetsanalysen. Myndigheterna ska särskilt beakta situationer som uppstår hastigt, oväntat och utan förvarning samt situationer som kräver brådskande beslut och samverkan med andra aktörer. I bilaga 1 redogör vi för vilka uppgifter myndigheterna ska redovisa i analysen. Analysen ska lämnas till Regeringskansliet samtidigt med årsredovisningen. En kopia ska också lämnas till Krisberedskapsmyndigheten.

Riksbankens uppföljning

Riksbankens uppföljning lämnas direkt till riksdagen. Här granskar vi årsredovisningarna för åren 2004–2006 samt stabilitetsrapporterna för åren 2005–2007. Riksbankens stabilitetsrapport ”Finansiell stabilitet” ges ut två gånger per år. Där ger banken en samlad bedömning av risker och hot mot det finansiella systemet samt av motståndskraften mot dessa.[110]

6.3 Tillsyn

Tre myndigheter med särskilt ansvar för tillsyn och övervakning av betalningssystem och dess kritiska infrastruktur är Riksbanken, Finansinspektionen samt Post- och telestyrelsen.

Riksbanken ska främja ett säkert och effektivt betalningsväsende och följer och övervakar fyra finansiella institutioner och system, som kan riskera att äventyra säkerheten i det finansiella systemet: Riksbankens betalningssystem (RIX), Stockholmsbörsen, Värdepapperscentralen och Bankgirocentralen.

Finansinspektionen är tillsynsmyndighet för cirka 3 700 enskilda finansiella företag, marknadsplatser och clearingorganisationer. Finansinspektionen utövar tillsyn även mot utländska filialer, ägare och ledning och kompletterar Riksbankens systeminriktade övervakning[111].

Post- och telestyrelsen är tillsynsmyndighet[112] över företag som tillhandahåller elektroniska kommunikationsnät eller elektroniska kommunikationstjänster[113] och ska se till att enskilda och myndigheter får tillgång till säkra och effektiva elektroniska kommunikationer. Mandatet omfattar samhällsviktig infrastruktur, till vilken betalningsväsendet hör[114].

108 Krisberedskapsförordningen gäller för statliga myndigheter under regeringen med undantag av Regeringskansliet, kommittéväsendet och Försvarsmakten.
109 9 § förordningen (2006:942) om krisberedskap och höjd beredskap.
110 *Riksbankens årsredovisning 2006, s. 30.*
111 Överenskommelse mellan Finansinspektionen och Sveriges riksbank om arbetsfördelning och samarbete rörande finansiell stabilitet och effektivitet.
112 1 kap. 9 § lagen (2003:389) om elektronisk kommunikation.
113 *Post- och telestyrelsens regleringsbrev för år 2007.*
114 *Post- och telestyrelsen (2006). Robusta elektroniska kommunikationer Strategi för åren 2006-08, s 17.*

Tillsynsmetoder

Riksbanken analyserar transaktionsstatistik samt system- och strukturförändringar utifrån internationella rekommendationer i sin övervakning[115]. Underlagen hämtas bland annat från möten med de företag som tillhandahåller finansiella infrastrukturtjänster. De institutioner som omfattas av Riksbankens övervakning granskas gemensamt med Finansinspektionen.

Finansinspektionen[116] har övergått från traditionella statiska tillsynsformer till att fokusera på strategiska nyckelfrågor. Sedan år 2003 har checklistor och definitioner rörande operativ risk införts[117]. Urval från checklistorna används vid tillsynsarbetet, där såväl egna som Baselkommitténs regler om riskhantering använts som kriterier för granskningen. Från år 2007 är även Basel II och EU:s direktiv om kapitaltäckning tillsynskriterier.

Finansinspektionen ställer vid platsbesök frågor rörande incidenter och möter regelbundet storbankerna. Finansinspektionen tolkar inte som sitt uppdrag att enbart utföra kontroll. Tillsynen ska fungera samlat och flexibelt tillsammans med de krav nya regler ställer på omvärldsbevakning, regel- och metodutveckling, datainsamling, dialog och analys av de finansiella företagens självvärderingar av sin egen riskhantering.[118] Finansinspektionen granskar underlag avseende planer och processer för kontinuitetshantering och krisorganisation. Bankerna ska omgående inrapportera *väsentliga* incidenter till Finansinspektionen. Under åren 2005-2007 inrapporterades åtta incidenter av teknisk karaktär. Rapporterna inkom i snitt 16 dagar efter incidenten inträffat. Under samma period skrev tidskriften Computer Sweden om minst 29 incidenter som enligt Riksrevisionens bedömning borde avrapporterats. Flera av artiklarna utgavs dessutom samma dag som incidenten ägde rum.

Post- och telestyrelsens policydokument för tillsyn konstaterar att det inte går att ge någon enhetlig arbetsbeskrivning på hur tillsynen generellt går till eftersom den har så olika karaktär och att det är svårt att dra gräns mellan tillsyn och övrig verksamhet. Styrelsen har tagit fram egna riktlinjer för tillsynsarbetet[119] och bedriver i princip två typer av tillsyn: Förebyggande eller planlagd tillsyn av driftsäkerhet och händelsestyrd tillsyn vid större avbrott. Tillsynsarbetet är främst inriktat på den senare typen. Styrelsen granskar orsak till avbrott och störningar, åtgärder som vidtagits samt omfattning och planering för att undvika upprepning. I de riktlinjer för löpande tillsyn som är under utarbetande[120] förordas att tematiska (planlagda) tillsynsåtgärder avgränsas till en viktig fråga per år.

115 T.ex. BIS. Core Principles for Systemically Important Payment Systems.
116 Finansinspektionen (2002). *FI:s samverkan med granskningsmän*, s. 4 och 5.
117 Finansinspektionen (2003). Samlad riskbedömning. Finansinspektionen (2004). Checklista Riskanalys operativa risker (ROP) Block III och Finansinspektionen (2004). Riskmätning och kapitalkrav.
118 Finansinspektionen (2004) Tillsyn – Förslag om en tydligare och effektivare offentlig tillsyn. Remissvar.
119 Telefonintervju, PTS, 2007-09-30.
120 PTS (2007) Tillsyn på N.

Sanktionsmöjligheter

Riksbanken, Finansinspektionen och Post- och telestyrelsen får utfärda föreskrifter, men utfärdar hellre allmänna råd om god funktion, säkerhet, uthållighet och tillgänglighet genom riskanalyser och riskhantering, planering för och uppföljning av avbrott och störningar. Inga sanktioner har kopplats till tekniska miniminivåer, även om myndigheterna har rätt att utdela varningar och att döma till böter. Både Finansinspektionen och Post- och telestyrelsen har utdelat sanktioner, men inte för ärenden som specifikt rör tekniska risker.

Riksbankens tillsyns- och sanktionsmöjligheter är inte uttalade. Riksbanken *kan* dock ingripa om den upptäcker så allvarliga problem att de kan hota den finansiella stabiliteten och kan även i samarbete med finansinspektionen rekommendera påföljder eller åstadkomma förändringar i lag eller reglering[121]. Några möjligheter att bötfälla institut har inte Riksbanken, som i stället belyser systemrisker i rapporter som den anser ger aktörer incitament att vidta åtgärder.

Bedriven tillsyn och övervakning

Finansinspektionen har inte utövat en aktiv och kontrollerande tillsyn av tekniska risker i storbankerna under de senaste åren. Inspektionens begränsade resurser har i stor utsträckning gått till utvecklingsarbete och till att granska ansökningar från bankerna om att använda en viss internmätningsmetod[122]. Finansinspektionen menar att man inte har resurser för att kontrollera verksamheten på plats. Den tidigare typ av IT-tillsyn som i enstaka fall gjordes för cirka tre år sedan utförs inte längre. En enhet för IT-relaterad tillsyn likt den i Nederländerna och våra grannländer saknas inom den svenska Finansinspektionen. Även Riksbankens övervakning är också av övergripande karaktär. Övervakningen avser Riksbankens eget system för stora betalningar (RIX), Stockholmsbörsens, Värdepapperscentralens och Bankgirocentralens system.

Post- och telestyrelsen har hittills inte bedrivit en aktiv och planlagd tillsyn av teleoperatörerna. Tillsynen har varit händelsestyrd med insatser vid större driftavbrott, då Post- och telestyrelsen vill ha reda på orsak till avbrott och störningar, åtgärder som vidtagits, omfattning samt planering för att undvika upprepning.

121 PTS (2007) Post- och telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid, 7 kap. lagen (2003:389) om elektronisk kommunikation samt Riksbanken (2001) Övervakning av den finansiella infrastrukturen och finansiella stabiliteten, Finansiell stabilitet.

122 Genom den nya kapitaltäckningslagen införs en skyldighet att beräkna kapitalkrav även för operativa risker. Detta kapitalkrav ska beräknas med stöd av en basmetod, en schablonmetod eller, efter tillstånd av Finansinspektionen, en internmätningsmetod.

