



UPPSALA
UNIVERSITET

EXAMENSARBETE
Företagsekonomiska institutionen
Företagsekonomi D, vt 2010

Kontinuitetshantering i finanssektorn

Svenska finansiella företags hantering av operativa risker

Författare
Johanna Busk
Magnus Friberg

Handledare
Mats Karén

SAMMANDRAG

I takt med förändringar såsom ökad globalisering och teknologisk utveckling har begrepp som riskhantering vuxit fram som en vital del av företags långsiktiga strategi. En del av ett företags riskhantering bör innehålla en plan som anger hur den operativa verksamheten kan fortgå när en kris inträffar. Detta kallas för kontinuitetshantering, vilket är desamma som hantering av operativa risker. I en rapport från 2005 fastslog Finansinspektionen att det fanns generella brister i kontinuitetshantering inom den svenska finanssektorn då kvalitén och omfattningen på företags kontinuitetsplaner varierade kraftigt.

Denna studie genomfördes i det övergripande syftet att analysera hur svenska finansiella företag hanterar de risker som uppkommer i den dagliga verksamheten och om detta görs på ett tillfredställande sätt, givet Finansinspektionens rekommendationer och brittisk standard för kontinuitetshantering. Studien ämnade också undersöka vilka faktorer som driver företagens kontinuitetshanteringsarbete och identifiera förbättringsmöjligheter.

Det teoretiska ramverket utgjordes av Finansinspektionens vägledande dokument för kontinuitetshantering samt den brittiska standarden BS25999.

Vi valde att undersöka hur väl finansiella företag hanterar operativa risker samt om de följer de riktlinjer som finns, genom en så kallad mognadsmodell. Business Continuity Maturity Model (BCM-modellen) illustrerar hur utvecklad kontinuitetshantering är genom att placera företag i sex olika nivåer. För att även undersöka vilka faktorer som driver kontinuitetshanteringsarbetet utgick det empiriska materialet och analysen från BCM-modellens kontinuitetskompetenser; ledarskap och implementering, anställdas medvetenhet och övning, resursfördelning och mätning samt externa förbindelser.

Undersökningen bestod av totalt 17 företag som delades in i kategorierna banker, pensions- och försäkringsbolag, storbanker och övriga finansiella aktörer. Resultaten av studien ledde fram till flera slutsatser. Vi anser att svenska finansiella företag tenderar att överlag hantera operativa risker genom att hålla en medelhög beredskapsnivå gentemot störningar i kärnverksamheten, vilket inte är högt nog. Företagen uppnår en genomsnittlig mognadsnivå om 4,26 enligt BCM-modellen. Företagen har därmed en kortsiktigt god kontinuitetshantering men för att nå högre kvalitetsnivåer måste kontinuitetshantering ingå till större del i företagens långsiktiga strategi.

Vidare visade resultaten att ledarskap och implementering generellt sett är de mest drivande faktorerna och resursfördelning och mätning de minst drivande faktorerna - en trend som kan ses inom alla fyra företagstyper.

Det är fortfarande för stor spridning bland de finansiella företagen för att kunna dra slutsatsen att branschen som helhet följer Finansinspektionens rekommendationer. Inget företag i undersökningen skulle heller enligt vår tolkning inte vara redo att certifieras mot BS25999.

INNEHÅLLSFÖRTECKNING

1. INTRODUKTION.....	3
1.1 Bakgrund.....	3
1.2 Problemdiskussion	4
1.3 Syfte	5
1.4 Definitioner	5
1.4.1 Vad är risk?	5
1.4.2 Vad är "en störning" i verksamheten?	5
2. TEORETISKA BEGREPP	6
2.1 Riskhantering	6
2.2 Kontinuitetshantering	7
3. TEORETISKT RAMVERK.....	8
3.1 Kontinuitetshanterings mognadsgrad	8
3.2 Ledarskap och implementering.....	9
3.2.1 Finansinspektionens rekommendationer	9
3.2.2 Riktlinjer enligt BS25999.....	10
3.3 Anställdas medvetenhet och övning.....	10
3.3.1 Finansinspektionens rekommendationer	10
3.3.2 Riktlinjer enligt BS25999.....	11
3.4 Resursfördelning och mätning	11
3.4.1 Finansinspektionens rekommendationer	11
3.4.2 Riktlinjer enligt BS25999.....	12
3.5 Externa förbindelser	13
3.5.1 Finansinspektionens rekommendationer	13
3.5.2 Riktlinjer enligt BS25999.....	13
3.6 Spelar kontinuitetshantering verkligen någon roll?	14
3.7 Sammanfattning; analysmodell.....	14
4. METOD.....	16
4.1 Business Continuity Maturity Model	16
4.2 Datainsamlingsmetod och operationalisering	18
4.2.1 Studiens giltighet och trovärdighet.....	20
4.3 Metodproblematik.....	21
4.3.1 Kvantitativ metod.....	21
4.3.2 Att använda en "konsultmodell" för datainsamling	21
4.3.3 Urval av företag.....	22
5. EMPIRISK ANALYS	22
5.1 Mognadsnivå inom kontinuitetshantering.....	22
5.2 Faktorer som påverkar mognadsnivån	25
5.2.1 Ledarskap och implementering.....	26
5.2.2 Anställdas medvetenhet och övning.....	30
5.2.3 Resursfördelning och mätning.....	32
5.2.4 Externa förbindelser	35
6.1 Hur väl hanterar svenska finansiella företag operativa risker?	37
6.2 Vilka faktorer driver deras kontinuitetshanteringsarbete?	38
6.3 Är det tillräckligt för att möta Finansinspektionens rekommendationer och hur står sig detta mot internationell standard?.....	39
6.5 Utvärdering av metod.....	40
6.6 Förslag till fortsatt forskning.....	40
KÄLL- OCH LITTERATURFÖRTECKNING	42

1. INTRODUKTION

1.1 Bakgrund

Människans tillvaro har i alla tider präglats av olika former av risk som i varierande grad påverkat levnadssituationen. Historiskt sett har människans överlevnad och framgång bestämts av förmågan att övervinna eller undvika dessa risker. Det är också medvetenheten om den förmågan som leder till att människor avsiktligt tar risker varje dag. Att kunna hantera en okänd situation leder till en lärdom av hur liknande situationer bör hanteras i framtiden (Bernstein, 1998:1-5).

Liksom för människan gäller detta för företag och organisationer. I takt med förändringar såsom ökad globalisering och teknologisk utveckling har begrepp som riskhantering vuxit fram som en vital del av företags långsiktiga strategi. En av de mest minnesvärda händelser som illustrerar vikten av risk- och krishantering är terrorattacken mot World Trade Centre den 11 september 2001. Investmentbanken Morgan Stanley, vars kontor var beläget i ett av tornen, var kapabel att återuppta sin aktiehandel inom 48 timmar efter katastrofen (Swartz et al., 2003:66). Senast i raden av exempel kan nämnas det vulkanutbrott på Island som höll luftrummet är avstängt i 26 länder i Europa under flera dagars tid - någonting som orsakade kaos i åtskilliga tusentals människors liv och fick förödande konsekvenser för företags affärsverksamheter (Aberg & Holmberg 2010).

Båda händelserna exemplifierar att en del av ett företags riskhantering bör innehålla en strategi som anger kan fortgå när en kris inträffar. Det syftar dels till att minimera kostnaderna av störningen och dels till att minska den tid det tar för företaget att återställa verksamheten till den ursprungliga kapaciteten. Detta kallas för kontinuitetshantering, vilket är desamma som hantering av operativa risker. Det är även starkt kopplat till företagets varumärke. Ett företag som kan visa hur de säkerställer kontinuitet i sin kärnverksamhet kan därmed öka sitt värde. Myndigheter, kunder, leverantörer och aktieägare är några exempel på intressenter som gynnas av att veta i vilken utsträckning företaget effektivt kan hantera en störning (Cosserat & Rodda, 2009:2-3).

1.2 Problemdiskussion

I en rapport från 2005 fastslog Finansinspektionen att det fanns generella brister i kontinuitetshanteringen inom den svenska finanssektorn då kvalitén och omfattningen på företags kontinuitetsplaner varierade kraftigt. Dessutom visade rapporten att företagen saknade kapacitet till strukturerad omvärldsbevakning av operativa risker och att de hade en bristande förmåga att genomföra hotbildsanalys av dessa (Finansinspektionen, rapport 2005:3). Det visade sig tydligt under 2009 när finanssektorn drabbades hårt av den ekonomiska krisen. Trots att krisen huvudsakligen uppkom ur finansiella risker kan vi konstatera att det är viktigare än någonsin att dessa företag förbereder sig på kriser som kan påverka verksamheten. De utgör en så pass viktig samhällsfunktion som, satt ur spel, får förödande konsekvenser. Krisen orsakade överlag stora förluster för skattebetalare och aktieägare då åtskilliga företag försattes i konkurs. Finansbolagen tillhörde också de företag som tvingades genomföra några av de största nyemissionerna i näringslivet, för att öka kapitaltäckningsgraden och undvika en finansiell härdsmälta (Flood, L. 2009).

För att hjälpa företagen har Finansinspektionen upprättat ett vägledande dokument som är ett övergripande ramverk som sammanfattar de viktigaste delarna av kontinuitetsprocessen och kontinuitetsplanerna. Därtill finns det internationellt standarder inom kontinuitetshandling, vilka är riktlinjer snarare än regleringar. I Sverige gäller ansvarsprincipen vid krishandling, vilken i praktiken innebär att den som normalt har ansvaret för en viss funktion i samhället, även har detta ansvar vid en kris. För finansiella företag betyder detta att det bör finnas en beredskap att hantera kriser för att tillvarata företagets intressen och för att skydda sitt varumärke. Genom en god krisberedskap skyddas även kundernas och, i förlängningen, samhällets intressen. Det finns omkring ett hundratal finansiella företag som kan sägas ha direkt eller indirekt påverkan på det finansiella systemets stabilitet, samt direkt påverkan på marknadens och allmänhetens förtroende (Finansinspektionen, 2005). Vad det gäller företag i finansbranschen, ställer vi oss därför frågan;

- *Hur väl hanterar svenska finansiella företag operativa risker?*

För att förstå de bakomliggande orsakerna till varför företagen hanterar sina operativa risker på det sättet de gör, samt jämföra våra resultat med givna rekommendationer och riktlinjer kring området, ställer vi oss därtill frågorna;

- *Vilka faktorer driver deras kontinuitetshandlingsarbete?*
- *Är kontinuitetshandlingen tillräckligt för att möta Finansinspektionens rekommendationer och hur står sig detta mot internationell standard?*

1.3 Syfte

Studien syftar till att analysera hur väl svenska finansiella företag hanterar sina operativa risker, vilka faktorer som driver företagens kontinuitetshanteringsarbete och om detta görs på ett tillfredställande sätt, givet Finansinspektionens rekommendationer och i jämförelse med brittisk standard. Därmed ämnar undersökningen visa vilken kvalitetsnivå de finansiella företagen uppnår inom området och diskutera vilka faktorer som är avgörande.

Resultatet av undersökningen kan dels användas i jämförande syfte företag emellan och dels fungera som underlag för att identifiera förbättringsmöjligheter inom kontinuitetshantering. Detta är av intresse för företagens intressenter såväl som för samhället i stort. Genom studien som helhet hoppas vi även kunna bidra till en ökad förståelse för vikten av god kontinuitetshantering.

1.4 Definitioner

1.4.1 Vad är risk?

Sedan 2009 definierar International Organization for Standardization (ISO) en risk som "osäkerhetens effekt på målsättningar", en översättning av "the effect of uncertainty on objectives" (ISO 31000). Definitionen är övergripande i den meningen att den kan appliceras på alla former av risk, i alla typer av branscher, världen över. Den bidrar också till att vidga riskbegreppet genom att länka samman företagets risker med konsekvenserna för dess målsättning. På så sätt tydliggörs vilken värdeskapande och avgörande betydelse hanteringen av risker har för ett företag (*Broadleaf Capital International, 2010*).

1.4.2 Vad är "en störning" i verksamheten?

En störning i ett företags verksamhet är en plötslig händelse, som antingen är förutsedd som exempelvis en strejk eller oförutsedd som exempelvis ett strömavbrott. Händelsen orsakar en oplanerad, negativ avvikelse från företagets ursprungliga kapacitet och dess förväntade förmåga att leverera en vara eller tjänst i enlighet med företagets målsättning (BS25999-2:2007).

2. TEORETISKA BEGREPP

2.1 Riskhantering

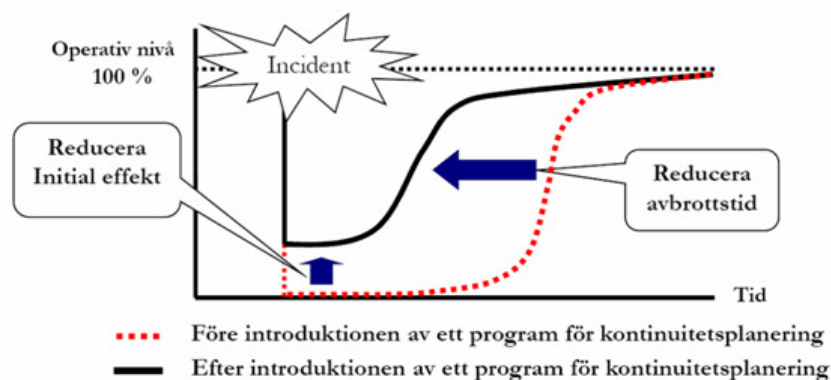
Riskhantering är ett vitt begrepp som innefattar hur alla former av risk hanteras i en organisation. Riskerna ett företag utsätts för är många till antalet, av varierande karaktär och svåra att förutse (Snedaker, 2007:135-137). Företagsrisker delas in i fem huvudsakliga kategorier. *Strategiska risker* är de risker som kan orsaka att de långsiktiga målen inte uppfylls eller att företaget misslyckas med sin affärsverksamhet. *Finansiella risker* är de risker som har att göra med företagets finansiella ställning och kontrollen av den. *Operativa risker* är de risker som uppkommer i den dagliga verksamheten, som rör kärnkompetensen, och kan orsakas bland annat av den mänskliga faktorn och de anställdas prestationer. *Kommersiella risker* är de risker som uppstår i kontakten med andra företag, myndigheter, massmedia och andra relationer företaget kan tänkas omges av. *Tekniska risker* är de risker som är associerade med att anläggningstillgångar och fysiska ting blir skadade eller upphör att fungera (Hiles & Barnes, 1999:31). Viktigt att poängtera är att dessa former av risker inte utesluter varandra. Just de operativa riskerna har speciell innebörd då operativa risker nästan alltid har teknisk eller strategisk karaktär. Denna sammanflätning är viktigt att vara medveten om när operativa risker diskuteras. Kort sagt, en operativ risk är i princip alltid samtidigt en teknisk eller en strategisk risk, samt kan även ha kommersiella inslag (Friberg 2010, muntl.).