6.4 Iakttagelser

6.4.1 Iakttagelser om uppföljning

Myndigheternas årsredovisningar ger begränsad information[123]

Det finns flera typer av rapporter och underlag med relevant information om att följa upp robusthet och förmåga att akut hantera en allvarlig störning i det centrala betalningssystemet. Riksbankens stabilitets- och övervakningsrapporter berör endast en begränsad del av de risker och sårbarheter som identifierats i det centrala betalningssystemet. Finansinspektionens tillsynsrapporter avser å sin sida endast enskilda aktörer inom det finansiella systemet, men omfattar inte detaljerade uppgifter om bankernas tekniska krisberedskap.

Krisberedskapsmyndighetens årliga uppföljning är inte fullständig. Verksamhet utöver anslag 7:5 Krisberedskap ingår till exempel inte, och inte heller verksamhet inom Riksbanken, Regeringskansliet eller de finansiella institutionerna. Samverkansorganen delar upp sin rapportering enligt de områden de täcker, medan myndigheter med ansvar för telenät- och elsäkerhet rapporterar var för sig till sitt departement. Informationen om uppföljningen är alltså utformad så att en samlad syntes inte låter sig göras. Det saknas således ett enhetligt rapporteringssystem.

Rapporteringen har ingen central mottagare

Eftersom det inte finns någon organiserad hantering och central mottagare i Regeringskansliet för all relevant rapportering som kommer till departementen blir det omöjligt för regering och riksdag att få en heltäckande bild av beredskapen inom betalningssystemet. En bristfällig bild av krisberedskapen ökar risken för att man prioriterar fel åtgärder.

Informationen handlar mest om likviditets- och marknadsrisker

Årsredovisningarna och stabilitetsrapporterna lämnar knappast något substantiellt bidrag till den samlade bilden av förmågan att hantera tekniska hot och risker. Sådana risker står det till exempel mycket litet om i stabilitetsrapporterna. Rapporterna fokuserar i stället på finansiella risker. Även i årsredovisningarna är de delar som behandlar tekniska risker förhållandevis små.

123 Granskningen avser årsredovisningarna för åren 2004-2006. Fokus är rapporteringen av myndighetens krisberedskap.

Myndigheterna redovisar ofta insatser, men inte hur insatserna har påverkat förmågan. Sammantaget kan vi alltså konstatera att årsredovisningarna och stabilitetsrapporterna inte är tillräckliga som underlag för att bedöma förmågan. Informationen är oprecis och svår att tolka när det gäller tekniska brister.

Bedömningen av förmåga är personberoende

I dag bedömer myndigheterna förmåga utan stöd av gemensamma begrepp och definitioner. Det finns exempelvis ingen definition av vad de fyra stegen i förmågeskalan innebär. Olika aktörer kan uppfatta god förmåga på olika sätt, vilket gör det svårt att jämföra myndigheter. Det är också svårt att jämföra bedömningarna från samma myndighet mellan olika år, särskilt som de är utformade så att de blir mycket beroende av vem som bedömer. Denna kritik framförs också av Skatteverket, som menar att myndigheters egen uppskattning av förmåga erfarenhetsmässigt alltid redovisas högre än den verkliga förmågan. Den mest trovärdiga bedömningen av den samlade förmågan att hantera kriser görs av oberoende granskare.[124] Krisberedskapsmyndigheten är visserligen oberoende i förhållande till övriga myndigheter, men har inte mandat att föreskriva hur myndigheterna ska gå till väga vid bedömningarna och kontrollerar inte heller på vilket underlag bedömningarna har gjorts. Hur Riksrevisionen bedömer förmåga i denna granskning framgår av bilaga 1.

6.4.2 Iakttagelser om tillsyn

Ingen samverkan i tillsynen

Ansvarsfördelningen mellan de myndigheter som bedriver tillsyn över betalningssystemet och den grupp myndigheter som granskar de underliggande infrastrukturerna är oklar. Det är oklart vem som ska ta ansvar för gränssnittet mellan betalningsväsendets tekniska system och underliggande tekniska system för el, tele och IT. Därmed riskerar tillsynen av kritisk infrastruktur för betalningssystemet att falla mellan stolarna. De två grupperna av myndigheter har inte bedrivit tillsyn tillsammans. Detsamma gäller tillsynen inom gränsområdet mellan betalningssystem och informationssäkerhet. Riksbanken och Finansinspektionen har dock utvärderat VPC och Stockholmsbörsen tillsammans.

124 Skatteverket (2007) Yttrande över Krisberedskapsmyndighetens remiss: Indikatorer på krisberedskapsförmåga.

Viktiga delar av betalningssystemet får ingen tillsyn

Finansinspektionen har inte tolkat sitt tillsynsansvar som att omfatta en systeminriktad riskanalys. Det har Riksbanken däremot gjort. Riksbanken har dock endast analyserat vissa systemviktiga institutioner och inte gjort någon syntes för hela sektorn vad gäller tekniska sårbarheter. Därmed finns det luckor i tillsynen. Ingen av myndigheterna har till exempel bedrivit tillsyn över massbetalningssystemens säkerhet i sin helhet (från ax till limpa). Inte heller har någon gjort en regelrätt tillsynsundersökning av storbankerna med fokus på tekniska säkerhetsfrågor under de senaste tre åren. Undantaget är tillsyn av operativa risker under åren före år 2004.

Likviditets- och kreditrisker dominerar

Riksbanken och Finansinspektionen ägnar huvuddelen av tillsynen åt likviditets- och kreditrisker. Tekniska risker prioriteras inte ur systemsynpunkt. Ändå nämner både Riksbanken och Finansinspektionen ofta att operativa risker kan utlösa systemkriser. Riksbanken behandlar dock sällan frågor kring tekniska risker i ett hot- och sårbarhetsperspektiv i sin utvärdering av Värdepapperscentralen, Bankgirocentralen och Stockholmsbörsen.

Myndigheterna har dubbla roller

Finansinspektionen, Post- och telestyrelsen och Riksbanken bedriver samtidigt tillsyn och verkar främjande för samarbete inom krisberedskap. Finansinspektionen och Post- och telestyrelsen menar båda att tillsynen är svår att särskilja från andra, främjande aktiviteter. Att Riksbanken driver RIX innebär också att man samtidigt främjar och övervakar det centrala betalningssystemet.

Tillsynen bygger på aktörernas självvärderingar

En stor del av Finansinspektionens resurser har de senaste åren gått till utvecklingsarbete och till att ta fram policydokument och checklistor med mera. Finansinspektionen uppger också att man inte – med nuvarande resurser och arbetssätt – kan kontrollera att VPC, BGC och bankerna faktiskt har tillräcklig reservkraft. Bankerna och infrastrukturföretagen får själva hantera tillsynen av tekniska hot och risker utifrån kriterierna risk och väsentlighet. Finansinspektionens tillsyn bygger till exempel till stor del på aktörernas självvärderingar. Varken Finansinspektionen, Riksbanken eller Post- och telestyrelsen har verifierat bankernas bedömningar av tekniska risker under senaste år. Att dessa faktiskt fungerar ses som de privata finansiella institutionernas ansvar. Myndigheterna litar till de privata finansiella institutens bedömningar.

Myndigheterna utnyttjar inte sin föreskriftsrätt

Finansinspektionen, Riksbanken och Post- och telestyrelsen har alla rätt att ta fram föreskrifter för hur operativa risker ska hanteras. Men myndigheterna har i stället valt att utfärda allmänna råd och att lita till så kallad ”moral suasion”[125]. Varken allmänna råd eller ”moral suasion” ger underlag för att ställa rättsligt bindande krav på företag[126]. Ett argument för att välja denna modell har varit att strängare krav kan ses som handelshinder ur ett europeiskt perspektiv. EU:s regelverk hindrar dock inte att det ställs hårdare krav med hänvisning till säkerhetskrav.

6.5 Bedömning av uppföljning och tillsyn

Omfattande rapporteringsrutiner om krisberedskap har utvecklats över tiden av Krisberedskapsmyndigheten och andra aktörer. Vad och hur myndigheterna följer upp, har gjorts på olika sätt genom åren. Flera olika uppföljningssystem finns nu parallellt. Det saknas en strategi och systematik för att ta fram relevant innehåll åt en central mottagare som kan göra en oberoende sammanställning och analys av avrapporteringen och därefter ge en sådan återföring att åtgärder kan vidtas. Bedömningen av förmåga bygger främst på en personberoende värdering utan tillräckligt stöd från definierade begrepp. Regeringen har inte gjort en självständig analys och sammanställning av den information som har levererats. Regeringen har inte heller reagerat på kvaliteten i uppföljningen. Äldre system för att rapportera har efterhand överlappats av nya system. Det finns heller ingen central mottagare för all rapportering som avser betalningssystemet.

Eftersom det i dag inte finns en tydlig samordning av informationshanteringen i Regeringskansliet blir det svårare för regering och riksdag att få en heltäckande bild av beredskapen i det centrala betalningssystemet och svår. are att jämföra myndigheternas skyddsåtgärder och bedömningar mellan olika år. En felaktig bild av krisberedskapen inom betalningssystemet ökar risken för felaktiga prioriteringar, ineffektiva investeringar i förebyggande åtgärder eller underinvesteringar i säkerhetsåtgärder.

Riksrevisionen bedömer också att den tekniska tillsynen är alltför begränsad inom samtliga tre granskade tillsynsmyndigheter. Myndigheterna förlitar sig på allmänna och översiktliga bestämmelser om operativa risker, där det ytterst är företagen själva som ska göra lägesbedömningar och där myndigheterna eftersträvar ett främjande samarbetsklimat med företagen.
Detta i kombination med avsaknad av faktisk kontroll på plats innebär att

125 Indirekt påverkan, utan maktmedel men genom övertygelse, att förmå någon att följa en policy.

126 Lagenliga krav kan för Finansinspektionens del ställas bland annat enligt lagen om bank- och finansieringsverksamhet. Finansinspektionen har föreskriftsrätt enligt portalparagraferna i bank- och finansieringsrörelselagen. Frågan om nuvarande allmänna råd ska ersättas av föreskrifter utreds för närvarande inom Finansinspektionen.

ingen verifierar att en samlad förmåga finns i enlighet med tydligt fastlagda bedömningsgrunder för betalningssystemet.

Finansinspektionen har endast begränsade kontakter med de myndigheter som arbetar med säkerhet i elektroniska kommunikationer. Därmed utnyttjas inte den samlade expertis som finns att tillgå i staten effektivt.

Post- och telestyrelsen har ett tekniskt tillsynsansvar men anser att företagen har primärt ansvar för den kritiska infrastrukturen. Samtidigt pekar både internationella normer och företagen på staten som ansvarig för infrastruktur. Tillsynssystemet är reaktivt i den meningen att tillsyn utövas först vid större brister, men då kan det vara för sent. Det saknas således en förebyggande och planlagd tillsyn som även systematiskt bearbetar incidentrapporteringen. Redovisningen av resultatet från tillsynen är knapphändig och inte integrerad i myndigheternas övergripande rapportering om risker och sårbarheter.

7 Sammanfattande bedömningar och rekommendationer

Den revisionsfråga som granskningen ska besvara är följande:
Är statens åtgärder tillräckliga för att allvarliga tekniska störningar inom det centrala betalningssystemet kan förebyggas eller hanteras om de inträffar?

Den finansiella sektorns aktiviteter när det gäller krisberedskap har utvecklats på senare år och särskilt under år 2007. Det gäller såväl dess samverkan, som övningar och tillsyn som görs utifrån internationellt vedertagna normer. Samtliga myndigheter som Riksrevisionen granskat är engagerade i och avsätter i varierande omfattning tid och resurser för krishantering. Ett ökat engagemang från Regeringskansliet kan även noteras. Riksrevisionens granskning visar emellertid att det också finns ett antal avgörande brister i statens åtgärder för att förebygga och hantera allvarliga störningar i det centrala betalningssystemet när de inträffar. Dessa sammanfattas nedan.

7.1 Slutsatser och bedömningar

7.1.1 Sammanfattande slutsatser

Är statens åtgärder för att förebygga allvarliga tekniska störningar i betalningssystemet tillräckliga?

- Riksrevisionen anser att vare sig regeringen eller myndigheterna har tillräckliga underlag för att kunna bedöma om vidtagna åtgärder räcker för att *förebygga* allvarliga tekniska störningar i det centrala betalningssystemet. Det finns brister i myndigheternas risk- och sårbarhetsanalyser på området, i den uppföljningsinformation och den tillsyn som myndigheterna har genomfört samt i analyser av kostnader för samhället av omfattande tekniska störningar.

Är statens åtgärder för att hantera allvarliga tekniska störningar i betalningssystemet tillräckliga?

- Riksrevisionen bedömer att statens åtgärder inte heller ger tillräckliga förutsättningar för *att hantera* allvarliga tekniska störningar i betalningssystemet *om de inträffar*. Granskningen visar att myndigheterna och

privata aktörer inte har förberett sig tillräckligt genom krisplanering, övningar och andra typer av förberedelser så att skadeverkningarna för medborgare och samhälle kan begränsas när en allvarlig störning inträffar.

Riksrevisionen bedömer därför att förmågan att förebygga och hantera allvarliga störningar inom det centrala betalningssystemet är bristfällig.

Skälen för Riksrevisionens slutsatser och bedömningar

Regeringen har inte organiserat och samordnat hanteringen av risk- och sårbarhetsanalyser och annan uppföljningsinformation på ett sådant sätt att allt underlag som efterfrågas låter sig sammanställas till en nationell bild av krishanteringsförmågan. Nuvarande underlag uppfyller i dag inte heller krisberedskapsförordningens krav. Ett sådant underlag borde enligt Riksrevisionen innehålla bedömningar av sannolikheter för och konsekvenser av tänkbara händelser samt analyser av samhällets kostnader för omfattande avbrott i betalningssystemet. Inte heller har regeringen fastställt vilken uthållighet och vilka grundläggande säkerhetskrav som betalningssystemet och dess infrastruktur ska uppfylla. Regeringen har därmed varken en norm att utgå ifrån eller tillräckligt underlag för att kunna bedöma rimligheten i skyddsåtgärdernas omfattning och betalningssystemets robusthet i förhållande till samhällets kostnader för omfattande avbrott i betalningarna.

Riksrevisionen anser därför att regeringen saknar nödvändiga förutsättningar för att kunna bedöma om det vidtagits rimliga åtgärder inom betalningssystemet. Vad gäller förutsättningarna för att hantera ett omfattande avbrott i betalningssystemet är ansvarsfördelningen mellan aktörer för operativ krishantering oklar i vissa avseenden: Ingen myndighet har fått ett entydigt övergripande och samlat ansvar för ledning, planering, samverkan och uppföljning av krisberedskapsåtgärder inom betalningssystemet. Det statliga ansvaret för informationssäkerhet och incidenthantering inom den finansiella sektorn är uppsplittrat mellan flera myndigheter. Regeringen har inte beslutat att funktionen ”Tjänsteman i beredskap” ska finnas inom den finansiella sektorn. En sådan funktion har beslutats inom många andra samhällssektorer där en god förmåga att hantera kriser är av stor vikt. Penetrationsanalyser görs inte heller systematiskt och regelbundet inom granskade myndigheter. Initiativ till att systematiskt täcka avgörande kunskapsluckor som direkt rör betalningssystemet har inte tagits av Krisberedskapsmyndigheten eller Riksbanken.

Riksrevisionen bedömer också att myndigheternas övningsverksamhet inte i tillräcklig utsträckning speglar de omvärldsförhållanden som kan förväntas råda i samband med omfattande tekniska störningar i betalnings-

systemet. Det sker inte heller krisövningar där samhällsviktiga finansiella institutioner inklusive regeringen övar tillsammans.

Riksrevisionens sammanfattande slutsatser vilar på de bedömningar och slutsatser inom respektive granskat delområde som redovisas nedan.

7.2 Brister i regeringens givna förutsättningar

7.2.1 Otydliga mål och krav från regeringens sida

Riksrevisionen anser att det finns en otydlighet i målbilden som beror på att regeringen inte fastställt krav på grundläggande säkerhet och uthållighet i betalningssystemet. Detta kan bidras till såväl onödiga som uteblivna investeringar i säkerhetsåtgärder hos ansvariga myndigheter och företag.

Om målen inte är tydliga och enhetliga blir det också svårare att följa upp resultat av skyddsåtgärderna, värdera effekter av åtgärderna och få en samlad lägesbild. Otydliga mål försvårar därmed möjligheterna för myndigheterna att kunna förbereda och inrikta beredskapsåtgärder på ett effektivt sätt.

Rekommendation

Regeringen bör fastställa vilka grundläggande säkerhetskrav som ska gälla för betalningssystemet och dess nödvändiga infrastruktur. Regeringen bör också fastställa hur uthålligt betalningssystemet måste vara.

7.2.2 Ansvarsförhållandena och samverkan har svagheter

Riksrevisionen kan konstatera att ett stort antal myndigheter har ett ansvar för den finansiella sektorns krisberedskap. Den finansiella sektorns privat-offentliga samverkan har också märkbart breddats och intensifierats. Riksrevisionens granskning visar dock på vissa kvarstående brister i ansvarsfördelningen mellan myndigheter och i samverkansformer.

Ingen myndighet anser sig ha ett övergripande och samlat ansvar för ledning, planering, samverkan och uppföljning av krisberedskapen inom betalningssystemet. Sekretessproblem försvårar samarbete mellan myndigheter och näringsliv. Myndigheternas samverkan försvåras även av otydliga mål för det arbetet. Dessutom gäller formellt sett inte krisberedskapsförordningen för Riksbanken. Förordningar gäller bara för myndigheter under regeringen.

Därmed finns oklarheter i ansvarsförhållanden och uppgifter som enligt Riksrevisionens mening bidragit till att det i dag bland annat saknas en samlad bild av hot, risker, sårbarheter och konsekvenser. Detta har även bidragit till att myndigheterna ännu inte har samordnat sina förberedande åtgärder tillräckligt och att inte kunnat enas om gemensamma krav på myndigheter och andra aktörer utanför den finansiella sektorn som har en direkt påverkan på sektorns operativa förmåga.

Rekommendation

Riksrevisionen rekommenderar därför regeringen att fastställa vilken myndighet, exempelvis Finansinspektionen, som har det övergripande krisberedskapsansvaret för betalningssystemet och incidentbevakningen samt föreslå riksdagen i vilka avseenden Riksbanken ska ha ansvar för krisberedskapen. Regeringen bör också precisera samverkansområdenas arbete och sammansättning.