Ett företag bör arbeta grundligt med riskhantering eftersom det ökar sannolikheten att det uppfyller sina långsiktiga mål samt skapar värde till sina ägare och kunder (Kallman & Maric, 2004:57). Värdeökningen kan ske av en rad anledningar. För det första minskar det risken att händelser som har en negativ påverkan på verksamheten äger rum. För det andra ökar det chansen att händelser som har en positiv påverkan på verksamheten tas till vara. Ett exempel på en sådan situation är tsunamin i Thailand 2004 då Fritidsresor vände katastrofen till något positivt för företaget (TT, 2006). En tredje orsak är att det identifierar möjligheter där ett risktagande faktiskt kan vara till nytta för verksamheten och borde genomföras. En uttalad riskhantering ökar även trovärdigheten, underlättar beslutsfattandet samt ökar transparensen och insynen i företaget. Vidare skapar det en ökad förståelse för lagar, regleringar och andra föreskrifter hos de anställda. Därtill kan det underlätta effektiviteten och legitimera genomförande av nödvändiga organisatoriska förändringar. Sist men inte minst är fokus på riskhantering ett tecken på ett proaktivt sätt från ledningens sida att driva företagets utveckling framåt (BS31100, 2010).

2.2 Kontinuitetshantering

Kontinuitetshantering är en del av ett företags riskhantering och ger ett ramverk för att bygga organisatorisk motståndskraft mot risker. Till skillnad från riskhantering, fokuserar kontinuitetshanteringen endast på de operativa riskerna som är associerade med kriser eller störningar i verksamheten. Därmed har den en annan utgångspunkt än den generella riskhanteringen. *Först* identifieras de kritiska aktiviteterna för den operativa verksamheten, *därefter* bestäms vilka risker som är kopplade till dessa och en kontinuitetsplan upprättas (BS25999-2, 2007).

Företag bör utarbeta en kontinuitetsplan för att säkerställa att inga tillgångar går förlorade vid en eventuell kris eller störning. Förmågan att skydda företagets intressenter, dess rykte, varumärke och värdeskapande aktiviteter står på spel. I slutändan handlar det förstås om företagets fortsatta lönsamhet (Hiles & Barnes, 2010:xiii). I praktiken är målet med en effektiv kontinuitetsplan att minimera tiden för återhämtning samt minimera kostnaderna av avbrottet i verksamheten, vilket illustreras av figur 2.1 nedan. Hur kontinuitetshanteringen ter sig i olika företag och hur planerna utformas, bestäms av vilka kritiska aktiviteter just det företaget har i sin kärnverksamhet. Dessa identifieras genom att svara på frågan; vilken del av verksamheten måste företaget alltid hålla igång, oavsett vad som inträffar (Friberg 2010, muntl.).



Figur 2.1 Effekten av kontinuitetshantering, kontra avsaknaden av densamma (4C Strategies, 2010).

3. TEORETISKT RAMVERK

3.1 Kontinuitetshanteringens mognadsgrad

Trots att företag i alla tider har varit tvungna att hantera sina risker är kontinuitetshantering ett relativt nytt begrepp inom näringslivet och det har kommit på tal som en strategiskt viktig fråga först de senaste tio åren. Av den anledningen kan det vara stor spridning bland företag och hur långt gångna de är i deras arbete med kontinuitetshantering - vilket kan benämnas som att olika företag har uppnått olika mognadsgrader på området. Ett företag som till fullo följer Finansinspektionens rekommendationer utifrån det vägledande dokument för kontinuitetshantering som finns, måste anses ha en hög grad av kontinuitetsmognad (Finansinspektionen, rapport 2005:3).

För finansiella bolag skiljer sig de operativa riskerna från marknads- och kreditrisker genom att de sällan medvetet tar på sig den förstnämnda typen av risker för att tjäna pengar. Typiska exempel på operativa risker för finansiella företag är risken för handhavandefel vid manuella moment, nyckelpersonberoende, risken för bedrägerier eller brott mot interna instruktioner, systemtillgänglighetsrisker och risken för rån (Finansinspektionen, 2006:18:5-8).

Förutom myndigheter i olika länder finns det organisationer som tillhandahåller standarder för kontinuitetshantering, såsom International Organization for Standardization (ISO) och British Standards Institute (BSI). Liksom Finansinspektionens vägledning är de dokument som finns internationellt endast rekommendationer. Dock kan den andra delen av den brittiska standarden BS25999 utgöra en slags checklista för företag i arbetet med kontinuitetshantering och det är den enda standard som företag kan certifieras emot i dagsläget. Därför är det den standarden som internationellt sett anses vara "best practice" och ett företag som uppfyller certifieringen har en hög mognadsgrad i sin kontinuitetshantering (Friberg 2010, muntl.).

Ett sätt att undersöka hur väl ett företag hanterar operativa risker är genom en så kallad mognadsmodell. År 2003 lanserades Business Continuity Maturity Model (BCM-modellen) av det amerikanska företaget Virtual Corporation då en av deras kunder var i behov av verktyg som kunde jämföra deras kontinuitetshantering med konkurrerande företag. BCM-modellen illustrerar hur utvecklad kontinuitetshantering är genom att placera företag i sex olika nivåer. Den första nivån innebär att kontinuitetshantering ännu inte identifierats som en strategisk fråga av ledningen och den sista nivån innebär att samtliga affärsenheter inom

företaget håller en hög nivå av kontinuitetskompetens (*Virtual Corporation*, 2010). Det är med denna modell vi väljer att undersöka hur väl svenska finansiella företag hanterar sina operativa risker, vilket vi kommer att beskriva mer ingående under metodavsnittet. Vilken mognad ett företag uppnår påverkas av vilka faktorer som driver kontinuitets-hanteringsarbetet. Det beror på hur ledningen ser på kontinuitetshantering, hur den implementeras, om de anställda är medvetna om kontinuitetsarbetet, om övningar genomförs, om tillräckliga resurser är allokerade till kontinuitetsarbetet, till vilken grad företaget mäter prestation samt i vilken utsträckning företaget har externa samarbeten eller förbindelser vad det gäller kontinuitetshanteringen. BCM-modellen är därför konstruerad utifrån olika kontinuitetskompetenser; ledarskap och implementering, anställdas medvetenhet och övning, resursfördelning och mätning samt externa förbindelser.

3.2 Ledarskap och implementering

3.2.1 Finansinspektionens rekommendationer

Finansinspektionen anger att det är den yttersta ledningen som har ansvar för att företaget uppfyller verksamhetsmålen och därmed även ansvarar för att det finns en acceptabel kris-hanteringsförmåga i organisationen (Finansinspektionen, 2005:03:7). Därför bör finans-bolagens styrelser fastställa företagets definition av operativa risker och en kategorisering av dess konkreta toleransnivåer. Ett dokument bör finnas som anger roller och ansvar för styrelse, riskkontrollenhet, affärsområdeschefer, processägare och andra befattningshavare som är inblandade i hanteringen av operativa risker. Styrelsen bör också bestämma vilka verktyg som ska användas för identifiering och värdering av operativa risker och hur rapporteringen ska ske, inklusive krav på innehåll i rapporterna (Finansinspektionen, 2006:18:5-8).

Kontinuitetsarbetet bör beskrivas i en övergripande säkerhetspolicy eller i särskilda riktlinjer eller instruktioner. Finansinspektionen menar dock att hur finansbolagen väljer att dokumentera ambitionerna i kontinuitetsarbetet inte är av överordnad betydelse - huvudsaken är att dokumentet är fastställt av ledningen och att det kommuniceras i hela organisationen. Dokumentet bör åtminstone innehålla accepterade avbrottstider, uthållighet, befogenheter och ansvar (Finansinspektionen, 2005:03:8).

3.2.2 Riktlinjer enligt BS25999

Den brittiska standarden BS25999 anger också att ledningen i företaget ansvarar för att en kontinuitetspolicy utformas. Policyn ska innehålla organisationens målsättningar med kontinuitetshanteringen och dess omfattning med avgränsningar och begränsningar. Med jämna mellanrum och när signifikanta ändringar inträffar, ska policyn revideras och uppdateras. Policyn ska definiera kontinuitetshanteringens omfattning, fastställa dess målsättningar och kommuniceras till samtliga anställda. Den ska bland annat innehålla lagstadgade, reglerande och avtalsenliga förpliktelser samt även organisationens huvudintresser (BS25999-2, 2007:9-10).

Vidare anger BS25999 att företaget bör ha dokumenterade kontinuitetsplaner som beskriver hur organisationen hanterar en störning och hur den återhämtar verksamheten till en förbestämd nivå. Varje plan ska ha ett definierat syfte och omfattning, en person ska vara ansvarig för dess utvärdering, uppdatering och genomförande (BS25999-2, 2007:15). Omfattningen på organisationens kontinuitetshantering ska utgå från kritiska funktioner och processer som tillhör kärnkompetenser. De aktiviteter i företaget som anses vara kritiska ska vara samkörda med påverkansanalyser som påvisar nyttan med att inkludera dessa aktiviteter i kontinuitetshanteringen (BS25999-1, 2006:11).

Att kunna hantera förändringar för att säkerställa det fortlöpande arbetet är vitalt för organisationen. Överförandet av kunskap vid personalomsättning hamnar därför under kontinuitetshantering, inte minst är detta viktigt för ledningen. BS25999 anger att organisationen bör ha en successionsplan för ledningar och VD:ar som minimerar kunskapsförluster vid överlämningar av poster i höga positioner (BS25999-1, 2006:15).

3.3 Anställdas medvetenhet och övning

3.3.1 Finansinspektionens rekommendationer

Finansinspektionen anger att många företag i den finansiella sektorn har säkerhetschefer eller en motsvarande roll, som ansvarar för säkerhetsarbetet och kontinuitetsplaneringen. Denne bör bidra med kunskap om risker och deras konsekvenser samt vilken typ av skyddsåtgärder som är lämpliga att införa. En säkerhetschef är dock inte alltid insatt i verksamhetens alla delar. Därför bör det finnas personer från andra avdelningar som även kan verka som verksamhetens ambassadörer i kontinuitetsfrågor med uppdrag att höja medvetenheten hos sina

medarbetare (Finansinspektionen, 2005:03:8). Sådana ambassadörer anger även BS25999 att det bör finnas i företaget (BS25999-2, 2007:10).

Alla delar av företaget kan drabbas av kriser i olika former, vilket måste medvetandegöras inom hela organisationen. Enligt Finansinspektionen är den enda vägen till denna medvetenhet, förutom genom verklig krishantering, utbildning och övning av all personal. Målet är att alla ska veta vad de ska göra om den egna verksamheten drabbas. Övningar och mätning bidrar till att identifiera förbättringsåtgärder som bör vidtas för att ytterligare höja företagets krishanteringsförmåga. Förbättringsåtgärder kan omfatta allt från uppdatering av larmlistor till att göra investeringar i teknisk utrustning (Finansinspektionen, 2005:03:13).

3.3.2 Riktlinjer enligt BS25999

Standarden BS25999 anger också att företaget bör genomföra övningsaktiviteter för att försäkra sig om att planerna uppfyller verksamhetens krav på kontinuitet. De ska genomföras regelbundet, utvärderas efter målsättning och ske särskilt när signifikanta förändringar har ägt rum. Övningarna i sig får inte medföra någon risk för deltagarna (BS25999-2, 2007:11).

Enligt BS25999 bör kontinuitetshantering finnas oavsett ett företags storlek - det bör vara en del av kärnvärderingarna och kulturen. Medvetenhet kring kontinuitetshantering förstärks och underhålls genom utbildning och övning, där färdigheter och erfarenhet skall dokumenteras skriftligt (BS25999-2, 2007:11).

3.4 Resursfördelning och mätning

3.4.1 Finansinspektionens rekommendationer

Finansinspektionens rekommendationer avser såväl den centrala verksamheten som mer lokal verksamhet på exempelvis ett regionkontor. En rapport som ger företagsledningen en överblick av alla operativa risker, inklusive säkerhetsrelaterade risker och risker med ”compliance”, från företagets olika enheter bör sammanställas med jämna mellanrum. Detta ger ledningen en samlad bild av företagets riskexponering (Finansinspektionen, 2006:18:13-16).

Risk- och sårbarhetsanalyser ska tydliggöra vilka risker organisationen är utsatt för. Dessa analyser bör sedan kombineras med en sannolikhetsbedömning för att kunna bedöma vilka

investeringar som är rimliga i förhållande till vilken skada för verksamheten som hoten och riskerna kan leda till (Finansinspektionen, 2005:03:9).

Enligt Finansinspektionen är de operativa riskerna generellt högre i en investmentbank än i annan finansiell verksamhet, vilket gör att dessa företag och storbanker oftare använder sig av så kallade riskindikatorer för mätning. En riskindikator i detta avseende är ett nyckeltal som mäter en operativ funktion i verksamheten och vars utveckling följs över tiden. Det kan exempelvis röra sig om att mäta andelen transaktioner som har makuleras (Finansinspektionen, 2006:18:5-8).

Finansinspektionen anger att det bör finnas en ansvarsdelning mellan styrelse, riskkontrollenheten och berörda befattningshavare. Detta eftersom operativa risker måste identifieras och bedömas av personer med god kunskap om de berörda processerna (Finansinspektionen, 2006:18:13-15).

3.4.2 Riktlinjer enligt BS25999

BS25999 anger att det är viktigt att företagsledningen tillhandahåller nödvändiga resurser för att etablera och underhålla kontinuitetsarbetet. Störningar kan bland annat mätas genom en påverkansanalys där genomslaget mot företagets nyckelprodukter eller nyckeltjänster bedöms (BS25999-2, 2007:10). Företagets kontinuitetsarbete bör mätas både genom intern utvärdering och genom revision från ett oberoende bolag. Liksom Finansinspektionen föreslår, anger den brittiska standarden att ledningen bör informeras om status på risk- och sårbarhetsanalyserna, förebyggande åtgärder, utvärdering av övning och faktiska störningar samt förslag till förbättring i kontinuitetshanteringsarbetet (BS25999-2, 2007:17).

BS25999 anger att en organisations policy ska innehålla målsättningar med sitt kontinuitetsarbete. Policyn ska tillhandahålla principer som organisationen ska sträva att uppfylla och använda som måttstock för att kunna uppnå målsättningarna. För att underlätta för organisationen att uppnå målsättningarna bör de principer som policyn innehåller byggas upp av referenspunkter som utgår från standarder eller regelverk (BS25999-1, 2006:11).

BS25999 anger att för varje kritisk affärsprocess eller -funktion som organisationen anser måste fortgå även vid händelse av en störning, bör det finnas krav på accepterad tid för återhämtning samt krav på accepterad nivå så kallade återställningspunkter. Dessa accepterade

krav skall utarbetas så att de hamnar under de åtaganden som organisationen gjort mot intressenter såsom kunder, leverantörer och myndigheter. (BS25999-1, 2006:17).

BS25999 anger att organisationen bör tillsätta representanter från olika enheter och funktioner att understödja arbetet med kontinuitetshandlingen. I mindre bolag är det dock mer vanligt att en person täcker in fler områden. Representanternas ansvar bör förstärkas genom att inkludera arbetsuppgifterna i organisationens kompensationsprogram (BS25999-1, 2006:14)

Utvärderingar bör genomföras för att säkerställa kontinuitetshandlingens lämplighet och effektivitet vad det gäller organisationens målsättningar. Utvärderingen ska utformas så att den kan upptäcka behovet av förändringar vad gäller rådande policys och "best practices" utifrån analyser och mätresultat från övningar och verkliga störningar (BS25999-1, 2006:38).