Riksrevisionen vill också fästa riksdagens uppmärksamhet vid behovet av att överväga en ändring av lagen (1988:1385) om Sveriges riksbank i syfte att bestämmelserna i förordningen (2006:942) om krisberedskap och höjd beredskap ska gälla för Riksbanken.

7.2.3 Uppföljning och tillsyn

Ett omfattande rapporteringsflöde som gäller krisberedskap har utvecklats, bland annat genom Krisberedskapsmyndighetens försorg. Uppföljningen inom området är dock enligt Riksrevisionen alltför uppsplittrad. Vad myndigheterna följer upp och hur man gör det, har gjorts olika under åren. Det saknas en genomarbetad strategi för hur uppföljningen ska ske. Bedömningen av förmåga är personberoende och saknar stöd av tydligt definierade begrepp.

Resultatet av tillsynen är inte heller integrerad i myndigheternas övergripande rapportering om risker och sårbarheter. Redovisningen är också i sig relativt knapphändig.

Eftersom det i dag inte heller finns en tydlig samordning av informationshanteringen i Regeringskansliet blir det svårare för regering och riksdag att få en heltäckande bild av beredskapen i det centrala betalningssystemet och svårare att jämföra myndigheternas skyddsåtgärder och bedömningar mellan olika år. En felaktig bild av krisberedskapen inom betalningssystemet ökar risken för felaktiga prioriteringar, ineffektiva investeringar i förebyggande åtgärder eller andra säkerhetsåtgärder.

Rekommendation

Riksrevisionen rekommenderar regeringen att se över hur krisberedskapen inom betalningssystemet följs upp. Här ingår att utse en central samordnare för all information om betalningssystemets krisberedskap och att kräva att myndigheterna återrapporterar all väsentlig information. Då blir det möjligt att göra en samlad analys av krisberedskapen inom betalningssystemet. Regeringen bör också se över tillsynen inom betalningssystemet. Här ingår att undersöka vilken teknisk kompetens som behövs, om föreskrifter behövs och hur myndigheterna bör redovisa resultatet av tillsynen.

7.3 Myndigheternas genomförande av krishanteringen

7.3.1 Risk- och sårbarhetsanalyser

En samlad bild av hot, risker och sårbarheter inom det centrala betalningssystemet som uppfyller krisberedskapsförordningens krav saknas i dag. Finansinspektionen har ställt samman en viss analys som har karaktären av samlad riskbedömning. Den saknar dock fördjupade analysresultat från el-, tele- och IT-området samt resultat från de fördjupade analyser som Riksbanken gör. Flera typer av hot har inte analyserats och sannolikhetsbedömningar saknas överlag. Analyser av åtgärder är ofullständiga.

En förklaring är att myndigheterna upplever att sekretesslagen är otillräcklig för att förhindra att grundläggande information om sårbarheter inom det egna ansvarsområdet lämnas ut till andra. Myndigheterna anser också att betalningssystemet är ett svårt område att analysera. Dock har inga initiativ till forskning tagits. Riksbankschefen lämnade en ytterligare förklaring i en intervju. Han menar att många ekonomer som sysslar med stabilitetsfrågor är makroekonomer och att dessa inte är skolade i hur mikroekonomer och säkerhetspersonal tänker om risker. Dessa olika professioner har ännu inte kunnat enas om ett gemensamt sätt att se på risker inom betalningssystemet. Åtgärder som avser IT-säkerhet, krisberedskapsåtgärder, traditionella tillsynsåtgärder samt åtgärder som framkommer i risk- och sårbarhetsanalyser respektive stabilitetsanalyser bedöms därför inte alltid tillsammans. Dessutom har aktörerna inte utvecklat civilrättsligt bindande sekretessavtal och tillämpat dessa i samverkansaktiviteterna.

Konsekvenserna av bristande risk- och sårbarhetsanalyser blir att det inte är säkerställt att de förebyggande åtgärder som vidtagits av ansvariga myndigheter och institut är tillräckliga för att kunna förhindra omfattande skadeverkningar för medborgare, företag och samhälle.

Rekommendation

Regeringen bör säkerställa att analyser av risker och sårbarheter i det centrala betalningssystemet görs och att dessa analyser uppfyller krisberedskapsförordningens krav. Regeringen bör också se över hanteringen av sekretessbelagda uppgifter och överväga att ge en myndighet föreskriftsrätt över hur risk- och sårbarhetsanalyserna ska utformas och följas upp.

Myndigheterna bör se till att deras risk- och sårbarhetsanalyser uppfyller krisberedskapsförordningens krav och beakta den kritik som framkommit i Krisberedskapsmyndighetens genomgångar av risk- och sårbarhetsanalyserna. I samband med detta bör myndigheterna sammanställa all information som finns tillgänglig inom den egna organisationen inklusive tillsynsenheterna. Myndigheterna ska också se till att analysen täcker hela myndighetens ansvarsområde. Riksgälden ska exempelvis se till att analysen täcker det statliga betalningssystemet i sin helhet.

7.3.2 Ej säkerställd operativ förmåga i ett krisläge

Enligt Riksrevisionens bedömning är det i dag inte säkerställt att aktörernas krisledningar fungerar väl tillsammans om en kris inträffar, eftersom dessa inte förberett sig och övat tillsammans i tillräcklig omfattning. Detta gäller särskilt händelseförlopp som kan få allvarliga skadeverkningar för medborgare, företag och samhälle. Om genomtänkta förberedelser saknas riskeras omfattande skadliga konsekvenser. Bortfall av centrala delar av betalningssystemet kan få långtgående konsekvenser för samhället redan efter några timmar eller något dygn. Då ställs stora krav på snabbt agerande och att inte onödig tid går åt till sådant som kunnat klaras av innan störningarna inträffade. Bristande förberedelser ökar också riskerna för konflikter kring vem ska göra vad och att det blir personal utan tillräcklig kompetens som får hantera en krissituation. Riksrevisionen bedömer därför att förmågan att hantera en allvarlig kris inom det centrala betalningssystemet är bristfällig.

Rekommendation

Regeringen bör se över hur myndigheter och institut förbereder sig för en akut allvarlig störning i betalningssystemet. Bland annat behöver en långsiktig strategi för gemensamma övningar utarbetas och funktionen ”Tjänsteman i beredskap” etableras inom den finansiella sektorn[127]. En sådan funktion har regeringen beslutat ska finnas inom många andra samhällsområden där en god förmåga att hantera kriser är av stor vikt. Regeringen bör också se

127 En ”Tjänsteman i beredskap” har enligt krisberedskapsförordningen (2006:942) i uppgift att initiera och samordna det inledande arbetet för att upptäcka, verifiera, larma och informera vid allvarliga kriser.

över ledningsansvaret för krisförberedelserna och behovet av en förberedd gemensam ledningsorganisation och en central ledningsplats inom sektorn.

Myndigheterna bör även komplettera sina krisplaner med åtgärder som behövs för att kunna samverka med andra aktörer som kan bidra till att höja beredskapen i betalningssystemet.

7.3.3 Myndigheternas genomförande av tillsynen

Granskningen visar att tillsynen och övervakningen av tekniska risker inom betalningssystemet är svag. Varken Finansinspektionen, Riksbanken eller Post- och telestyrelsen har verifierat bankernas och teleoperatörernas riskbedömningar på senare år. Finansinspektionen har valt att prioritera utvecklingsarbete och att granska ansökningar från bankerna om kapitalberäkningsmetod. Det finns i dag inga föreskrifter om skyddsåtgärder mot tekniska hot och risker. Det beror enligt myndigheterna på att man inte anser sig ha tillräckligt lagstöd för att avkräva bankerna en viss föreskriven säkerhet.

Finansinspektionen anser sig till exempel inte kunna meddela sanktioner som håller i domstol. Då krävs enligt inspektionen att regeringen definierar grundläggande säkerhetskrav.

Gemensamt för tillsynen inom Riksbanken, Finansinspektionen och Post- och telestyrelsen är att myndigheterna samtidigt vill främja goda kontakter med den privata sektorn. Riksrevisionen anser dock att det är rimligt att tillsynen via inspektioner på plats och stickprov faktiskt kontrollerar att bankerna har infört de skyddsåtgärder man säger sig ha och att kontrollsystemet faktiskt fungerar som det är tänkt.

Rekommendation

Riksbanken, Finansinspektionen och Post- och telestyrelsen bör via inspektioner på plats och genom stickprov faktiskt kontrollera att bankerna och infrastrukturföretagen har infört de skyddsåtgärder man säger sig ha och att kontrollsystemet faktiskt fungerar som det är tänkt. Riksrevisionen anser också att Finansinspektionen bör använda sin föreskriftsrätt och sina sanktionsmöjligheter så att brister i skyddet och regelbrott får konsekvenser för instituten och så att möjligheter skapas att få prövat i domstol hur långt skyldigheten enligt gällande lagar sträcker sig hos bankerna i principiellt viktiga fall.

7.4 Sammantagna konsekvenser av identifierade brister

Staten har ett ansvar för att säkerställa en förmåga att förebygga respektive hantera allvarliga störningar inom betalningssystemet. Riksrevisionen bedömer att det i granskningen framkommit brister i underlaget för att bedöma om motståndskraften i betalningssystemet är tillräcklig för att förhindra allvarliga betalningsstörningar. Därmed blir det också svårt att avgöra om den aktuella risknivån är acceptabel eller inte ur samhällets synvinkel. Ytterst är regeringen ansvarig för att landets infrastruktur är tillräckligt robust för att stå emot allvarliga störningar. Även om de grundläggande förutsättningar som Riksrevisionen identifierat saknas och många brister finns i de förberedelser som myndigheter vidtagit kan Riksrevisionen inte utesluta att det finns förmåga inom sektorn att hantera en allvarlig störning om den skulle inträffa. Eftersom en allvarlig störning ännu inte inträffat måste en bedömning av förmåga baseras på de förberedelser som gjorts i ett antal grundläggande avseenden. Riksrevisionen bedömer således att förmågan att förebygga och hantera allvarliga störningar inom det centrala betalningssystemet är bristfällig.

Skulle det bli avbrott i försörjningen av el, tele eller IT inom RIX-systemet eller inom annan central komponent i betalningssystemet och reservförfaranden inte fungerar kommer sektorn att uppleva likviditetsstörningar efter bara några timmar och bankernas kunder kommer inte att kunna genomföra normala bankfunktioner som att lösa lån, göra fastighetsaffärer och företagsköp. Värdepappershandeln kommer också att drabbas och myndigheternas betalningar inte kunna utföras. Om Riksgälden inte kan betala statens lån riskerar Sverige att internationella ratingorgan sätter ned sitt betyg och svenska banker får svårt att ta lån, för att bara nämna några följdverkningar.

En allvarlig el- eller telestörning kan också göra det omöjligt för medborgarna att ta ut kontanter, girera eller betala med kort. Inträffar detta kan förtroendet för det finansiella systemet skadas. Det kan i sin tur få än mer långsiktiga och skadliga effekter på samhället.

Referenser

Riksdagstryck och författningar

Regeringsformen (1974:152)
Myndighetsförordning (2007:515)
Lag (2006:1371) om kapitaltäckning och stora exponeringar
Lag (2005:240) om ändring i lagen (2003:389) om elektronisk kommunikation
Lag (2004:297) om bank- och finansieringsrörelse
Lag (2003:389) om elektronisk kommunikation (EkomL)
Lag (1988:1385) om Sveriges riksbank
Förordning (2006:942) om krisberedskap och höjd beredskap
Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten
Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap
Förordning (1997:401) med instruktion för Post- och telestyrelsen
Verksförordning (1995:1322); författningen är upphävd genom SFS 2007:515
Förordning (1994:714) med instruktion för Försvarets radioanstalt
Proposition 1986/87:143 om ny riksbankslag och ändrat huvudmannaskap för riksgäldskontoret
Proposition 2005/06:133 Samverkan vid kris – för ett säkrare samhälle. Försvarsdepartementet, 22 mars 2006
Betänkande 2005/06:FöU9. Samverkan vid kris – för ett säkrare samhälle
Betänkande 1999/2000: Utvecklingen av den ekonomiska styrningen FiU13, rskr.1999/2000:106
Betänkande 1994/95:FiU3 Riksbankens och Finansinspektionens beredskapsansvar (prop. 1994/95:47)

Övriga tryckta källor

Bank for International Settlements. 2007. *The Committee on Payment and Settlements systems*

Bank for International Settlements. 2006. *The Joint Forum – High level principles for business continuity*

Bank for International Settlements. 2005. *Central Bank oversight of payment and settlement systems*

Bank for International Settlements. 2001. *Core principles for systemically important payment systems*

Bank for International Settlements. 2001. *Recommendations for Securities Settlement Systems*

British Standards. 2007. *BS 25999 Business Continuity assessment Online*, spring 2007

Computer Sweden. 2005-10-05. *Sitic stängde koreanska sajten - inte polisen.*

ECB. 2006. *Business Continuity oversight expectations for systemically important payment systems (SIPS),* June 2006

ECB. 2005-05-18. *Memorandum of understanding on co-operation between the banking supervisors, central banks and Finance Ministries of the European Union in Financial crisis situations, Press release*

ECB. 2004. *Assessment of Euro-large payment systems against the core principles,* May 2004

ECB. 2004. *Standards for Securities Clearing and Settlement in the European Union*, September 2004

Erixon,C m.fl. 2006. *Basel II – En studie om regelverkets tillförlitlighet hos det svenska bankväsendet,* Kandidatuppsats. Ekonomihögskolan, Lunds universitet

FI.2007. *Förslag till förordnande av sakkunnig i företag under Finansinspektionens tillsyn samt ändrade regler för förordnade revisorer*

FI. 2007. *Anmälan om schablonmetoden, operativ risk*

FI. 2007. *Remissyttrande från Finansinspektionen*

FI. 2006. *Operativa risker – företagens hantering och FI:s rekommendationer.*

FI. 2005. *Finanssektorns krisberedskap*

FI. 2005. *Vägledning vid kontinuitetsplanering*

FI. 2005. *Överenskommelse mellan Finansinspektionen och Sveriges riksbank om arbetsfördelning och samarbete rörande finansiell stabilitet och krishantering*

FI. 2005. *Överenskommelse mellan Regeringskansliet (Finansdepartementet), Sveriges riksbank och Finansinspektionen för samarbete om finansiell stabilitet och krishantering*

FI. 2004. *Checklista Riskanalys operativa risker (ROP)* Block III

FI. 2004. *Tillsyn – remissförslag om en tydligare och effektivare offentlig tillsyn*

FI. 2004. *Riskmätning och kapitalkrav – vägledning II Operativ risk*

FI. 2003. *Samlad Riskbedömning. Riskanalys operativa risker (ROP)*

FI. 2003. Tillsynsstrategi

FI. 2002. *FI:s samverkan med granskningsmän*
FI. 1999. *Allmänna råd om rapportering av händelser av väsentlig betydelse,* FFFS 1999:7 (Upphävd)
Finlands bank. *Regulation and control of payment system risks – a Finnish perspective,* Bank of Finland Studies A:106
FOI. 2004. *Telekommunikationernas sårbarhet och risker för samhället*
FOI. 2002. *Marinens lessons learned process*
Försvarsdepartementet. 2006-11-30. *Uppdrag avseende bedömning av samhällets samlade krisberedskaps- respektive försvarsförmåga från och med 2007.* Regeringsbeslut 3, Fö2006/2843/CIV
Franck, E. 2005. *Riskmanagement in electronic banking*. Examensarbete i civilrätt, Stockholms universitet
Försvarsdepartementet. 2006. *Översyn av Statens räddningsverk, Krisberedskapsmyndigheten och Styrelsen för psykologiskt försvar för att skapa en myndighet för frågor om samhällets beredskap och säkerhet*. Kommittédirektiv, dir. 2006:80
Försäkringskassan. *Remissyttrande från Försäkringskassan Indikatorer på krisberedskapsförmåga*
GAO. 29/07/2005 *Financial Market Organizations Have Taken Steps to Protect against Electronic Attacks, but Could Take Additional Actions*
H M Treasury. 2003. *The financial system and major operational disruption*
International Monetary Fund. 2002. *Sweden: Financial System Stability Assessment, including Reports on the Observance of Standards and Codes on the following topics: Monetary and Financial Policy Transparency, Banking Supervision, Securities Regulation, Insurance Regulation, and Payment Systems*
KBM. 2007. *Verksamheten i samverkansområdena under perioden 1 september – 31 december 2006*
KBM. 2007. *Indikatorer på krisberedskapsförmåga*
KBM. 2007. *Samhällets krisberedskap förmåga 2006/2007*
KBM. 2007. *Öva krishantering*
KBM. 2006. *Så vill vi utveckla övningsverksamheten*
KBM. 2006. *Privat-offentlig samverkan från idé till fungerande praktik*
KBM. 2005. *Mind the gap! Hur bygger vi broar mellan stat och näringsliv i arbetet med krisberedskap?*
KBM. 2005. *Samverkan mellan offentlig sektor och näringsliv vid krishantering. En studie av kriser i Sverige 1993-2003*
KBM. 2005. *Samhällets krisberedskap för verksamheten 2007*, planeringsprocessen
KBM. 2003. *Metodutveckling av den årliga uppföljningen*
Lind, G. 2003. *Krisövning ger krisfärdighet.* Penning- och valutapolitik 4/2003
Mandia, K & Prosise, K. 2001. *Incident reports*
Nationella styrgruppen för privat-offentlig samverkan. 2005-03-02. *Utvecklingen av privat-offentlig samverkan för den tekniska infrastrukturens säkerhet och beredskap.* Energimyndigheten