3.5 Externa förbindelser

3.5.1 Finansinspektionens rekommendationer

Verksamhetens kritiska processer är starkt beroende av interna resurser men även externa resurser krävs för att verksamheten ska fungera. Krisberedskap hos leverantörer och andra samarbetspartners har också stor betydelse. I värsta fall kan det egna företaget bli det enda som fungerar vid en större kris, men ändå inte förmå bedriva sin verksamhet på grund av de andra parternas bristande kontinuitetshandling. Organisationen och dess samarbetspartner bör därför synkronisera de delar av kontinuitetsplanerna som berör bägge parter. Genom exempelvis kravställning i avtal kan finansbolagen dessutom skapa större förutsättningar för att matcha den egna skyddsnivån mot omvärlden (Finansinspektionen, 2006:18:11-12).

3.5.2 Riktlinjer enligt BS25999

Krav på ett samarbete med exempelvis leverantörer eller andra externa förbindelser är någonting som knappt nämns i den brittiska standarden BS25999. Den anger att ett företag bör definiera och kommunicera målsättningen med sin kontinuitetshandling med hänsyn till företagets intressenter samt myndigheter och regelverk, dock förekommer inga krav på samarbeten i själva utformandet av kontinuitetsplanerna (BS25999-2, 2007:9).

3.6 Spelar kontinuitetshantering verkligen någon roll?

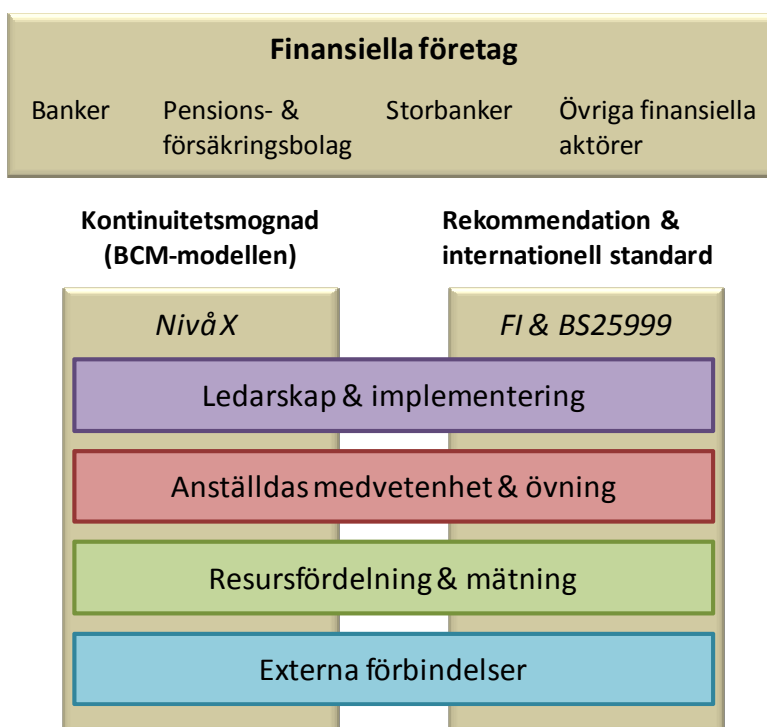
En grundläggande svårighet med riskhantering och följaktligen också kontinuitetshantering är att definiera begreppet *risk*. Hur ett företag väljer att definiera risker styr även arbetet med att hantera dessa. I litteraturen, den akademiska världen eller i näringslivet finns idag inte en entydig och allmänt vedertagen definition av vad en risk egentligen innebär. Risk kan exempelvis ses som någonting enbart negativ eller som både ett hot och en möjlighet. Detta skapar svårigheter i implementeringen av risk- och kontinuitetsarbetet hos de anställda och som en prioritering hos företagsledningen. Begreppet *risk* är helt enkelt svårt att kommunicera kring (Hansson, 2005:7-9). Riskbegreppet såsom det är definierat av ISO (se avsnitt 1.4.1) är tänkt att råda bot på denna problematik.

Osäkerhetsfaktorn inom kontinuitetshanteringen är generellt högre än inom den övergripande riskhanteringen i företaget. Det är därmed troligt att en störning inte kommer att inträffa exakt så som kontinuitetsplanerna har förutsett. Detta är naturligtvis problematiskt vilket ofta gör att kritiker ställer sig frågan om kontinuitetshantering verkligen spelar någon roll? Svaret blir att kontinuitetshantering skapar en medvetenhet genom planeringsprocessen och ett handlingsutrymme som kan vara svårt att uppnå annat än genom ett verkligt krisscenario. Verkligt krisscenario, det vill säga när en kris faktiskt inträffar, är något ett företag gör allt för att undvika. Kontinuitetsplanering bygger således på den grundtanke som den amerikanska presidenten Eisenhower förde fram i ett tal under en militär konferens år 1957; "*Plans are worthless, but planning is everything.*" (Finansinspektionen, rapport 2005:3).

3.7 Sammanfattning; analysmodell

Finansinspektionens rekommendationer kommer att utgöra grunden för analys vad det gäller att studera hur väl svenska finansiella företag hanterar sina operativa risker, och vi kommer även att nämna hur det står sig mot den brittiska standarden BS25999. Vi kommer att studera svenska finansiella företag som grupp men också urskilja dem baserat på företagstyper; banker, pensions- och försäkringsbolag, storbanker och övriga finansiella aktörer. Då riskhantering är ett vitt begrepp som innefattar alla former av risk, kommer vi att fokusera på kontinuitetshantering eftersom detta behandlar de operativa riskerna av en störning. Kontinuitetshantering ser till företagets kritiska aktiviteter vilka en kontinuitetsplan upprättas utifrån, vars mål är att minimera tiden för återhämtning samt minimera kostnaderna av ett avbrott i kärnverksamheten. Det kan vara stor spridning bland företag vad det gäller utvecklingen av kontinuitetshanteringsarbetet - vilket kan klassificeras in i olika mognads-

grader. En mognadsmodell kan användas för att undersöka i vilken utsträckning kontinuitets-
hantering förekommer och således vilken kvalitetsnivå ett företag har inom området. Vi
kommer att mäta detta hos svenska finansiella företag med hjälp av BCM-modellen, lanserad
av konsultföretaget Virtual Corporation. För att undersöka vilka faktorer som driver
kontinuitetshanteringsarbetet kommer det empiriska materialet och analysen att utgå från
BCM-modellens kontinuitetskompetenser; ledarskap och implementering, anställdas med-
vetenhet och övning, resursfördelning och mätning samt externa förbindelser. Detta illustreras
genom figur 3.1 nedan.



Figur 3.1 Vår modell för att analysera mognadsnivån och drivande faktorer inom kontinuitetshantering för svenska finansiella företag

4. METOD

Att mäta mognad har ofta varit ett sätt för företag att mäta kvalitet och säkerställa en viss standard på verksamheten inom olika områden. Att tillämpa en standardiserad, och av industrin, vedertagen mognadsmodell är ett enkelt sätt att klassificera sitt företags arbetssätt då det klart och tydligt framgår hur man ligger till i relation till konkurrenter inom samma industri. Främst inom system- och mjukvaruutveckling har sådana mognadsmodeller förekommit då det är extremt viktigt att kunna påvisa kvalitet för intressenter som inte kan skilja bra system från dåliga. En mognadsmodell syftar till att klassificera företag i olika nivåer beroende på hur långt de har kommit i utvecklingen inom det området som mognadsmodellen avser att mäta.

Även kontinuitetshantering är svårt att utvärdera kvalitetsmässigt utan ett ramverk som likt modellerna inom mjukvaruutveckling mäter ett företags mognadsnivå på området. Av den anledningen utvecklande Virtual Corporation modellen Business Continuity Maturity Model (BCM-modellen) som placerar företag i sex olika nivåer för kontinuitetsmognad och lämpar sig som mätverktyg för att besvara vår första forskningsfråga, det vill säga hur väl svenska företag finansiella företag hanterar sina operativa risker.

För att därefter besvara vår andra och tredje forskningsfråga samt analysera de rekommendationer som Finansinspektionens och standarden BS25999 anger, delar vi in vårt teoretiska ramverk efter det BCM-modellen kallar företagskompetenser. Påståendena i vår undersökning hör ihop med var och en av kompetenserna, vilket beskrivs mer ingående i avsnitt 4.2.1.

4.1 Business Continuity Maturity Model

BCM-modellen kategoriserar ett företags mognadsgrad inom kontinuitetshantering i sex nivåer, vilka illustreras i figur 3.1. Den lodräta axeln visar nivåerna och den horisontella axeln visar vad som i huvudsak karakteriserar respektive nivå. Certifiering mot den brittiska standarden BS25999, vilket kräver att samtliga punkter i standarden uppfylls, implicerar att företagen befinner sig i mognadsnivå sex.

Competency Maturity Level	Program Basics			Program Development		
	Sr. Mgmt Commitment	Professional Support	Governance	All Units Participating	Integrated Planning	Cross-Functional
Level 1 Self-Governed	No	No	No	No	No	No
Level 2 Supported Self-Governed	Marginal	Partial	No	No	No	No
Level 3 Centrally Governed	Partial	Yes	Partial	No	No	No
Level 4 Enterprise Awakening	Yes	Yes	Yes	Yes	No	No
Level 5 Planned Growth	Yes	Yes	Yes	Yes	Yes	No
Level 6 Synergistic	Yes	Yes	Yes	Yes	Yes	Yes



 Increasing Business Continuity Competency Maturity

Figur 4.1 Mognadsnivåer i Business Continuity Maturity Model (Virtual Corporation, 2010)

Nivå 1 – Självstyre

Kontinuitetshantering har ännu inte identifierats som en strategisk fråga av ledningen (engelska: no Sr. Mgmt Commitment). Det finns ingen centralstyrd supportfunktion för kontinuitetshantering inom organisationen och även om organisationen har en kontinuitetspolicy upprätthålls den inte. Det är upp till varje enhet att utforma och implementera den egna kontinuiteten. Beredskapen inom organisationen är generellt låg (Virtual Corporation, 2010).

Nivå 2 - Stöttat självstyre

Minst en affärsenhet har identifierat kontinuitetshantering som strategiskt viktigt och påbörjat försök att öka medvetenheten hos ledningen och anställda. Åtminstone en rådgivare inom kontinuitetshantering finns tillgänglig att stödja enheternas arbete med kontinuitetsfrågor (engelska: partial Professional Support). Beredskapen är dock fortfarande låg. Ledningen väljer att inte prioritera kontinuitetshantering (Virtual Corporation, 2010).

Nivå 3 - Centralstyre

Flera affärsenheter har upprättat kontinuitetsplaner och håller en relativt god beredskap. En centralstyrd kontinuitetsavdelning finns, vilken stödjer de aktuella affärsenheterna (engelska: partial Governance). Intresset att utveckla det hittills genomförda arbetet till ett fullständigt kontinuitetsprogram för företaget som helhet ökar hos ledningen och ledningsgruppen har troligen tillsatt en utredning av dessa möjligheter (Virtual Corporation, 2010).

Nivå 4 - Upplysning

Ledningen är engagerad och förstår vikten av kontinuitetshantering som en del av företagets långsiktiga strategi. En central avdelning styr utformandet av planerna som har börjat standardiseras inom hela företaget (engelska: All Units Participating). Kritiska affärsprocesser

har identifierats, övningar genomförts och varje enhet har tilldelats egna kontinuitetsresurser. (*Virtual Corporation, 2010*).

Nivå 5 - Tillväxtsplan

Revidering av kontinuitetsplanerna har lett till förbättringar och en översiktsplan på flera år säkerställer att organisationens beredskap förbättras kontinuerligt (engelska: Integrated Planning). Övningar, som även ledningsgruppen deltar i, ser till att medvetenhet kring kontinuitetshantering upprätthålls. Kontinuitetsplaner och övningar spänner över flera avdelningars perspektiv kring kritiska affärsprocesser (*Virtual Corporation, 2010*).

Nivå 6 - Synergi

Samtliga affärsenheter håller en hög nivå av kontinuitetskompetens och tvärfunktionella koordinerade övningar leder till utveckling (engelska: Cross-Functional). Kontinuitetsplanerna har framgångsrikt integrerats och en nära koppling till organisationens övriga förändringsprocesser håller beredskapen på en hög nivå. Innovativa kontinuitetspolicys och "best practices" formas av pilotprojekt (*Virtual Corporation, 2010*).

4.2 Datainsamlingsmetod och operationalisering

Undersökning genomfördes med hjälp av en enkätundersökning, i form av en strukturerad intervju. En sådan intervju är informationsorienterad och innebär att såväl frågeformuleringen som ordningsföljden är bestämd på förhand (Lundahl & Skärvad, 1999). Vi valde att använda en kvantitativ datainsamlingsmetod som dock har inslag av en kvalitativ metod. Fördelar med en kvantitativ ansats är att den standardiserar informationen och därmed gör den lätt att bearbeta. Av den anledningen är det även lättare att låta fler respondenter medverka i undersökningen (Jacobsen, 2000:146). Undersökningen har dock ett kvalitativt inslag i den meningen att den är subjektiv, då resultaten grundar sig i respondentens uppfattning om eller uppskattade hur arbetet med kontinuitetshanteringen i respektive företag går till. Trots att mätetalet i sig är av kvantitativ karaktär innehåller svaren tolkningar från den enskilde uppgiftslämnaren.

Undersökningen består av ett webbaserat frågeformulär som mäter de olika företagens mognadsnivåer. Frågeformuläret skickades elektroniskt via e-post. I utskicket fanns även ett informationsbrev om syftet med uppsatsen, kontaktuppgifter till oss och vår handledare samt företagens rättigheter. E-posten, informationsbrevet och enkätformuläret finns sammanställda

i bilaga 1, 2 och 3. Enkäten skickades löpande vartefter företagen hade tackat ja att medverka via telefon. Svaren samlades in mellan den 23 april 2010 och den 5 maj 2010.

Undersökningen inkluderar totalt 17 företag inom den svenska finansiella sektorn. Med hänsyn till undersökningens krav på konfidentialitet kommer inget enskilt företag att benämnas med sitt riktiga namn. Istället delades företagen in i fyra olika kategorier baserat på deras verksamhetsområde. Av de 17 företagen som medverkade är fyra storbanker, fyra banker, fyra pensions- och försäkringsförvaltare och fem övriga finansiella aktörer. Den sistnämnda kategorin kan innehålla investmentbanker, fondkommissionärer eller statliga organ. Uppdelningen mellan storbanker och banker baseras på storbankernas dominerande roll då de sammanlagt innehar uppemot 80 procent av marknadsandelarna för kommersiella banker i Sverige. De andra bankerna utgörs av lokala sparbanker (Finansinspektionen, 2006:14:29). Då samtliga storbanker har medverkat i undersökningen, anser vi att en uppdelning därför är nödvändig för att resultaten inte ska bli missvisande.