PTS. 2007. *PTS allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid*
PTS. 2007. *PTS allmänna råd om god funktion och teknisksäkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid*
PTS. 2007. *Tillsyn på N*, Internt arbets-PM
PTS. 2006. *Konsekvensutredning*
PTS. 2006. *Robusta elektroniska kommunikationer Strategi för åren 2006–2008*
PTS. 2006. *Policy för tillsyn*
PTS. 2005. *Strategi för att säkra Internets infrastruktur*
PTS. 2005. *Tillsynsutredningens slutbetänkande: Tillsyn. Förslag om en tydligare och effektivare offentlig tillsyn (SOU 2004:100)*
PTS. 2005. *Utredning och länderinformation rörande driftavbrott och krav på god teknisk funktion och säkerhet m.m*
PTS. 2004. *Uppbyggnaden av Sveriges IT incidentcentrum.*
PTS. 2004. *Strategi för ett säkrare Internet*
Riksbanken. 2006. *Ansvar och samverkan för kontinuitets- och krisplanering i det finansiella systemet*
Riksbanken. 2006. *Yttrande över Remiss om Finansdepartementets promemoria om nya kapitaltäckningsregler*
Riksbanken. Eva Srejber, 2006. *Sårbarheter i det moderna betalningsväsendet*
Riksbanken. 2005. *Instruktion*
Riksbanken. 2004. *Arbetsordning*
Riksbanken. Sammanställning av resultatet av verksamhetsberoende analyser och Hot- och riskanalyser, år 2002 och 2003
Riksbanken. 2003. *Yttrande över Framtida finansiell tillsyn (SOU 2003:22)*
Riksbanken. 2002. *Riktlinjer för Riksbankens kontinuitetsskydd*
Riksbanken. 2001. *Riksbankens roll som övervakare av den finansiella infrastrukturen.* Penning- och valutapolitik
Sandebring, A. 2006. *Att organisera privat-offentlig samverkan*. Licentiatavhandling, HHS Stockholm.
Skatteverket. 2007. *Yttrande över Krisberedskapsmyndighetens remiss: Indikatorer på krisberedskapsförmåga*
SOES. 2005. *Sammanställning av RSA-arbetet inom SOES,* Samverkansområdet Ekonomisk Säkerhet, KBM
SOU 2004:100 *Tillsyn – Förslag om en tydligare och effektivare offentlig tillsyn*
US Securities and Exchange Commission. 2003-04-07. *Interagency Paper on Sound practices to strengthen the Resilience of the U.S. Financial System*

I granskningen ingår också årligen återkommande offentligt tryck såsom regleringsbrev, myndighetsinstruktioner, verksamhetsplaner och årsredovisningar för samtliga granskade myndigheter 2003—2007 samt Krisberedskapsmyndighetens årliga uppföljning för åren 2003—2006, Riksbankens stabilitetsrapporter 2001—2007 och Finansinspektionens stabilitetsrapporter 2005—2006.

Otryckta källor

De otryckta källor som ligger till grund för rapporten omfattar bland annat hemsidor på Internet, FSPOS mötesdokumentation 2005-2006, SOES mötesdokumentation 2005-06-08 till 2007-01-01, Risk- och sårbarhetsanalyser 2003–2006 för Riksbanken och samtliga granskade myndigheter samt slutrapporter och utvärderingar från övningar avseende tekniska hot och risker i betalsystemet under perioden 2003–2007.

Intervju- och mötesförteckning
Bankföreningen. 2007-03-19
Bankgirocentralen. 2007-06-05
Caleyon Bank. 2007-05-04
Finansinspektionen. 2007-02-05, 2007-04-03, 2007-08-08, 2007-09-04, 2007-09-06, 2007-09-31, 2007-10-02 och 2007-10-08
4 C Strategies. 2007-06-11 och 2007-09-17
Försvarets forskningsinstitut. 2007-03-23
Försvarets radioanstalt. 2007-04-27
Försäkringskassan. 2007-03-02
Krisberedskapsmyndigheten. 2006-11-20, 2007-02-26, 2007-05-02, 2007-06-04 och 2007-08-28
Post- och telestyrelsen. 2007-03-13,2007-08-30, 2007-09-30
Regeringskansliet, Finansdepartementet. 2007-03-05, 2007-09-14, 2007-09-27 Statsrådsberedningen/Enheten för beredskap och analys 2007-09-26
Riksbanken. 2007-02-02, 2007-03-21, 2007-04-17, 2007-05-25, 2007-06-01, 2007-06-05, 2007-09-05, 2007-09-19, 2007-10-04 och 2007-10-31
Riksgäldskontoret. 2007-04-25, 2007-05-07 och 2007-09-07
SEB. 2007-06-01
Sitic. 2007-02-05
Skandia. 2007-03-22
Värdepapperscentralen. 2007-06-20
FSPOS. 2007-11-27. FSKLÖ701. Seminarium i Norra Latin arrangerat av Finansinspektionen

Brev och e-post
Committee of European Banking superviors. 2007-10-16. e-post
FI. 2007-11-01. Brev till Riksrevisionen
Finansinspektionen i Finland. 2007-10-30. e-post
Finansinspektionen i Nederländerna. 2007-11-08. e-post
Riksbanken. 2007-11-02. Brev till Riksrevisionen
Riksbanken. 2007-10-25. Brev till Riksrevisionen
Riksbanken. 2007-08-27. Brev till Riksrevisionen

Övriga referenser
ECB. 2004. *Pressbriefing on the "ECB Financial Stability Review",*
Opening Remarks by Jean Claude Trichet
FI. 2004. *Finansinspektionens tillsyn i ett Basel II-perspektiv. Anförande av Finansinspektionens avdelningschef Kerstin af Jochnick vid Risk Management Forum*
KBM. 2007. *Samverkansområdet Ekonomisk säkerhet.*
Riksgäldskontoret. 2007. *Säkerhet och krishantering i Ramavtal för betalningar,*
Anita Schönbeck, OH-presentation.
Sveriges Radio. 2007-01-02. *Bankerna har för dålig IT-säkerhet.*
Uttalande av kriminalkommissarie Anders Ahlqvist vid Rikskriminalen
Stefan Ingves. 1996. *Riksbankens roll i ett elektroniskt betalningssystem*,
IIRs konferens, Berns Congress

Bilaga 1 Bedömningsgrunder för förmåga

För att bedöma förmåga har Riksrevisionen identifierat sex grundläggande förutsättningar som enligt krisberedskapsförordningen, uttalanden av regeringen och egna rimlighetsbedömningar krävs för en god förmåga att förebygga och hantera en kris. Dessa grundförutsättningar är följande:

- Risk- och sårbarhetsanalyser.
- Förberedelser för att kunna hantera kriser.
- Övningar.
- Penetrationstester.
- Incidentrapportering och incidentanalyser.
- Forskning för att täcka in luckor i kunskapen.

A. Bedömningsgrunder för risk- och sårbarhetsanalyser

Myndigheter under regeringen och samverkansorgan

Bedömningsgrunder här är ett antal krav som vi anser att det är rimligt att ställa på utpekade myndigheters risk- och sårbarhetsanalyser enligt krisberedskapsförordningen (2002:472) och (2006:942) vad avser bedömning av risker och sårbarheter. Att vi även utgår från den äldre förordningen förklaras av att den har utgjort normen för de risk- och sårbarhetsanalyser som myndigheterna har genomfört under åren 2003–2006. Vi anser att följande krav kan ställas direkt utifrån förordningarna[128]:

1. Myndigheten bör ha genomfört risk- och sårbarhetsanalyser årligen under perioden 2003–2007 (3§).
2. Analyserna bör ha ett samhällsperspektiv (3 §) och inte enbart avgränsas till risker för och sårbarheter i myndighetens egen verksamhet eller ansvarsområde.
3. Hot/risker och sårbarheter bör vara identifierade och hållas isär (för risk- och sårbarhetsanalyser enligt äldre förordning 3§).

Vidare anser vi att följande krav kan ställas utifrån en rimlig tolkning av förordningen:

4. Möjligheten att bedöma sannolikheten för att risk eller hot ska realiseras bör framgå (3 § andra stycket – myndigheten ska värdera resultatet).
5. Konsekvenser av realiserade hot/risker bör framgå.

128 Vi har här valt att hänvisa till den äldre förordningens paragrafer, i stället för att ange paragrafer från bägge förordningarna.

Vi anser därutöver att följande krav allmänt kan ställas för Risk och sårbarhetsanalyser:

6. Metod för analysernas genomförande bör framgå eller hänvisas till.
7. Hot/risker och sårbarheter bör vara så specificerade att det är möjligt att bedöma vilka åtgärder som kan komma i fråga.

Enligt krisberedskapsförordningen (2006:942) ska analysen av hot och risker även innefatta planerade åtgärder och en bedömning av behovet av ytterligare åtgärder. Mera precist är bedömningsgrunderna här följande:

8. Myndigheternas vidtagna och planerade åtgärder för att hantera identifierad risk/sårbarhet bör framgå (4 § första stycket).

Vidare anser vi att följande krav kan ställas utifrån en rimlig tolkning av förordningen:

9. Myndigheten bör också ta upp behovet av ytterligare åtgärder från den egna myndigheten (4 § första stycket).
10. Vidtagna, planerade eller nödvändiga åtgärder bör relateras till identifierad hot/risk eller sårbarhet (4 §) och till de konsekvenser som kan inträffa.
11. Metod för åtgärdsanalysernas genomförande bör framgå eller hänvisas till.
12. Kostnaderna för planerade eller nödvändiga åtgärder bör uppskattas och ställas i relation till den skadeverkan och de kostnader som kan uppstå om åtgärderna inte genomförs.