Urvalet gjordes utifrån de 28 företag som deltog i Finansinspektionens övningar inom kontinuitetshantering under åren 2001 till 2004. Av dessa finns 26 företag kvar idag och vi kontaktade samtliga av dem. Vad det gäller fyra företag var rätt person inte anträffbar under tiden för datainsamlingen. Enkäten skickades således till totalt 22 säkerhetschefer eller personer med relevant befattning på respektive företag - i slutändan valde 17 att delta i vår undersökning. Vi valde att undersöka dessa företag eftersom det ger en spridning inom finansbranschen som tillsammans täcker in stora kundgrupper och intressenter. Vidare är de av varierande storlek och har varit etablerade på marknaden under olika lång tid. Enligt den allmänna definitionen består finanssektorn av de företag som dels tillhandahåller grundfunktionerna i det finansiella systemet men också uteslutande arbetar med finansiella tjänster. Det är också denna kärna av företag som speglas i den officiella statistiken och består av banker, försäkringsbolag, börs- och värdepappersbolag samt betalningssystem (Finansplats Stockholm, 2010). De 17 företagen i undersökningen speglar dessa företagstyper mycket väl och innefattar samtliga fyra storbanker, några av de största försäkringsbolagen samt andra stora aktörer på marknaden. Vi menar därför att de kan sägas vara representativa för finansbranschen som helhet. En annan orsak till detta urval är att Finansinspektionens rapporter från 2005 och 2006 bygger på de övningar, avsedda att mäta kontinuitetshanteringen, gjorda tidigare år med just dessa företag - det föll sig därmed naturligt att även vår undersökning gör det.

4.2.1 Studiens giltighet och trovärdighet

Eftersom det är viktigt att undersökningen verkligen mäter det den avser att mäta (Eliasson, A. 2006:15), har vi använt oss av den mall för påståenden som finns i BCM-modellen. Mognadsnivåerna innehåller ett antal specificerade krav som företaget ska uppfylla, där varje krav motsvarar ett påstående. Respondenterna ombeddes svara hur väl påståendet stämmer in på deras företag, genom att ange ett värde på skalan 0-100%. Varje påstående var kopplad till en av de olika kontinuitetskompetenserna, dock är påståendena av sådan karaktär att de kan mäta fler än en faktor. 10 påstående kategoriseras under ledarskap och implementering (1,5,9,13,15,18,24,26,28,29), 8 påståenden under anställdas medvetenhet och övning (2,3,4,8,10,16,21,22), 7 påståenden under resursfördelning och mätning (6,11,12,17,19,20,27) och 5 påståenden under externa förbindelser (7,14,23,25,30).

Då modellen innehåller 63 påståenden, ansåg vi att en avvägning måste göras mellan antal påståenden och sannolikheten att företagen är villiga att besvara dessa. Ovanstående påståenden är ett urval som gjorts i samförstånd med vår handledare och genom jämförelse med innehållet i Finansinspektionens rekommendationer och standarden BS25999. Det är en till synes ojämn fördelning mellan påståendena där 10 påståenden går under ledarskap och implementering medan endast 5 påståenden behandlar externa förbindelser. Vårt urval representerar dock den inbördes fördelning som finns mellan de ursprungliga 63 påståendena och för att ingen faktor skulle väga tyngre än den andra valde vi att räkna ut ett snitt baserat på antalet påståenden i varje faktor. Således ger fler påståenden endast ett mer rättvisande svar utan att för den sakens skull väga mer i vår undersökning. Påståendena har inte omarbetats på annat sätt än att de har översatts från engelska till svenska.

Undersökningens trovärdighet bestäms av hur den utförs samt hur väl det empiriska materialet bearbetas (Eliasson, A. 2006:15). Till vår hjälp användes Google Formulär och svaren kopplades direkt till ett excelark där trender och diagram skapades. Varje företag uppnådde en viss mognadsnivå. Därefter beräknades den sammanlagda mognadsnivån för gruppen företag genom att procenttalen lades ihop och dividerades med 100. Resultatet blev ett vägt genomsnitt av den sammanlagda överensstämmelsen av det givna påståendet, och en form av "branschsnitt", se bilaga 4 för ett beräkningsexempel.

4.3 Metodproblematik

4.3.1 Kvantitativ metod

Det finns en rad anledningar till varför en kvantitativ undersökningsmetod kan ifrågasättas. Kanske den främsta invändningen är att undersökaren i förväg definierar vad som är relevant att besvara, vilket skapar en mindre flexibel studie (Jacobsen, 1999:147). Den kvantitativa datainsamlingsmetoden vi valde genom BCM-modellen grundar sig på det teoretiska ramverket, då den är ett verktyg för att undersöka hur ingående företag arbetar med kontinuitetshantering. Därigenom anser vi att denna metod lämpar sig för uppsatsens syfte. Då mognadsmodellen därtill innehåller ett tillvägagångssätt för att mäta mognadsgraden fann vi ingen anledning att frånga det. Faktum är att det för vår del finns en poäng med att på förhand ha definierat vad som är relevant att besvara. Eftersom rekommendationer och standarder finns för hur företag borde arbeta med kontinuitetshantering och vår studie går ut på att undersöka hur detta efterföljs, bör dessa dokument också avgöra vad som är relevant i förväg.

Vi ser att det kan finnas ett problem med att undersökningen baserades på respondenternas subjektiva tolkningar och självskattning. Detta kan ge upphov till förvridda svarsvärden om respondenten exempelvis svarar med ett högre värde än vad företaget faktiskt har, då det framställer både företaget och det egna ansvarsområdet i en bättre dager. Denna problematik tror vi avhjälps mycket genom att undersökningen är helt konfidentiell.

4.3.2 Att använda en "konsultmodell" för datainsamling

Invändningar kan förekomma mot att använda en konsultmodell i en akademisk studie. Det kan ha att göra med det faktum att ett konsultföretag ofta utvecklar en modell i akt och mening att sälja den till kunder, där problemet som lyfts fram faktiskt måste gå att lösa genom modellen. I och med detta finns en risk att generella akademiska problem och teoretiska begrepp översätts av konsultbolaget för att passa deras ekonomiska intressen. Dock finns en rad exempel i den akademiska världen som visar på användningen av vad som från början bör betraktas som en konsultmodell, exempelvis de välkända modellerna Five Forces av Porter och Balanced Score Card av Kaplan och Norton (Drogendijk 2010, muntl.). Vidare stämmer BCM-modellens användningssyfte väl överens med syftet för vår uppsats och modellen visade sig vara mycket lämplig att använda som mått för att besvara vår huvudfråga då den specifikt är utformad att mäta företags mognadsnivå gällande deras kontinuitetshantering.

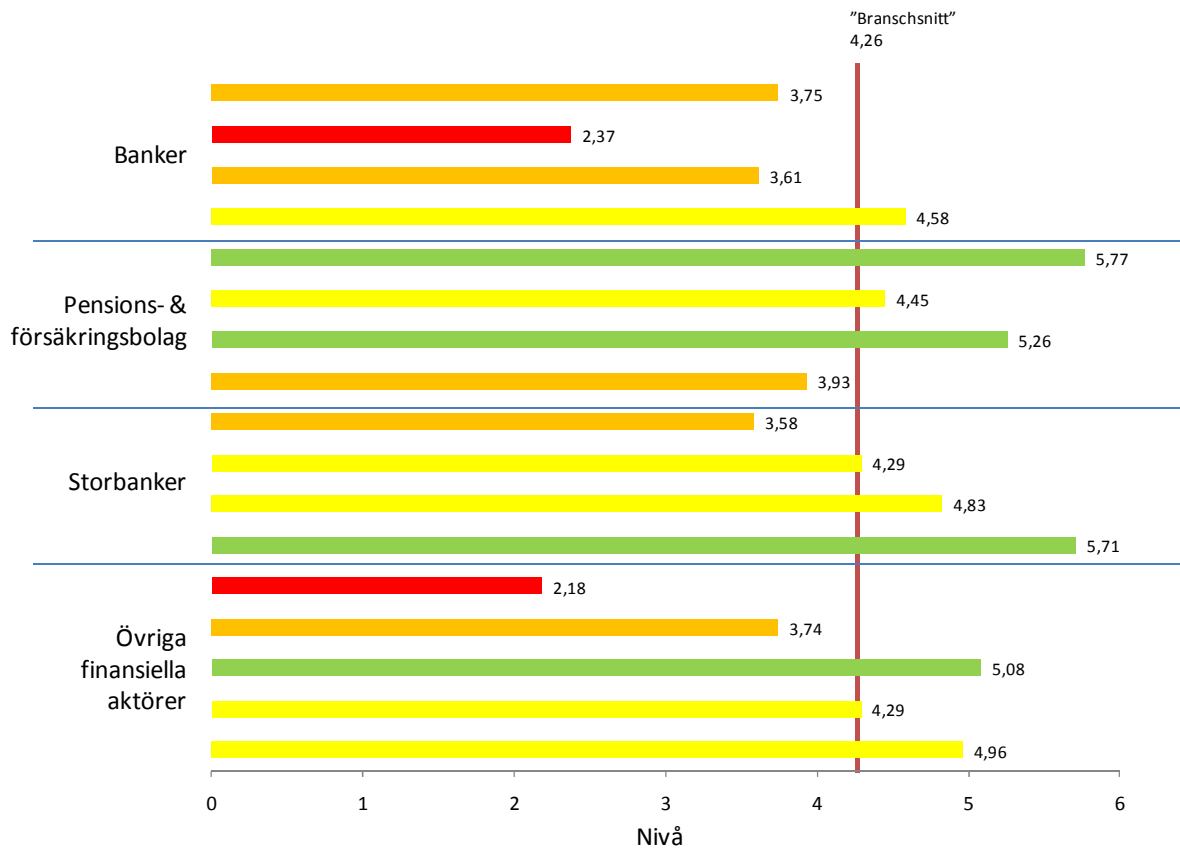
4.3.3 Urval av företag

Att använda sig av de medverkande företagen i finansinspektionens övningsverksamhet har både sina för- och nackdelar. Vi sätter stor tilltro till att Finansinspektionen då gjorde ett så representativt urval som möjligt eftersom rapportens slutsatser generaliseras till att gälla hela finansbranschen. Att det i vår undersökning saknas 11 företag från de ursprungliga 28 ser vi inte som ett problem då ingen företagskategori blev underrepresenterad till följd av bortfallet. Dock är vi medvetna om att företagen som deltog i Finansinspektionens kontinuitetsövningar därefter kan ha förbättrat sitt kontinuitetsarbete och ökat medvetenheten kring riskhantering. Vi menar ändå att urvalet är representativt för finanssektorn idag, då majoriteten av företagen i undersökningen tillhör de största aktörerna på marknaden, eller är de enda i sitt slag.

5. EMPIRISK ANALYS

5.1 Mognadsnivå inom kontinuitetshantering

Efter en resultatsammanställning av de 17 finansiella företag som deltog i undersökningen visar det sig att de sammanlagt har en kontinuitetsmognad av nivå fyra. Det exakta "branschsnittet" för företagen är 4,26. Det innebär att de finansiella företagen som grupp hanterar sina operativa risker genom att hålla en medelhög beredskapsnivå vad det gäller störningar eller kriser i kärnverksamheten. Enligt Business Continuity Maturity Model kallas denna mognadsnivå *Upplysning*. Generellt betyder det enligt modellen att ledningen är engagerad och förstår vikten av kontinuitetshantering som en del av företagets långsiktiga strategi och en central avdelningen styr utformandet av planerna som har börjat standardiseras inom hela företaget. Kritiska affärsprocesser har identifierats, övningar genomförs och varje enhet har tilldelats egna kontinuitetsresurser. Figur 5.1 på nästa sida illustrerar samtliga företag i undersökningen. Vid en första anblick kan detta tolkas som en övergripande godkänd kvalitetsnivå givet Finansinspektionens rekommendationer och standarden BS25999 men på grund av den stora spridningen bland företagen anser vi att så inte är fallet. Förbättringar krävs i synnerhet för de företag som hamnar i nivå två och tre.



Figur 5.1 Samtliga respondenters mognadsnivå

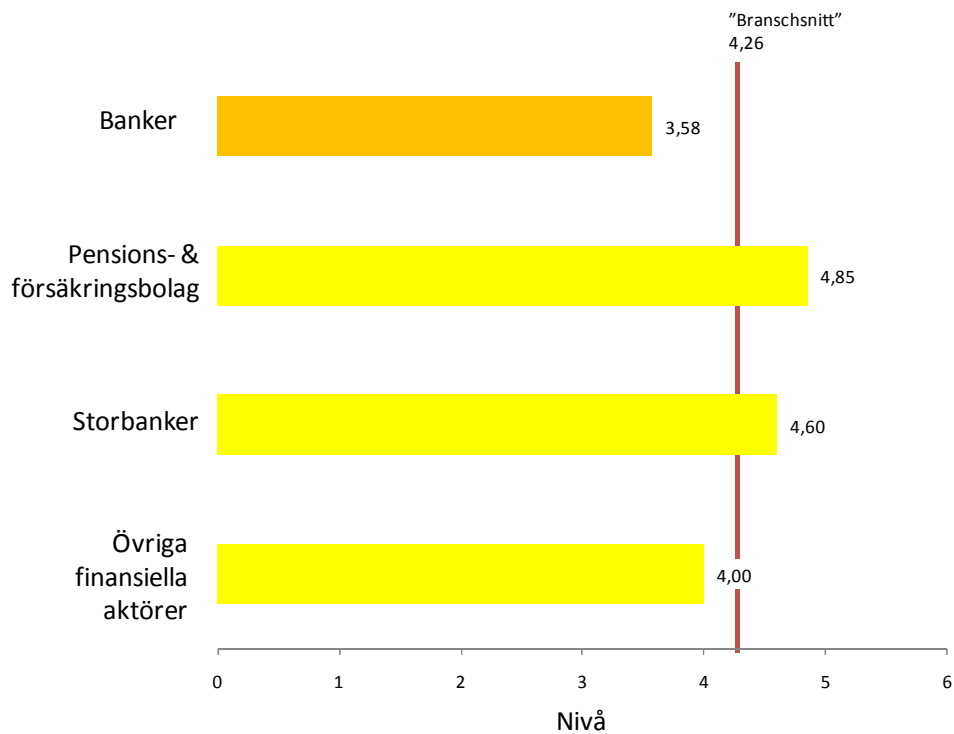
Vad det gäller detta urval av företag står det klart att Finansinspektionens slutsats kan bekräftas - det är fortfarande stor spridning vad det gäller kontinuitetshanteringen för finansiella företag. Inte heller kan en typ av företag sägas vara bättre än någon annan, då kontinuitetsmognaden är spridd även inom de fyra olika företagstyperna. **Den största spridningen ses inom gruppen övriga finansiella aktörer som har en variation mellan 2,18 och 5,08.** Detta resultat är dock inte förvånande då det inom denna grupp finns företag av olika karaktär. Det kan exempelvis vara fondbolag, investmentbanker, värdepapperscentral eller börs. **Mot bakgrund av att Finansinspektionen anger att de operativa riskerna generellt sett är högre i investmentbanker och storbanks borde det föränta en högre grad av kontinuitetsmognad.** Det bekräftades inte av studien. En av storbanks har endast en mognadsgrad av 3,58 vilket är under branschnittet. **En investmentbank och en annan storbanks har en mognad av 4,29 vilket är precis omkring genomsnittet.** Vi anser att detta är anmärkningsvärda låga resultat. Dessa företag borde driva upp snittet, snarare än att prestera under eller precis

omkring genomsnittet. Med tanke på deras storlek och betydelse för det svenska finansiella systemet menar vi att de måste förbättra sitt kontinuitetshanteringsarbete.

Totalt sett är det fyra företag som uppnår nivå fem för kontinuitetsmognad. Det innebär bland annat att revidering av kontinuitetsplaner görs kontinuerligt, att det finns en medvetenhet kring kontinuitetshantering som säkerställer att arbetet upprätthålls samt att planer och övningar inkluderar flera avdelningars perspektiv kring kritiska affärsprocesser. De allra flesta rekommendationer från Finansinspektioner efterföljs i ett företag som uppnår nivå fem i kontinuitetsmognad. Det högsta värdet i undersökningen är 5,77 vilket uppnås av ett försäkringsbolag. Detta företag angav att 25 av totalt 30 påståenden "stämmer helt överens" (100%) med deras kontinuitetsarbete.

Två av företagen i undersökning hamnar endast i nivå 2, där det sämsta resultatet är ett företag av typen övriga finansiella aktörer med en mognadsgrad på 2,18. Nivå 2 innebär bland annat att beredskapen för närvarande är låg inom organisationen och engagemanget är måttlig hos de anställda. Det finns exempelvis inte etablerade krav för återhämtningstider av kritiska funktioner vid en kris och det förekommer inte övningar för att öka anställdas medvetenhet inom kontinuitetshantering, vilket kan tolkas som att väldigt få riktlinjer från Finansinspektionen eller BS25999 efterföljs. Företaget med den lägsta mognadsgraden meddelade under "övrigt att tillägga" att de precis har inrättat en tjänst för kontinuitetshantering som är i uppstartsfasen, vilket kan förklara den i dagsläget låga kontinuitetsmognaden. Vi menar dock att det är anmärkningsvärt att de inte har kommit längre i kontinuitetshanteringsarbetet eftersom de redan under åren 2005 och 2006 deltog i Finansinspektionens övningar på området. Att ett finansiellt företag idag då inte uppnår mer än 2,18 i mognadsgrad är helt klart underkänt enligt vår bedömning.

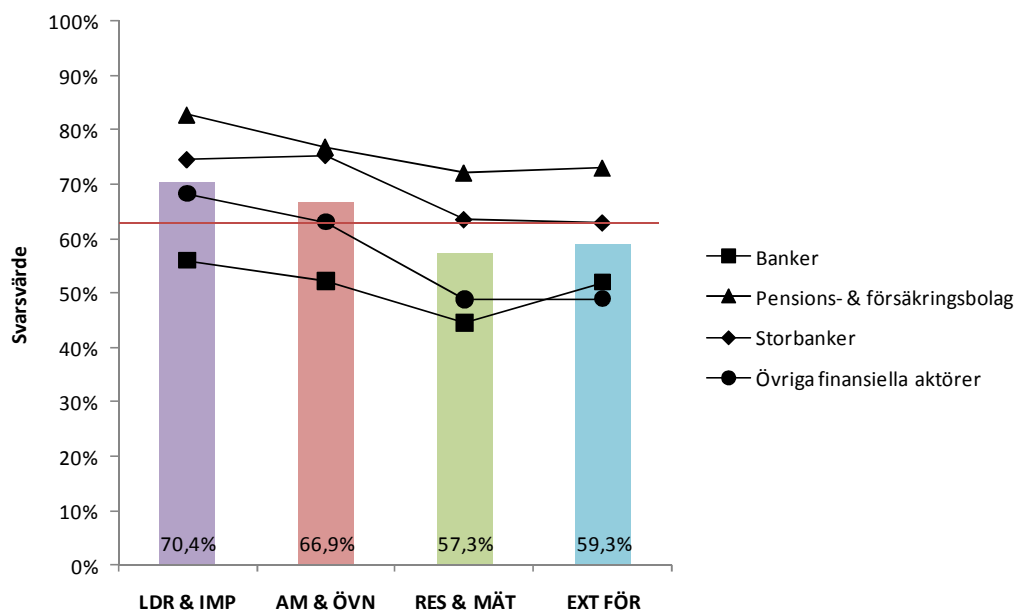
Av de fyra olika företagstyper som studien baseras på är det pensions- och försäkringsbolag som i snitt uppnår den högsta kontinuitetsmognaden på 4,85 och är den enda företagstyp som är i närheten av att uppnå nivå fem enligt BCM-modellen då två bolag gör just detta. Storbankerna och övriga finansiella aktörer har en mognadsgrad på 4,60 respektive 4,00. Den enda företagstyp som hamnar i den tredje nivån är banker med en kontinuitetsmognad om 3,58. Detta illustreras av diagrammet nedan som visar respektive företagstyp och dess mognadsnivå – "branschsnittet" 4,26 anges av det röda strecket.



Figur 5.2 Kontinuitetsmognad för svenska finansiella företag

5.2 Faktorer som påverkar mognadsnivån

För att bättre förstå varför de finansiella företagen i undersökningen sammanlagt uppnår en mognadsnivå fyra och undersöka vad som driver kontinuitetshanteringsarbetet har vi närmare studerat hur svaren ser ut inom faktorerna ledarskap och implementering (LDR & IMP), anställdas medvetenhet och övning (AM & ÖVN), resursfördelning och mätning (RES & MÄT) samt externa förbindelser (EXT FÖR). För varje påstående angav företagen ett värde mellan 0-100%. Värdet 0% innebär att företaget inte alls uppfyller påståendet, 50% innebär att det uppfylls till hälften och 100% att företaget uppfyller påståendet helt. Figur 5.3 illustrerar detta. Staplarna visar det genomsnittliga svarsvärdet för varje kontinuitetskompetens och det röda strecket visar det genomsnittliga svaret för samtliga faktorer vilket är 63,5%. Vad är då ett bra svar? Främst beror detta i stor grad på vilket påstående som svarsvärdet avser. Vi har dock generellt följt uppfattningen att ett svarsvärde under 70% indikerar att förbättringar behöver genomföras, ett svarsvärde mellan 70% till 80% visar på en godkänd nivå av det påståendet behandlar och ett svarsvärde över 80% visar att företaget uppfyller påståendet bra. Som tidigare nämnt behandlar påståendena olika saker, varför avvikelser från ovanstående indelning förekommer.



Figur 5.3 De olika faktorerna och dess påverkan på mognadsnivån

Resultaten visar att företagen generellt sett uppfyller påståendena inom ledarskap och implementering bättre än inom resursfördelning och mätning. Detta tolkar vi som att de finansiella företagen har kommit längre vad det gäller att upprätta styrdokument och identifiera kritiska affärsprocesser än att faktiskt allokera resurser till exempelvis förbättringar av kontinuitetshanteringen. Detta är en trend som kan ses inom alla fyra företagstyper.

5.2.1 Ledarskap och implementering

Denna kontinuitetskompetens (LDR & IMP) har sammanlagt det högsta svarsvärdet med ett snitt på 70,4%. Detta betyder att de finansiella företagen till relativt hög grad uppfyller de påståenden som är kopplade till ledarskap och implementering och att det är mer drivande i kontinuitetshanteringsarbetet, jämfört med de andra tre faktorerna. Tabell 5.1 på nästa sida visar företagens genomsnittliga svarsvärde för respektive påstående och det sammanlagda snittet för varje företagstyp.

	P1	P5	P9	P13	P15	P18	P24	P26	P28	P29	Snitt:
Bank	82,5%	72,5%	40,0%	70,0%	57,5%	42,5%	55,0%	47,5%	47,5%	45,0%	56,0%
Pensions- & försäkringsbolag	92,5%	90,0%	85,0%	82,5%	92,5%	82,5%	95,0%	55,0%	70,0%	82,5%	82,8%
Storbank	92,5%	95,0%	80,0%	90,0%	100,0%	82,5%	42,5%	55,0%	52,5%	55,0%	74,5%
Övrig finansiell aktör	90,0%	91,7%	63,3%	65,0%	80,0%	65,0%	56,7%	33,3%	60,0%	78,3%	68,3%
Snitt:	89,4%	87,3%	67,1%	76,9%	82,5%	68,1%	62,3%	47,7%	57,5%	65,2%	70,4%

P1 Det finns mindre omfattande manual för åtgärder vid nödsituationer och kriser

P5 Det förekommer en eller flera planer inom områdena verksamhetsåterhämtning, teknisk återhämtning, säkerhetsföreskrifter och/eller olycksfall

P9 Det finns ett styrprogram för avdelningar (vilka är involverade i kontinuitetshantering) som upprätthåller, åtminstone i begränsad utsträckning, efterlevnad gentemot gemensamma policys, standarder och "best practices" av företagets kontinuitetshantering

P13 Det finns en prioritetsordning gällande återställning av varje kritisk affärsfunktion

P15 Det finns dokumenterat att företaget efterlever de rekommendationer och krav som myndigheter ställer gällande kontinuitetshantering

P18 Kontinuitetshantering är identifierat som en del av strategin, vilket visas genom att analyser av risk- och påverkansanalyser genomförs regelbundet

P24 Det finns en successionsplan för ledning och VD

P26 Kontinuitetshanterings processer bidrar till strategisk utveckling

P28 Det finns ett översiktligt kontinuitetsprogram som sträcker sig över en

P29 Det finns en specifik enhet inom kontinuitetshantering som samarbetar nära andra avdelnings- och enhetschefer

Tabell 5.1 Svarevärde per företagstyp inom ledarskap och implementering

Vi tolkar resultaten som att de finansiella företagen har en bra kortsiktig kontinuitetshantering baserat på ledarskap och implementering, vilket är en av anledningarna till att de uppnår en mognadsnivå fyra i BCM-modellen. Samtliga företagstyper anger att det finns en manual för åtgärder vid nödsituationer och kriser, då det påståendet uppfylls till 89,4%. Finansinspektionen anger att ett sådant dokument bör finnas och de starka svarsfrekvenserna visar på att de finansiella företagen har det. Det visar sig också finnas särskilda planer för återhämtning av verksamheten och informationssystem samt säkerhetsföreskrifter då företagen i snitt uppfyller detta nästan lika väl, med 87,3%. De särskilda planerna är en mer avancerad nivå än endast en manual - de har formen av riktiga kontinuitetsplaner. För att bli certifierad mot BS25999 måste dessa planer innehålla ett definierat syfte vilket vi anser uppfylls av de finansiella företagen.

När det gäller ett styrprogram som kommunicerar kontinuitetspolicyn och kan användas för kontroll att den efterlevs, brister två av företagstyperna i undersökningen något. Bankerna hamnar klart sist på denna punkt med 40,0% och övriga finansiella aktörer efterlever kontinuitetspolicyn något bättre då påståendet uppfylls till 63,3%. Storbankerna och pensions- & försäkringsbolagen håller fortfarande god nivå då de i genomsnitt uppfyller detta till 80% respektive 85%. Varken Finansinspektionen eller BS25999 nämner några speciella regler om *hur* efterlevnad och kontroller ska ske. Finansinspektionen rekommenderar att kontinuitetsarbetet beskrivs i en övergripande policy men att det är av mindre vikt hur det kommuniceras; bara det kommuniceras till samtliga anställda. Vi tolkar resultatet som att

banker och övriga finansiella aktörer i sämre utsträckning än storbanker och pensions- och försäkringsbolag lyckas kommunicera sin policy kring kontinuitetshantering.

BS25999 har inga krav på efterlevelse gentemot internpolicys. Däremot nämner de att själva policyn ska innehålla reglerande och avtalsenliga förpliktelser. Detta finner vi mycket starkt stöd för hos storbankerna som till 100% uppfyller detta. Även pensions- & försäkringsbolagen med 92,5% och övriga finansiella aktörer som till 80% gör detta. Bankerna däremot svarar att de endast till 57,5% efterlever rekommendationer och kraven från myndigheterna. Vi tror att större aktörer uppmärksammas mer av myndigheter och således genomgår många fler kontroller, vilket kanske kan förklara det höga resultatet. De finansiella företagen som grupp klarar sig någorlunda bra men bankerna som drar ner snittet bör förbättra sig.

Företagen i undersökningen har lägre genomsnittliga svarsvärden för de påståenden som mäter en långsiktig och strategisk kontinuitetsplanering. Det är bland annat detta som är orsaken till att företagen inte når mognadsnivåerna fem eller sex. I snitt 68,1% anser ändå samtliga företagstyper att kontinuitetshantering är en viktig del av strategin och även här är pensions- och försäkringsbolag samt storbanker i framkant. Bankerna drar ner snittet då de endast uppfyller detta till 42,5%. Här ser vi dock en anledning att kommentera mätmetoden. Vi valde att anamma BCM-modellens syn att frekvensen i antalet genomförda risk- och påverkansanalyser visar kontinuitetshanterings strategiska vikt. För de större aktörerna, det vill säga storbanker jämfört med andra banker, faller det naturligt att genomföra många analyser för att kunna omfatta en större affärsverksamhet, vilket inte behövs i samma omfattning för ett mindre bolag. Om vi återgår till antagandet att större aktörer granskas mer av myndigheter, kan vi även anta att de måste vara mer frekventa i sina egna analyser för att säkerställa att de uppfyller de krav som finns. Dock bör det sättas i relation till företagets uppfattning om hur viktig kontinuitetshanteringen är för strategin. Enligt Finansinspektionen ansvarar ledningen för att företaget uppfyller sina verksamhetsmål och därför också ansvarar för kontinuitetshanteringen. Finansinspektionen anser att styrelsen bör fastställa definitioner och toleransnivåer av operativa risker vilket vi kategoriserar som strategiskt arbete. BS25999 anger att verktyget för att kunna fastställa sådana definitioner och toleransnivåer är just påverkansanalyser. Vi tolkar därmed resultatet som att det finns brister vad det gäller detta hos alla fyra företagstyper men framför allt hos de mindre bankerna och övriga finansiella aktörer.

Att de finansiella företagen har en successionsplan för VD och ledning, det vill säga ett formaliserat sätt att sköta överlämningen mellan personer i ledande befattning, uppfylls i snitt till 62,3% vilket bör betraktas som ett relativt lågt svarsvärde. Pensions- och försäkringsbolagen urskiljer sig dock som ett undantag och uppfyller det nästan helt, till 95%. Mest överraskande är att storbankerna står för det sämsta resultatet här och uppfyller påståendet till 42,5%. Vid närmare granskning visar det sig att det är stor skillnad storbankerna emellan om de har en successionsplan eller inte. Två storbanker uppfyller inte alls detta påstående medan de andra två ligger i toppskiktet. BS25999 anger att förändringar av kontinuitetshanteringen aktivt bör övervakas där successionsförvaltning för ledningen ska ingå som en del - att detta görs av pensions- och försäkringsbolagen förklarar varför de uppnår ett markant bättre resultat än övriga tre företagstyper. Klart står att de flesta av de finansiella företagen inte har uppmärksammat successionsförvaltning som en del av kontinuitetshanteringsarbetet.