Riksbanken – internationella standarder och krav

Riksbanken är inte skyldig att redovisa en risk- och sårbarhetsanalys enligt kriterier i krisberedskapsförordningen. Riksbanken följer dock som tidigare nämnts internationella standarder som rekommenderats av CPSS. I sina huvuddrag liknar Princip VII som avser säkerhet, tillförlitlighet och reservkapacitet i betalningssystemen kriterierna i krisberedskapsförordningen. Följande rekommenderas bland annat av CPSS:

- Identifiera möjliga hot och deras storlek (konsekvenser och sannolikhet)... Ägaren av betalningssystem och deltagarna samt leverantörer av infrastruktur ska genomföra analyser och planera arrangemang som kan ge kontinuitet i en mångfald av möjliga scenarier. Dessa scenarier ska utgå ifrån att vardera av centrala komponenter och infrastruktur slås ut. Både interna och externa hot ska bedömas och följderna av varje utslagning identifieras och utvärderas. Lokaliseringen av ett andra produktionsställe kommer till exempel att bero på naturen hos de hot den ska skydda emot. Ett vanligt övervägande är att få skydd mot avbrott i telekommunikationer och elförsörjning som påverkar både det primära

och sekundära produktionsstället. Systemägaren behöver också överväga om deltagarna ska ha ett andra produktionsställe.

- Identifiera existerande eller potentiella skyddsåtgärder.
- Identifiera residualrisker och sårbarheter.

B. Grunder för bedömning av förberedelser för att hantera en kris

Som grund för att bedöma krishanteringsförmågan och den operativa förmågan analyseras de centrala aktörernas *förberedelser* för att kunna hantera omfattande tekniska avbrott i det centrala betal- och transaktionssystemet. Med väl avvägda förberedelser ökar förutsättningarna för en god operativ förmåga. Krisberedskapsmyndigheten har för de förmågebedömningar som myndigheterna ska göra tagit fram framgångsfaktorer för den operativa krishanteringen i sex faser före, under och efter en kris. I varje fas finns ett antal indikatorer på operativ förmåga som Riksrevisionen finner rimliga att använda vid förmågebedömningar. Faserna och indikatorerna är följande:

Tidigt upptäcka

- Utsedd ”Tjänsteman i beredskap” finns.
- Metoder och vägar att höja uppmärksamheten utnyttjas.
- Olika former av kontinuerlig omvärldsbevakning eller andra förvarningssystem finns etablerade.
- Larmförbindelser inklusive kontakter med Säpo har etablerats.

Övningsverksamhetens inriktning och omfattning

Se bedömningsnormer i avsnitt C nedan.

Ledningskompetens

- Tillgänglig kompetens enligt krisplan.
- Information för nödvändiga beslut.

Planlagd operativ ledning och samverkan

- Tydligt angivna och uppdaterade uppgifter om vem som gör vad.
- Dokumenterade rutiner finns för att snabbt skapa en lägesbild (analysera lägesinformation om tillstånd, förväntad utveckling, vidtagna åtgärder och tillgängliga resurser).
- Ett klart fastställt nätverk, internt inom egen organisation eller med externa organisationer och av de strukturer som krävs för en effektiv samordning vid kris- Uppdaterade checklistor med kontaktuppgifter till samverkande aktörer.
- Säkerställt att det finns tillräckligt med materiel och personal.

Förberedda kanaler för spridning av information till omvärlden

- Förberedda mallar för pressmeddelanden med mera.
- Uppdaterade adressuppgifter.
- Flera alternativt tillgängliga informationskanaler.

Förberedelser för att minska skadeverkningar och återställa funktion efter avbrott

- Dokumenterade åtgärder som ska vidtas för att skydda akut hotade objekt, hindra utbredning och spridning av effekterna.
- Förberedda åtgärder som sörjer för att medborgarna får tillgång till finansiella tjänster på andra sätt.
- Förberedelser för att kunna ta hand om hjälpbehövande (i akut behov av pengar).
- Identifierade och förberedda tillfälliga lösningar som snabbt ska finnas tillgängliga inklusive reservlösningar, alternativa rutiner och arbetsmetoder som reducerar spridningen av skadeverkningarna.
- Rutiner och garantier för att försvunna medel återbetalas.
- Regelverk. Det finns legalt stöd för hur myndigheten/sektorn ska hantera händelsen, riktlinjer och policy för hur myndigheten/sektorn ska hantera händelsen och avtal som gäller vid händelsen.
- Identifierade och i förväg beslutade åtgärder som förbättrar möjligheterna att snabbt och tillfredsställande återställa ordinarie funktioner.

C. Grunder för att bedöma övningar

Våra bedömningsgrunder för övningar baseras dels på krav i krisberedskapsförordningen, dels på rimlighetsbedömningar. Den senare typen av bedömningar understöds här av rekommendationer från Krisberedskapsmyndigheten om hur väl fungerande övningar bör se ut. Bedömningskriterierna är följande. För att bibehålla och utveckla förmågan bör övningarna enligt krisberedskapsförordningen ske planlagt och regelbundet[129]. Alla aktörer, både privata och offentliga, som har en uppgift vid en kris bör enligt Krisberedskapsmyndigheten öva tillsammans.[130] För planering av övningarna bör dessutom bland annat risk- och sårbarhetsanalyserna utgöra ett underlag.[131] Enligt Krisberedskapsmyndigheten bör en övning även innehålla följande moment:

- Upptäcka en händelse.
- Hantering av information till allmänhet och media.
- Ledning och samverkan.
- Minska konsekvenserna.
- Återställning av betalnings- och transaktionsfunktionerna.

För att en övning ska förbättra förmågan att hantera kriser krävs också en fungerande återkoppling till organisationen.[132] Övningarna bör därför utvärderas omedelbart efter övningen. En noggrannare utvärdering som resulterar i en skriftlig rapport bör också genomföras i närtid efter övningen.[133] Det är även viktigt att övningarna är öppna så att deltagarna kan ta del av andra aktörers erfarenheter.[134]

D. Grunder för att bedöma penetrationstester

I ”Säkerhet i en ny tid” (SOU 2001:41), från Sårbarhets- och säkerhetsutredningen betonades vikten av att säkerställa att viktiga IT-system skyddas från angrepp och FRA fick ansvar för bland annat penetrationstester. Sådana tester är enligt utredningen ett effektivt medel för en organisation att få graden av informationssäkerheten tydliggjord, vilket också är Riksrevisionens uppfattning. Vi anser det dessutom rimligt att betalningssystemets IT-miljö regelbundet prövas med penetrationstester.

129 Se även KBM (2006) *Så vill vi utveckla övningsverksamheten.*
130 KBM (2007) *Öva krishantering.*
131 KBM (2007) *Öva krishantering.*
132 FOI (2002) *Marinens lessons learned process.*
133 Göran Lind: *Krisövning ger krisfärdighet,* Penning- och valutapolitik 4/2003.
134 FOI (2002) *Marinens lessons learned process.*

E. Grunder för att bedöma incidentrapportering och incidentanalyser

Myndigheterna inom samverkansområdet Ekonomisk säkerhet ska enligt krisberedskapsförordningen särskilt beakta annan kunskapsinhämtning såsom erfarenhetsåterföring av inträffade händelser. Försvarets radioanstalt, Sitic och Finansinspektionen har även fått i uppgift att sammanställa erfarenheter från incidenter som inträffar inom IT-området. Ett rimligt krav är att den incidentrapportering som berör betalningssystemet antingen är samordnad eller kan samlas på ett ställe. Ett annat rimligt krav är enligt Riksrevisionen att allvarliga incidenter bör rapporteras så fort som möjligt och till rätt mottagare[135].

F. Grunder för att bedöma forskningen

Myndigheterna inom samverkansområdet Ekonomisk säkerhet ska enligt krisberedskapsförordningen särskilt beakta behovet av forsknings- och utvecklingsinsatser. KBM ska enligt sin instruktion initiera forskning och studier samt ta del av, analysera och förmedla forskningsresultat.
Målet med den ekonomiska forskning som bedrivs inom Riksbanken är enligt banken själv att tillhandahålla en solid begreppsmässig och empirisk grund för politiska beslut. Högkvalitativ forskning är enligt Riksbanken avgörande för att garantera att Riksbanken är väl förberedd att möta de utmaningar som hänger samman med att främja ett säkert och effektivt betalningssystem. En viktig uppgift för den ekonomiska forskningen är – också enligt banken – att tillhandahålla modeller, verktyg och analyser för att Riksbanken ska kunna fullgöra sina åligganden. Det är enligt Riksrevisionen då rimligt att även forskning inom området tekniska hot och risker inom betalningssystemet bör finnas för att tillhandahålla modeller, verktyg och analyser i den utsträckning detta behövs och saknas.

G. Samlad bedömning av förmåga

Vid en bedömning av samlad förmåga hos regering och myndigheter att förebygga och hantera allvarliga störningar i betalningssystemet använder Riksrevisionen regeringens och Krisberedskapsmyndighetens klassificeringar: God, god men vissa briser, bristfällig och mycket bristfällig. Den samlade bedömningen görs utifrån vilka brister som konstaterats i de sex enskilda grundförutsättningar som redovisats ovan. För att kunna väga samman och klassificera förmåga har vi ställt följande krav på uppfyllda grundförutsättningar.