Något som ytterligare visar att de finansiella företagen har en sämre kontinuitetshantering på längre sikt är att de inte anser att kontinuitetshantering bidrar till strategisk utveckling, då det genomsnittliga svarsvärdet endast är 47,7% för detta påstående. Något mer vanligt är ett program för kontinuitetshantering som sträcker sig över fler år där de sammanlagt uppfyller detta till 57,5%. Ännu lite bättre var samarbetet mellan avdelnings- eller mellanchefer och avdelningen för kontinuitetshanteringen där detta till 65,2% fungerade.

Vidare visar undersökningen en intressant diskrepans gällande företagens egen uppfattning om huruvida kontinuitetshantering är en viktig del av strategin, och de påståenden som faktiskt mäter detta. Detta illustreras av att titta närmare på påstående 18 och jämföra det med resten av de påståenden som behandlar kontinuitetshantering på strategisk nivå (P24, P26, P28 och P29). Påstående 18 lyder; "Kontinuitetshantering är identifierat som en del av strategin. Detta visas genom att analyser av risk- och påverkansanalyser genomförs regelbundet". Tabell 5.2 på följande sida visar skillnaden i svarsvärde för de olika påståendena.

	P18	Snitt P24, P26, P28 och P29
Bank	42,5%	48,7%
Pensions- & försäkringsbolag	82,5%	75,6%
Storbank	82,5%	51,2%
Övrig finansiell aktör	65,0%	57,1%

Tabell 5.2 Kontinuitetshantering på strategisk nivå

Tabellen visar att banker är den enda kategori som har ett högre svarsvärde för P18 än för de andra påståenden som mäter om kontinuitetshandlingen ingår i företagets långsiktiga strategi. Resten av företagstyperna överskattar detta hos sig själva. Det enligt oss mest intressanta i denna jämförelse är storbanker som anser till 82,5% att kontinuitetshandling är strategiskt viktigt men endast till 51,2% uppfyller de påståenden som mäter detta. Sammantaget tolkar vi detta återigen som att företagen inte fullt ut tillämpar kontinuitetshandlingen som en långsiktig del i strategiarbetet, och inte heller är medvetna om att detta är en brist.

5.2.2 Anställdas medvetenhet och övning

De anställdas medvetenhet och övning (AM & ÖVN) har ett svarsvärde om i genomsnitt 66,9%. Pensions- och försäkringsbolagen samt storbankerna utmärker sig även här genom att uppnå ett högre snitt än de andra två företagstyperna. Efter ledarskap och implementering av kontinuitetsplaner är det alltså de anställdas medvetenhet och övningar som driver kontinuitetsarbetet för de finansiella företag och som orsakar att "branschen" uppnår den fjärde mognadsnivån i BCM-modellen. Tabellen nedan visar en sammanställning av svarsvärdena inom denna kontinuitetskompetens.

	P2	P3	P4	P8	P10	P16	P21	P22	Snitt:
Bank	67,5%	57,5%	60,0%	57,5%	35,0%	55,0%	62,5%	22,5%	50,0%
Pensions- & försäkringsbolag	85,0%	90,0%	82,5%	72,5%	62,5%	87,5%	80,0%	55,0%	76,9%
Storbank	75,0%	90,0%	77,5%	100,0%	60,0%	77,5%	77,5%	45,0%	75,3%
Övrig finansiell aktör	71,7%	61,7%	88,3%	65,0%	55,0%	73,3%	66,7%	23,3%	63,1%
Snitt:	74,8%	74,8%	77,1%	73,8%	53,1%	73,3%	71,7%	36,5%	66,9%

P2 Anställda är medvetna om en enklare terminologi inom kontinuitetshandling

P3 Anställda och ledning är medvetna om behovet av samarbete och interna förbindelser för mer täckande och smidigare kontinuitetshandling

P4 Det finns en "förkämpe" bland chefer eller inom ledningen till kontinuitetshandling

P8 Det finns en gemensam terminologi inom kontinuitetshandling som används av samtliga avdelningar som är involverade i företagets kontinuitetshandling

P10 Det finns ett träningsprogram som ökar medvetenheten av kontinuitetshandling för avdelningar som är involverade i företagets kontinuitetshandling

P16 Företaget har genomfört övningar inom kontinuitetshandling för kritiska affärsprocesser

P21 Majoriteten av organisationen deltar i kontinuitetshandlingen

P22 Det finns ett kompetensutvecklingsprogram för personalen som är ansvariga för företagets kontinuitetshandling

Tabell 5.3 Svarsvärde per företagstyp inom anställdas medvetenhet och övning

Samtliga företagstyper anger till relativt hög grad att det finns en "förkämpe" bland chefer eller inom ledningen till kontinuitetshandling då detta var det påståendet med högst svarsvärde 77,1%. Vi menar att detta är så pass högt att det måste anses följa Finansinspektionens och BS25999:s riktlinjer eftersom vi tolkar det som att en sådan ambassadör

finns i de flesta företagen. Båda riktlinjerna rekommenderar att det bör finnas personer inom företaget som kan ses som verksamhetens ambassadörer i kontinuitetsfrågor med uppdrag att höja medvetenheten hos sina medarbetare. Samtliga företagskategorier brister dock i en mer långsiktig hantering kring medvetenheten hos anställda. Att det finns ett kompetensutvecklingsprogram för dem i personalen som är ansvariga för företagets kontinuitets- hantering uppfylls endast till 36,5% i genomsnitt. Banker och övriga finansiella aktörer är de som påverkar snittet mest negativt. Intressant att notera är att storbankerna visar störst varians inom företagstypen vad det gäller detta. **Två av bankerna anger att ett kompetens- utvecklingsprogram för ansvariga inte finns alls, 0%, och de andra två uppfyller det till 50% respektive 70%.** Återigen anser vi att det är anmärkningsvärt att inte samtliga storbanker ligger i framkant vad det gäller detta.

Enligt Finansinspektionen måste medvetenhet kring kontinuitetsfrågor genomsyra inom hela organisationen och medvetenheten skapas genom utbildning och övning av all personal. Målet är att alla ska veta vad de ska göra om den egna verksamheten drabbas. Svaren i under- sökningen visar att detta uppfylls till stor del för de finansiella företagen som helhet, men i synnerhet hos pensions- och försäkringsbolagen samt storbankerna. Alla företagstyper har ett svarsnitt på över 70% för påståendet att majoriteten av organisationen deltar i kontinuitets- hanteringen. Detta kan dock vara en något svårtolkad fråga för respondenterna - då "att delta" kan betyda många olika saker. För att få en mer nyanserad bild kan då nämnas att de anställda är medvetna om en enklare terminologi inom kontinuitetshantering och att de är medvetna om behovet av samarbete och interna förbindelser för kontinuitetshantering med i snitt 74,8%. Med detta som bakgrund menar vi att dessa riktlinjer alltså till största del följs av samtliga företagstyper.

BS25999 poängterar vikten av utbildning och övning som en viktig del i att öka medvetenheten kring kontinuitetshantering. Detta är ett område som vi anser att företagen genomför med undantag för banker som endast uppfyller det delvis. Finansinspektionen fastslår hur viktigt detta är och för att bli certifierad mot BS25999 krävs att företaget regelbundet genomför övningsaktiviteter som ska utvärderas efter målsättning och ske särskilt när signifikanta förändringar har ägt rum. Med bakgrund av Finansinspektionens rekomm- endationer och de krav BS25999 ställer, behöver endast banker förbättra sig på detta område.

Liksom faktorerna ledarskap och implementering brister våra respondenter något i arbetet med att öka medvetenheten i organisationen på längre sikt. De finansiella företagen uppfyller endast delvis att det finns ett träningsprogram som ökar medvetenheten av kontinuitetshantering. Sammantaget tolkar vi resultaten vad gäller denna faktor att de anställda i de finansiella företagen generellt sett vet vad kontinuitetshantering innebär och vad som måste göras i händelse av en störning men att företagen inte vidareutvecklar kompetensen i företaget.

5.2.3 Resursfördelning och mätning

Resursfördelning och mätning (RES & MÄT) har det i snitt lägsta svarsvärdet av alla fyra kompetenser, 57,3% och är således den minst drivande faktorn i kontinuitetshanteringsarbetet hos de finansiella företagen. Tabell 5.4 nedan visar svarsvärdena för respektive påstående och företagstyp.

	P6	P11	P12	P17	P19	P20	P27	Snitt:
Bank	60,0%	62,5%	37,5%	30,0%	72,5%	30,0%	20,0%	44,6%
Pensions- & försäkringsbolag	85,0%	82,5%	67,5%	62,5%	72,5%	70,0%	65,0%	72,1%
Storbank	90,0%	92,5%	85,0%	17,5%	45,0%	62,5%	52,5%	63,6%
Övrig finansiell aktör	65,0%	71,7%	66,7%	15,0%	43,3%	45,0%	35,0%	48,8%
Snitt:	75,0%	77,3%	64,2%	31,3%	58,3%	51,9%	43,1%	57,3%

P6 Företaget har upprättat referenspunkter (benchmarks) inom sin kontinuitetshantering

P11 Det finns etablerade krav på återhämtningstider och återställningspunkter av kritiska funktioner vid inträffandet av en kris

P12 Samtliga avdelningar/affärsenheter har implementerat egna kontinuitetsplaner

P17 Det finns dokumenterade prestationsmål inom kontinuitetshantering som är länkade till kompensation

P19 Det finns en styrande kontinuitetskommitté vilken representerar organisationens samtliga avdelningar

P20 Företaget visar/har visat förbättrade resultat efter utvärderingar av kontinuitetshanteringen

P27 Det finns metoder och verktyg som används för kontinuerlig utvärdering av kontinuitetsprogrammets effektivitet och lämplighet

Tabell 5.4 Svarsvärde per företagstyp inom resursfördelning och mätning

Trots att ledningen har uppmärksammat kontinuitetshantering som en viktig del av arbetet, kontinuitetsplaner har implementeras och de anställda är relativt medvetna om kontinuitetshanterings betydelse, allokeras inte resurser till kontinuitetshanteringen i samma utsträckning. Mätningar för förbättringar genomförs inte heller på ett lika omfattande sätt.

Våra respondenter säger sig ha upprättat referenspunkter, det vill säga jämförelsemått, för kontinuitetshantering i snitt med 75%, med storbanker och pensions- & försäkringsbolag i

spetsen. Enligt BS25999 bör referenspunkterna utgå från standarder, vilket i och för sig säger sig självt eftersom det är just en standard. Som tidigare nämnt anser de finansiella företagen själva att de följer Finansinspektionens rekommendationer i hög grad, vilket kan implicera att de i mindre utsträckning utgår från internationell standard. Vi väljer att låta detta vara osagt då inget påstående direkt utvisar om det är så eller inte. Då BS25999 exempelvis anger att referenspunkter bör finnas i kontinuitetspolicyn, ser vi detta som en av anledningarna till varför banker och övriga finansiella aktörer inte i dagsläget skulle klara en certifiering mot standarden. Däremot uppfyller pensions- och försäkringsbolag samt storbanker BS25999:s krav på upprättade av referenspunkter till 90% respektive 85%.

Enligt studien har de finansiella företagen till 77,3% etablerade krav på återhämtningstider för kritiska affärsfunktioner, vilket vi anser vara en relativt bra nivå. Detta är någonting som verkligen har betydelse för företagets intressenter och generellt anser vi det vara tillräckligt för att möta kraven i BS25999 för accepterade avbrottstider vid i händelse av en störning. Även Finansinspektionen rekommenderar att företag definierar konkreta toleransnivåer, vilket resultatet visar att de finansiella företagen som helhet gör till en godkänd nivå.

Vad gäller resursallokering till kontinuitetshandlingen håller företagen i undersökningen generellt en låg nivå, vilket är en av anledningarna att de inte sammantaget når nivå fem eller sex i mognadsgrad. I snitt har 64,2% av företagets avdelningar implementerat egna kontinuitetsplaner, specifika för deras del i verksamheten. Banker underpresterar relativt de andra kategorierna här då endast 37,5% av avdelningarna har egna kontinuitetsplaner. Inte heller representeras hela organisationen i en central kontinuitetskommitté; i snitt är det drygt hälften av företagets avdelningar som medverkar, då detta påstående uppfylls till 58,3%. Storbanker och övriga finansiella aktörer har föga imponerande resultat på 45% respektive 43,3%. I Finansinspektionens riktlinjer poängteras hur viktigt det är att kontinuitetshandlingen avser central såväl som lokal verksamhet - utan en representation av samtliga avdelningar kan företaget inte få en samlad bild av den totala riskexponeringen. Vi tolkar således dessa resultat som att riktlinjerna inte efterföljs tillfredställande på den punkten. Dock bör nämnas något om företagstyperna vad det gäller detta. Eftersom mindre företag som banker består av färre avdelningar i förhållande till storbankerna, blir varje avdelning utan en representant i en kontinuitetskommitté ganska märkbar, vilket kan ge ett förstärkt negativt resultat.

Finansinspektionen anger att det bör finnas en ansvarsdelning mellan styrelse, riskkontrollenheten och berörda befattningshavare. BCM-modellen drar det så långt som att även koppla detta till kompensation för att nå de högre mognadsnivåerna. För att uppmuntra representanternas arbete i kontinuitetskommittén bör de kompenseras för att öka deras ansvarstagande i frågan. Avsaknaden av detta hos våra respondenter är dock påtaglig med undantag för pensions- & försäkringsbolagen som grupp. Ser vi till enskilda företag svarade totalt åtta stycken att det inte finns någon koppling alls mellan prestationsmått och kompensation. De resterande företagen har låga svarsvärden förutom ett försäkringsbolag som anger att detta uppfylls till 100%. Det kanske mest förvånande resultatet ser vi hos storbankerna som har så lite som 17,5%. Här är det samma två storbanker som inte implementerat detta i sin kontinuitetshantering, som heller inte hade någon successionsplan för ledning och styrelse.

Vi anser de finansiella företagen som helhet inte har en tillräckligt god förmåga att tillgodose hela organisationens behov i avseendet centrala kontinuitetskommitté, vilket är ett måste för att nå de högre mognadsgraderna fem och sex i BCM-modellen. För det första är inte tillräckligt stor del av avdelningarna representerade och för det andra uppmärksammas inte kontinuitetsarbetet tillräckligt då oftast ingen kompensation är knuten till det (se stycket ovan). Denna uppfattning förstärks då vi även väger in att samarbetet mellan avdelningschefer och kontinuitetsavdelningen endast fungerade till 65% (se sista stycket i avsnitt 5.2.1). Tittar vi närmre på storbankerna som har överraskande låga 45% ser vi att det återigen handlar om stora skillnader inom denna grupp och det är samma två som inte alls har någon central kommitté för kontinuitetshantering.

Studien undersöker också i vilken utsträckning det finns metoder och verktyg för att utvärdera kontinuitetshanteringens effektivitet och lämplighet. Det visar sig vara ett stort förbättringsområde. Sammantaget var resultatet mycket dåligt då detta uppfylls till i snitt 43,1%. Sämsta företagstypen är banker med ett snitt på 20%, där två banker överhuvudtaget inte hade några mätmetoder. Finansinspektionen rekommenderar att företagsledningen bör få en sammanfattande riskrapport som samlar bilden av företagets riskexponering. BS25999 anger också att det fordras mätverktyg för att kunna utvärdera kontinuitetshantering. Att företagen brister vad det gäller detta visar sig också när företagen fick ta ställning till påståendet om de visat förbättrade resultat i sitt kontinuitetsarbete. De två bankerna som inte hade några mätmetoder alls svarade, föga förvånande, att de inte alls kunde se några förbättringar.

5.2.4 Externa förbindelser

Externa förbindelser (EXT FÖR) är en mindre starkt drivande faktor för kontinuitetshantering i de finansiella företagen då svarsvärdet för dessa påståenden i snitt är 59,3%. Vi finner det dock inte så förvånande då varken Finansinspektionen eller BS25999 tar upp detta som någonting avgörande i sina rekommendationer - i den sistnämnda finns en sådan infallsvinkel inte med alls. BS25999 anger endast att företag bör definiera och kommunicera målsättningen med sin kontinuitetshantering med hänsyn till sina intressenter samt myndigheter, men några krav på externa samarbeten finns inte. Tabell 5.5 visar samtliga svarsvärden för varje påstående och genomsnittet.

	P7	P14	P23	P25	P30	Snitt:
Bank	70,0%	72,5%	52,5%	20,0%	45,0%	52,0%
Pensions- & försäkringsbolag	87,5%	92,5%	85,0%	47,5%	52,5%	73,0%
Storbank	87,5%	65,0%	65,0%	40,0%	57,5%	63,0%
Övrig finansiell aktör	65,0%	46,7%	61,7%	38,3%	33,3%	49,0%
Snitt:	77,5%	69,2%	66,0%	36,5%	47,1%	59,3%

P7 Företaget har i någon mån relationer och vissa koordineringar med lokala brandkåren, polisen och säkerhetsmyndigheter

P14 Det finns överenskommelser vad gäller servicenivåer och prestanda som ert företag ska upprätthålla gentemot externa intressenter vid händelse av en kris

P23 Det finns krav på efterlevnad av företagets kontinuitetshantering vid kontraktsutformningar med företagets intressenter

P25 Kontinuitetshantering marknadsförs som en konkurrensfördel gentemot företagets intressenter

P30 Externa intressenter deltar i gemensamma övningar av olika krisscenarion

Tabell 5.5 Svarsvärde per företagstyp inom Externa förbindelser

Finansinspektionen tar kort upp externa förbindelser i sin vägledning och menar att krisberedskap hos leverantörer och andra samarbetspartners har stor betydelse. Finansinspektionen föreslår kravställning i avtal som kan skapa förutsättningar för de finansiella bolagen att matcha den egna skyddsnivån mot omvärlden, och att företagen och dess motparter därför bör synkronisera de delar av kontinuitetsplanerna som berör bägge parter. Att det finns krav på efterlevnad av företagets kontinuitetshantering vid kontraktsutformningar med intressenterna uppfyller de finansiella företagen till i snitt 66,0%, där banker utmärker sig genom att göra det i mindre utsträckning och pensions- och försäkringsbolagen i stor utsträckning. En av tre storbanker, en av de två som inte har en successionsplan eller styrande kommitté, i väldigt liten utsträckning (10%) efterlever kraven på företagets kontinuitetshantering vid kontraktsutformningar medan övriga tre storbanker har

goda svarsvärden på detta påstående. Vi tolkar resultaten som att pensions- och försäkringsbolagen samt övriga tre storbanker är de enda företag som kan sägas följa Finansinspektionens riktlinjer och att resterande tre bör utveckla arbetet på den punkten och bättre inkorporera kontinuitetshantering i avtal med externa parter.

Andra förbättringsområden går att identifiera inom denna kontinuitetskompetens. Exempelvis förekommer inte gemensamma övningar av olika krisscenarion med externa intressenter såsom partners, leverantörer, kunder, myndigheter i särskilt hög utsträckning. Detta påstående uppfylls endast till 47,1%. Inte heller marknadsförs kontinuitetshanteringsarbetet som en konkurrensfördel gentemot företagets intressenter då detta endast uppfylls till 36,5%. Detta orsakar att snittet på kontinuitetskompetensen dras ner och bidrar till att företagen hamnar i den fjärde kontinuitetsmognadsnivån i BCM-modellen. Här finner vi således tydliga områden som behöver förbättras för att kontinuitetshanteringen ska nå ytterligare mognad, dock är det ingenting som varken BS25999 eller Finansinspektionen direkt kräver. Vi menar att de finansiella företagen ändå bör stäva efter detta då beroendet av externa förbindelser spelar stor roll för kontinuitetshanteringen. Det anser även Finansinspektionen som poängterar att i värsta fall kan det egna företaget bli det enda som fungerar vid en större kris, men ändå inte förmår bedriva sin egen verksamhet på grund av motparternas bristande kontinuitets-hantering.

Generellt har företagen en god beredskap vad det gäller koordineringar med lokala brandkåren, polisen och säkerhetsmyndigheter då detta uppfylls till 77,5%. Dock är det en relativt stor skillnad mellan företagstyperna vad det gäller överenskommelser om servicenivåer och prestanda som företagen ska upprätthålla gentemot externa intressenter vid händelse av en kris. Här svarar pensions- och försäkringsbolagen att det uppfylls till hela 92,5% när övriga finansiella aktörer inte ens uppfyller påståendet delvis, endast 46,7%. Vi finner det låga svarsvärdet för just det påståendet något förvånande då det inom gruppen övriga finansiella aktörer kan finnas bolag som investmentbanker, fondkommissionärer och börs. Vi antar att den typen av bolag ofta har sofistikerade samarbetspartners vilket i vår mening borde leda till att deras, liksom pensions- och försäkringsbolagens, intressenter är mer benägna att kräva sådana överenskommelser. Samma storbank som inte tillämpar kontinuitetshantering vid kontraktutformningar har svarat att de heller inte har några överenskommelser om servicenivåer gentemot sin omgivning vilket leder till att snittet dras ner då övriga tre storbanker till över 80% gör detta.

6. SLUTSATSER

6.1 Hur väl hanterar svenska finansiella företag operativa risker?

För att kunna uttala oss om hur väl ett företag hanterar operativa risker har vi studerat hur långt gångna de är i kontinuitetshanteringsarbetet och därmed vilken mognadsnivå de har på området. Enligt Business Continuity Maturity Model (BCM-modellen) uppnår företagen i undersökningen en mognadsnivå fyra av sex, med ett "branschsnitt" på 4,26. Vi ser alltså en tendens är att svenska finansiella företagen hanterar sina operativa risker genom att hålla en medelhög beredskapsnivå gentemot störningar eller kriser i kärnverksamheten. Med tanke på den viktiga samhällsfunktion som finanssektorn utgör anser vi att en medelhög mognadsnivå inte är hög nog. Studien bekräftar att det fortfarande är stor spridning bland företagen i utvecklingen av kontinuitetshanteringen, någonting som Finansinspektionen fastslog redan 2005. Vi hade förväntat oss att detta skulle ha förbättras de senaste fem åren och därmed att vår studie skulle ge en mer samlad bild av företagens kontinuitetshanteringen i finansbranschen. Framför allt är det inte orimligt att kräva att de fyra storbankerna gemensamt ligger i framkant i denna utveckling – vilket undersökningen visar att så inte är fallet.

Istället uppvisar storbankerna stora skillnader sinsemellan. Två av dem har inte i samma utsträckning; en successionsplan för styrelse och VD, en enhet som representerar eller samarbetar med samtliga av företagets avdelningar eller länkar prestation inom kontinuitetshantering med kompensation. En av dessa två storbanker utmärker sig ytterligare genom att dessutom inte utformat överenskomna servicenivåer vid händelse av en störning eller värdesätta kontinuitetshantering vid kontraktutformningar. Detta företag har en mognadsnivå på 3,58 – vilket är helt klart underkänt för att vara en storbank. Även vad det gäller banker och övriga finansiella bolag finns det stora utrymmen för förbättringar.

Studien visar att det är pensions- och försäkringsbolagen som har den genomsnittliga högsta kontinuitetsmognaden och således bäst hanterar de operativa riskerna.

Sammantaget har de finansiella företagen en kortsiktigt god kontinuitetshantering men för att nå högre kvalitetsnivåer, vilket är av intresse för företagets intressenter och samhället i stort, måste kontinuitetshanteringen ingå till större del i företagets strategiska planering. Detta kommer vi att förklara mer ingående i nedanstående slutsatser.

6.2 Vilka faktorer driver deras kontinuitetshanteringsarbete?

Resultaten visar att ledarskap och implementering generellt sett är de mest drivande faktorerna och resursfördelning och mätning de minst drivande faktorerna - en trend som kan ses inom alla fyra företagstyper. Hur stark drivkraften är mäts genom hur höga de genomsnittliga svarsvärdena var inom varje faktor. Ledarskap och implementering har ett svarsvärde om 70,4%, anställdas medvetenhet och övning 66,9%, resursfördelning och mätning 57,3% samt externa förbindelser 59,3%.

Engagemang hos ledningen och implementering av terminologi samt kontinuitetsplaner för kritiska funktioner med återställningskrav, tycks hittills ha drivit kontinuitetshanteringsarbetet hos de finansiella företagen. Däremot har de sammantaget låga svarsvärden hos de påstående som behandlar kontinuitetshandling som en del i företagets långsiktiga strategi. Studien visar också att det finns en diskrepans gällande företagets egen uppfattning gällande detta och de påstående som faktiskt mäter detta, vilket tyder på att de generellt inte är medvetna om att detta är en brist i deras kontinuitetshanteringsarbete.

De anställda hos företagen tycks vara medvetna om att kontinuitetshandling är viktigt för företaget, men utbildningsprogram för varken de anställda eller de ansvariga inom kontinuitetshandlingen förekommer dock i tillfredställande utsträckning.

Företagen har överlag bra kontakt med krismyndigheter såsom polis och brandkår, samt har i viss mån även uppmärksammat kontinuitetshandling vid kontraktutformningar med företagets intressenter. Dock genomförs inte övningar med företag i omgivningen, vilket krävs för att ytterligare öka kvalitetsnivån inom kontinuitetshandling.





De minst drivande faktorerna enligt studien är resursfördelning och mätning, vilket går hand i hand med slutsatsen att kontinuitetshandling inte ses ur ett långsiktigt perspektiv hos företagen. Så länge företagen har få verktyg och metoder att tillgå för att utvärdera arbetet, finns ingen lärdomsprocess och det långsiktiga kontinuitetshanteringsarbetet försvåras.

6.3 Är det tillräckligt för att möta Finansinspektionens rekommendationer och hur står sig detta mot internationell standard?

Företagen i studien uppnår visserligen i genomsnittlig mognadsnivå om 4,26 inom kontinuitetshantering, men den stora spridning som förekommer gör att vi inte kan dra slutsatsen att branschen som helhet möter Finansinspektionens rekommendationer tillräckligt. Förbättringar krävs i synnerhet för de företag som hamnar i mognadsnivå två och tre, samt de två storbanker som vi tidigare nämnt.

De olika kontinuitetskompetenserna utgör drivande faktorer och Figur 6.1 nedan illustrerar vilka områden som kräver förbättringar inom varje företagstyp. De orangea och röda fälten indikerar att åtgärder behöver vidtas för att möta Finansinspektionens och BS25999 rekommendationer. Slutligen kan sägas att inget företag i undersökningen skulle enligt vår tolkning vara redo att certifieras mot BS25999 då detta kräver att samtliga punkter i standarden uppfylls vilket implicerar att företagen befinner sig i mognadsnivå sex.

	LDR	IMP	AM	ÖVN	RES	MÄT	EXT FÖR
Banker	1. Fler kontroller 2. Ökat engagemang hos ledningen		1. Bättre genensam terminologi 2. Ökat samarbete mellan avd.	1. Fler övningar 2. Arbeta med kompetensutveckling	1. Fler avdelnings-specifika kontinuitetsplaner	1. Införa mätverktyg 2. Kompensation kopplat till prestation	1. Införa övning med externa samarbetspartners 2. Beakta kontinuitetshantering vid kontraktsutformning 3. Bättre samarbete polis osv.
Pensions- & försäkringsbolag							
Storbanker	1. Öka samarbetet mellan avd.			1. Arbeta med kompetensutveckling	1. Samtliga avdelningar repres. i kontinuitets-hantering	1. Införa mätverktyg 2. Kompensation kopplat till prestation	1. Införa övning med externa samarbetspartners 2. Beakta kontinuitetshantering vid kontraktsutformning 3. Bättre samarbete polis osv.
Övriga finansiella aktörer	1. Införa styrpogram 2. Sikta på strategisk utveckling		1. Bättre genensam terminologi 2. Ökat samarbete mellan avd.	1. Fler övningar 2. Arbeta med kompetensutveckling	1. Samtliga avdelningar repres. i kontinuitets-hantering	1. Införa mätverktyg 2. Kompensation kopplat till prestation	1. Införa övning med externa samarbetspartners 2. Beakta kontinuitetshantering vid kontraktsutformning 3. Bättre samarbete polis osv.

	Håller mycket god beredskapsnivå
	Håller en godkänd beredskapsnivå
	Bör förbättras i viss utsträckning
	Bör förbättras i stor utsträckning

Figur 6.1 Sammanfattande bild av de finansiella företagens kontinuitets-hantering baserat på de olika drivande kontinuitetskompetenserna - identifierar förbättringsområden

6.5 Utvärdering av metod

Vi anser även i efterhand att den kvantitativa metoden, med kvalitativt inslag, lämpade sig för denna undersökning. Business Continuity Maturity Model gav oss ett bra ramverk och verktyg att mäta hur väl finansiella företag hanterar operativa risker. Den största nackdelen som vi ser med tillvägagångssättet är att BCM-modellen trots allt inte är utvecklad varken från Finansinspektionens rekommendationer eller från BS25999:s riktlinjer. Detta gjorde att vissa påståenden ibland kändes något tagna ur luften och inte helt och hållet överensstämde med innehållet i respektive dokument. En konsekvens av det blev att vissa faktorer var svårare att mäta. Exempelvis nämns inte externa förbindelser i BS25999 och resursallokering och mätning ges lite fokus i Finansinspektionen vägledning.

Ett alternativ för oss hade varit att göra egna påståenden utifrån dokumenten, istället för att använda BCM-modellen. Vi menar dock att vi då hade missat en viktig del av undersökningen – vi hade i sådant fall inte kunnat uttala oss om utvecklingen av kontinuitetshanteringsarbetet, det vill säga mognadsgraden, hos de finansiella företagen. Det hade gjort det betydligt svårare att mäta hur väl företagen hanterar de operativa riskerna. En väl utarbetad modell kändes därmed mer gedigen som mätinstrument. Genom att använda BCM-modellen kunde vi dels studera kvalitetsnivån inom kontinuitetshantering och dels undersöka hur detta står sig gentemot Finansinspektionens rekommendationer och internationell standard.