135 Mandia , K och Prosise K.

Klassificering	Riksrevisionens krav
God förmåga	Samtliga grundförutsättningar är uppfyllda.
God förmåga men med vissa brister	Någon eller några grundförutsättningar har brister.
Bristfällig förmåga	Flertalet grundförutsättningar har brister.
Mycket bristfällig förmåga	Samtliga grundförutsättningar har allvarliga brister.

Tidigare utgivna rapporter från Riksrevisionen

2003	2003:1	Hur effektiv är djurskyddstillsynen?
2004	2004:1	Länsplanerna för regional infrastruktur – vad har styrt prioriteringarna?
	2004:2	Förändringar inom kommittéväsendet
	2004:3	Arbetslöshetsförsäkringens hantering på arbetsförmedlingen
	2004:4	Den statliga garantimodellen
	2004:5	Återfall i brott eller anpassning i samhället – uppföljning av kriminalvårdens klienter
	2004:6	Materiel för miljarder – en granskning av försvarets materielförsörjning
	2004:7	Personlig assistans till funktionshindrade
	2004:8	Uppdrag statistik – Insyn i SCB:s avgiftsbelagda verksamhet
	2004:9	Riktlinjer för prioriteringar inom hälso- och sjukvård
	2004:10	Bistånd via ambassader – en granskning av UD och Sida i utvecklingssamarbetet
	2004:11	Betyg med lika värde? – en granskning av statens insatser
	2004:12	Höga tjänstemäns representation och förmåner
	2004:13	Riksrevisionens årliga rapport 2004
	2004:14	Arbetsmiljöverkets tillsyn
	2004:15	Offentlig förvaltning i privat regi – statsbidrag till idrottsrörelsen och folkbildningen
	2004:16	Premiepensionens första år
	2004:17	Rätt avgifter? – statens uttag av tvingande avgifter
	2004:18	Vattenfall AB – Uppdrag och statens styrning
	2004:19	Vem styr den elektroniska förvaltningen?
	2004:20	The Swedish National Audit Office Report 2004
	2004:21	Försäkringskassans köp av tjänster för rehabilitering
	2004:22	Arlandabanan – Insyn i ett samfinansierat järnvägsprojekt
	2004:23	Regelförenklingar för företag
	2004:24	Snabbare asylprövning
	2004:25	Sjukpenninganslaget – utgiftsutveckling under kontroll?
	2004:26	Utgift eller inkomstavdrag? – Regeringens hantering av det tillfälliga sysselsättningsstödet
	2004: 27	Stödet till polisens brottsutredningar
	2004:28	Regeringens förvaltning och styrning av sex statliga bolag
	2004:29	Kontrollen av strukturfonderna

	2004:30	Barnkonventionen i praktiken
2005	2005:1	Miljömålsrapporteringen – för mycket och för lite
	2005:2	Tillväxt genom samverkan? Högskolan och det omgivande samhället
	2005:3	Arbetslöshetsförsäkringen – kontroll och effektivitet
	2005:4	Miljögifter från avfallsförbränningen – hur fungerar tillsynen
	2005:5	Från invandrarpolitik till invandrarpolitik
	2005:6	Regionala stöd – styrs de mot ökad tillväxt?
	2005:7	Ökad tillgänglighet i sjukvården? – regeringens styrning och uppföljning
	2005:8	Representation och förmåner i statliga bolag och stiftelser
	2005:9	Statens bidrag för att anställa mer personal i skolor och fritidshem
	2005:10	Samordnade inköp
	2005:11	Bolagiseringen av Statens järnvägar
	2005:12	Uppsikt och tillsyn i samhällsplaneringen – intention och praktik
	2005:13	Riksrevisionens årliga rapport 2005
	2005:14	Förtidspension utan återvändo
	2005:15	Marklösen – Finns förutsättningar för rätt ersättning?
	2005:16	Statsbidrag till ungdomsorganisationer – hur kontrolleras de?
	2005:17	Aktivitetsgarantin – Regeringen och AMS uppföljning och utvärdering
	2005:18	Rikspolisstyrelsens styrning av polismyndigheterna
	2005:19	Rätt utbildning för undervisningen – Statens insatser för lärarkompetens
	2005:20	Statliga myndigheters bemyndiganderedovisning
	2005:21	Lärares arbetstider vid universitet och högskolor – planering och uppföljning
	2005:22	Kontrollfunktioner – två fallstudier
	2005:23	Skydd mot mutor – Läkemedelsförmånsnämnden
	2005:24	Skydd mot mutor – Apoteket AB
	2005: 25	Rekryteringsbidrag till vuxenstuderande – uppföljning och utbetalningskontroll
	2005:26	Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten
	2005:27	Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten
	2005:28	Fokus på hållbar tillväxt? Statens stöd till regional projektverksamhet
	2005:29	Statliga bolags årsredovisningar
	2005:30	Skydd mot mutor – Banverket
	2005:31	När oljan når land – har staten säkerställt en god kommunal beredskap för oljekatastrofer?

2006	2006:1	Arbetsmarknadsverkets insatser för att minska deltidsarbetslösheten
	2006:2	Regeringens styrning av Naturvårdsverket
	2006:3	Kvalitén i elöverföringen – finns förutsättningar för en effektiv tillsyn?
	2006:4	Mer kemikalier och bristande kontroll – tillsynen av tillverkare och importörer av kemiska produkter
	2006:5	Länsstyrelsernas tillsyn av överförmyndare
	2006:6	Redovisning av myndigheters betalningsflöden
	2006:7	Begravningsverksamheten – förenlig med religionsfrihet och demokratisk styrning?
	2006:8	Skydd mot korruption i statlig verksamhet
	2006:9	Tandvårdsstöd för äldre
	2006:10	Punktskattekontroll – mest reklam?
	2006:11	Vad och vem styr de statliga bolagen?
	2006:12	Konsumentskyddet inom det finansiella området – fungerar tillsynen?
	2006:13	Kvalificerad yrkesutbildning – utbildning för marknadens behov?
	2006:14	Arbetsförmedlingen och de kommunala ungdomsprogrammen
	2006:15	Statliga bolag och offentlig upphandling
	2006:16	Socialstyrelsen och de nationella kvalitetsregistren inom hälso- och sjukvården
	2006:17	Förvaltningsutgifter på sakanslag
	2006:18	Riksrevisionens årliga rapport
	2006:19	Statliga insatser för nyanlända invandrare
	2006:20	Styrning och kontroll av regeltillämpningen inom socialförsäkringen
	2006:21	Finansförvaltningen i statliga fastighetsbolag
	2006:22	Den offentliga arbetsförmedlingen
	2006:23	Det makroekonomiska underlaget i budgetpropositionerna
	2006:24	Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten
	2006: 25	Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten
	2006:26	Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten
	2006:27	Regeringens uppföljning av överskottsmålet
	2006:28	Anställningsstöd
	2006:29	Reformen av Försvarets logistik – Blev det billigare och effektivare?
	2006:30	Socialförsäkringsförmåner till gravida – Försäkringskassans agerande för en lagenlig och enhetlig tillämpning
	2006:31	Genetiskt modifierade organismer – det möjliga och det rimliga
	2006:32	Bidrag som regeringen och Regeringskansliet fördelar

2007	2007:1	Statlig tillsyn av bostad med särskild service enligt LSS
	2007:2	The Swedish National Audit Office – Annual report 2006
	2007:3	Regeringens beredning och redovisning av skatteutgifter
	2007:4	Beredskapen för kärnkraftsolyckor
	2007:5	Regeringens skatteprognoser
	2007:6	Vägverkets körprov – lika för alla?
	2007:7	Den största affären i livet – tillsyn över fastighetsmäklare och konsumenternas möjlighet till tvistelösning
	2007:8	Regeringens beredning av förslag om försäljning av sex bolag
	2007:9	Säkerheten vid vattenkraftdammar
	2007:10	Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen
	2007:11	Statens företagsbefrämjande insatser. Når de kvinnor och personer med utländsk bakgrund?
	2007:12	Hur förbereds arbetsmarknadspolitiken? En granskning av regeringens underlag
	2007:13	Granskning av Årsredovisning för staten 2006
	2007:14	Riksrevisionens årliga rapport
	2007:15	Almi Företagspartner AB och samhällsuppdraget
	2007:16	Regeringens uppföljning av kommunernas ekonomi
	2007:17	Statens insatser för att hantera omfattande elavbrott
	2007:18	Bilprovningen och tillgängligheten – Granskning av ett samhällsuppdrag
	2007:19	Tas sjukskrivnas arbetsförmåga till vara? Försäkringskassans kontakter med arbetsgivare
	2007:20	Oegentligheter inom bistånd – Är Sidas kontroll av biståndsinsatser via enskilda organisationer tillräcklig?
	2007:21	Regeringens analys av finanspolitikens långsiktiga hållbarhet
	2007:22	Sambandet mellan utgiftstaket, överskottsmålet och skattepolitiken – regeringens redovisning
	2007:23	Statens insatser vid anmälningar av vårdskador – Kommer patienten till tals?
	2007:24	Utanförskap på arbetsmarknaden.
	2007:25	Styrelser med fullt ansvar.
	2007:26	Regeringens redovisning av budgeteffekter.
	2007: 27	Stödet till polisens brottsutredningar

Beställning: publikationsservice@riksrevisionen.se