Några respondenter reagerade mot användandet av Google Formulär, främst personer med tjänster inriktade mot IT-säkerhet. De var skeptiska till att använda ett nätbaserat formulär i Googles regi, vilket vi löste genom att skicka formuläret som ett Word-dokumentet som var lösenordsskyddat. Det var totalt tre företag som valde att svara på detta sätt.

6.6 Förslag till fortsatt forskning

För att få ytterligare kunskap och förståelse kring svenska finansiella företags risk- och kontinuitetshantering ser vi behov av ytterligare studier. Framför allt vore det önskvärt att undersöka ett större antal företag för att uppnå resultat som är ännu mer generaliserbara för finansbranschen. Vi har identifierat följande områden och problemformuleringar som kan vara av intresse att utreda vidare;

- Näst intill samtliga av de finansiella företagens huvudkontor är baserade i Stockholms innerstad och vi undrar vilka konsekvenser detta skulle kunna få vid en allvarig katastrof som drabbar det geografiska området? Exempelvis har de fyra storbankerna huvudkontor inom en mycket liten radie, vilket utifrån ett risk- och kontinuitetshanteringsperspektiv skulle vara intressant att studera närmare.
- I och med den tilltagande globaliseringen, står företag inför utmaningar i sin verksamhet. Hur påverkar detta en organisations operativa risker? Det vore intressant att se om det finns ytterligare dimensioner, relaterade till globaliseringen, som måste tas i beaktande när ett företags motståndskraft mot risker ska utvärderas.
- Då kontinuitetshantering är en fråga om sannolikhetsbedömning och resursallokering, kan det vara till hjälp för företagsledningarna att veta vilka generella hot (och möjligheter) som finns i den egna branschen. En undersökning som tar reda på vilka specifika operativa risker det finns inom olika branscher kan avhjälpa detta.

Som vi tidigare nämnde är kontinuitetshantering ett relativt nytt område i näringslivet, varför den fortfarande är i sin linda hos många företag i Sverige. Till synes behövs mer forskning inom området kontinuitetshantering; här ovan presenterar vi endast ett fåtal punkter som behöver utredas vidare. Dock hoppas vi att vår studie gett läsaren insyn i de finansiella bolagens hantering av operativa risker samt var i de brister i sin kontinuitetshantering, givet Finansinspektionens rekommendationer och internationell standard. Vi hoppas även att läsaren har fått en ökad förståelse för vikten av god kontinuitetshantering.

KÄLL- OCH LITTERATURFÖRTECKNING

Litteratur:

Bernstein, Peter (1998). *Against the Gods: The Remarkable Story of Risk*. New York: John Wiley & Sons

Cosserat, Graham W., Rodda, Neil (2009). *Modern auditing*. West Sussex: John Wiley & Sons

Eliasson, Annika (2006). *Kvantitativ metod från början*. Lund: Studentlitteratur

Hiles, Andrew & Barnes, Peter (1999). *The Definite Handbook of Business Continuity Management*. New York: John Wiley & Sons

Jacobsen, Dag Ivar (2000). *Vad, hur och varför?* Lund: Studentlitteratur

Lundahl, Ulf & Skärvad, Per-Hugo (1999). *Utredningsmetodik för samhällsvetare och ekonomer*. Studentlitteratur: Lund

Snedaker, Susan (2007). *Business Continuity & Disaster Recovery for IT Professionals*. Burlington: Syngress Publishing Inc.

Muntliga källor:

Drogendijk, Rian, Universitetslektor och docent, Företagsekonomiska institutionen, Uppsala universitet 2010: muntl. samtal (05.05.2010)

Friberg, Claes, *Områdesansvarig BCM*, 4C Strategies, 2010: muntl. Samtal/Presentation (01.04.2010)

Akademiska artiklar:

Hansson, Sven Ove 2005: Seven Myths of Risk, *Risk Management*. Vol. 7, No. 2, pp. 7-17. Palgrave Macmillan Journals.

Kallman, James Wm. & Maric, Violette R., 2004: A Refined Risk Management Paradigm , *Risk Management*. Vol. 6, No. 3, pp. 57-68. Palgrave Macmillan Journals.

Swartz Ethne, Dominic Elliott, Herbane Brahim, 2003: Greater than the Sum of Its Parts: Business Continuity Management in the UK Finance Sector, *Risk Management*. Vol. 5, No. 1, pp. 65-80. Palgrave Macmillan Journals.

Tidningsartiklar:

Aberg, Anna & Holmberg, Kalle (2010). Åskmolnet och flygtrafiken, *Dagens Nyheter*, 17 april.

Flood, Linda (2009). Nyemissioner för 60 miljarder, *Svenska Dagbladet Näringsliv*, 7 augusti.

Elektroniska källor:

4C Strategies, 2010: Organisation (28.03.2010)
<http://www.4cstrategies.com/?pageID=4&postID=140>

Broadleaf Capital International, 2010: Organisation (06.04.2010)
<http://www.broadleaf.com.au/iso31000/index.html>

Finansplats Stockholm, 2010: Organisation (04.06.2010)
<http://www.finansplatsstockholm.se/projectweb/portalproject/Index.html>

TT, 2006: Fritidsresor fördubblade sitt resultat efter tsunamikatastrofen. *Sydsvenskan*, 18 december. (02.06.2010)
<http://www.sydsvenskan.se/ekonomi/article149029/Fritidsresor-fordubblade-sitt-resultat-aret-efter-Tsunamin.html>

Virtual Corporation, 2010: Organisation (07.04.2010)
http://www.virtual-corp.net/html/bcmm_download.html

Standarddokument:

BS31100:2008 *Risk Management Code of Practise*, 2010: Informationscentral (08.04.2010)
<http://www.bs25999.com/2009/12/bs311002008-risk-management-code-of-practice/>

BS25999-1:2006 *Business Continuity Management Part 1: Code of Practise*. ISBN 0580496015. November, 2007.

BS25999-2:2007 *Business Continuity Management Part 2: Specification*. ISBN 9780580599132. November, 2007.

Finansinspektionen, 2005:03 Myndighet (12.04.2010)
http://www.fi.se/upload/10_Om20FI/10_Verksamhet/krisberedskap/Vagledning_kontinuitetsplan_0503.pdf

Finansinspektionen, 2006:14 Myndighet (01.06.2010)
http://www.fi.se/upload/20_Publicerat/30_Sagt_och_utrett/10_Rapporter/2007/Rapport2007_16.pdf

Finansinspektionen, 2006:18 Myndighet (12.04.2010)
http://www.fi.se/upload/20_Publicerat/30_Sagt_och_utrett/10_Rapporter/2006/Rapport2006_18.pdf

Finansinspektionen, 2005: Myndighet (12.04.2010)
http://www.fi.se/upload/20_Publicerat/30_Sagt_och_utrett/10_Rapporter/2005/Rapport2005_3.pdf

BILAGA 1 - E-post till företagen

ÄMNE: Enkätundersökning, Uppsala universitet

Hej [namn],

Tack för ett trevligt samtal. Nedan finner du länken till undersökningen om er kontinuitetshantering, bifogat finns även ett informationsbrev om uppsatsen samt våra kontaktuppgifter. Ert företagsnamn kommer inte att användas i uppsatsen och givetvis skickar vi ett exemplar när den är färdig.

Enkäten tar maximalt 15 minuter att fylla i och vi uppskattar att du tar dig tid till detta. Vi är beroende av ditt svar och hoppas kunna sammanställa svaren så fort som möjligt.

Tack för din medverkan!

[Till enkäten>>](#)

Med vänliga hälsningar,
Magnus & Johanna

ÄMNE: *PÅMINNELSE* Enkätundersökning, Uppsala universitet

Hej [namn],

X-dagen den X/4 skickade vi en enkätundersökning som är underlag till vår magisteruppsats inom risk- och kontinuitetshantering. Vi är mycket beroende av er medverkan och undrar om du har några frågor eller funderingar kring frågorna. I annat fall hoppas vi kunna sammanställa svaren så fort som möjligt.

Nedan finner du länken till undersökningen och enkäten tar maximalt 15 minuter att fylla i.

Återigen, tack för din medverkan!

[Till enkäten>>](#)

Med vänliga hälsningar,
Magnus & Johanna

BILAGA 2 - Informationsbrev

Hej,

I denna text följer information om den uppsats vi skriver vid Uppsala universitet och den undersökning du har tackat ja till att medverka i.

Uppsatsen ämnar undersöka kontinuitetshanteringen inom svenska finansiella företag och skrivs inom ämnet Företagsekonomi vid Företagsekonomiska institutionen, Uppsala universitet. Studien syftar till att belysa vikten av en god risk- och krishantering och undersöka om svenska finansiella företag tycks uppmärksamma riskerna som uppkommer i den dagliga verksamheten.

Ert deltagande sker anonymt, varken företagets eller besvararens namn kommer att användas i uppsatsen. Vi reserverar oss dock för att använda besvararens titel för att ge svaren validitet. Om så önskas, skickar vi gärna ett exemplar av den färdiga uppsatsen.

Uppsatsen kommer att lämnas till en examinator för bedömning samt diskuteras under ett seminarium den 1 juni på Ekonomikum, Kyrkogårdsgatan 10 i Uppsala.

Om du har några frågor om uppsatsen eller undersökningen, tveka inte att höra dig till någon av oss.

Magnus Friberg 0736987124 magnus-friberg@hotmail.com	Johanna Busk 0703679447 johanna.busk@gmail.com
--	--

Det går även bra att kontakta vår handledare Mats Karén på e-postadress mats.karen@fek.uu.se eller via telefon 018 – 471 1365.

Tack för din medverkan!

Med vänliga hälsningar,
Magnus Friberg & Johanna Busk

BILAGA 3 - Enkäten

Enkäten skickades genom ett webbformulär, vilket här är omgjort till wordformat

Kontinuitetsmognad inom finansbranschen

Nedan finner du 30 påståenden kring kontinuitetshandling att ta ställning till och du ska försöka uppskatta till vilken grad ditt företag uppfyller varje givet påstående. Svarsintervallet är 0-100% där 0% innebär att företaget inte alls uppfyller påståendet och 100% innebär att företaget uppfyller påståendet helt.

Under många påståenden finns en hjälptext som ytterligare förklarar och exemplifierar det ovanstående påståendet.

1. Det finns mindre omfattande manual för åtgärder vid nödsituationer och kriser. * *En mindre omfattande manual är exempelvis en enkel lista över åtgärder som behöver utföras, personer som behöver ringas etc*
2. Anställda är medvetna om en enklare terminologi inom kontinuitetshandling *
Exempel på terminologi inom kontinuitetshandling: operativa risker, kritiska funktioner, ringlista osv.
3. Anställda och ledning är medvetna om behovet av samarbete och interna förbindelser för mer täckande och smidigare kontinuitetshandling. * *Välj en högre siffra om anställda och avdelningschefer i hög grad diskuterar olika samarbeten och interna förbindelser inom kontinuitetshandling*
4. Det finns en "förkämpe" bland chefer eller inom ledningen till kontinuitetshandling *
Med "förkämpe" menar vi en person som uppmärksammar ett problem och kämpar för att problemet skall tas upp av ledningen.
5. Det förekommer en eller flera planer inom områdena verksamhetsåterhämtning, teknisk återhämtning, säkerhetsföreskrifter och/eller olycksfall *
6. Företaget har upprättat referenspunkter (benchmarks) för kontinuitetshandlingen *
Referenspunkter; ett antal krav på kontinuitetshandling som ledningen satt upp
7. Företaget har i någon mån relationer och vissa koordineringar med lokala brandkåren, polisen och säkerhetsmyndigheter *
8. Det finns en gemensam terminologi inom kontinuitetshandling som används av samtliga avdelningar som är involverade i företagets kontinuitetshandling *
9. Det finns ett styrprogram för avdelningar (vilka är involverade i kontinuitetshandling) som upprätthåller, åtminstone i begränsad utsträckning, efterlevnad gentemot gemensamma policys, standarder och "best practices" av företagets kontinuitetshandling. * *En slags "compliance" gentemot företagets kontinuitetshandling*
10. Det finns ett träningsprogram som ökar medvetenheten av kontinuitetshandling för företagets olika avdelningar*

11. Det finns etablerade krav på återhämtningstider och återställningspunkter av kritiska funktioner vid inträffandet av en kris * *Bedöm i vilken utsträckning detta förekommer - exempelvis om krav finns för samtliga kritiska funktioner (välj högre siffra) eller om endast krav för hur länge företagets server får ligga nere finns (välj lägre siffra)*
12. Samtliga avdelningar/affärsenheter har implementerat egna kontinuitetsplaner * *Om exempelvis få avdelningar har implementerat kontinuitetsplaner; Välj en lägre siffra*
13. Det finns en prioritetsordning gällande återställning av varje kritisk affärsfunktion * *Helt enkelt en rankinglista med den mest kritiska affärsfunktion först*
14. Det finns överenskommelser vad gäller servicenivåer och prestanda som ert företag ska upprätthålla gentemot externa intressenter (aktieägare, kunder, leverantörer osv) vid händelse av en kris * *Exempelvis hur många pallar mjölk Arla ska kunna leverera till ICA Maxi vid händelse av en strejk*
15. Det finns dokumenterat att företaget efterlever de rekommendationer och krav som myndigheter ställer gällande kontinuitetshantering * *Exempelvis Finansinspektionens: "Vägledning vid kontinuitetsplanering - Processen och planen" (Mars 2005)*
16. Företaget har genomfört övningar inom kontinuitetshantering för kritiska affärsprocesser * *Bedöm vilken nivå övningarna har; ju högre nivå desto högre siffra*
17. Det finns dokumenterade prestationsmål inom kontinuitetshantering som är länkade till kompensation *
18. Kontinuitetshantering är identifierat som en del av strategin. Detta visas genom att analyser av risk- och påverkansanalyser genomförs regelbundet * *Frekvensen visar hur viktigt detta är. Om företaget genomför analyser frekvent; välj en hög siffra*
19. Det finns en styrande kontinuitetskommitté vilken representerar organisationens samtliga avdelningar * *Om exempelvis hälften av företagets avdelningar finns representerade; Välj 50% - Uppfyller till hälften*
20. Företaget visar/har visat förbättrade resultat efter utvärderingar av kontinuitetshandlingen * *Välj en högre siffra om företaget visat stora förbättringar*
21. Majoriteten av organisationen deltar i kontinuitetshandlingen * *Om exempelvis hälften av företagets avdelningar deltar; Välj 50% - Uppfyller till hälften*
22. Det finns ett kompetensutvecklingsprogram för personalen som är ansvariga för företagets kontinuitetshantering * *Om ett sådant program är till hälften utvecklat; Välj 50% - Uppfyller till hälften*
23. Det finns krav på efterlevnad av företagets kontinuitetshantering vid kontraktutformningar med företagets intressenter (kunder, leverantörer osv) * *Om kravet gäller ett visst antal av kontrakt av totala antalet kontrakt - Välj motsvarande andel i ditt svar (Ex. 20% av alla kontrakt har detta krav)*

24. Det finns en successionsplan för ledning och VD * *En successionsplan innebär att företaget har ett formaliserat tillvägagångssätt vid överlämning mellan gamla och nya personer i ledning och för VD*
25. Kontinuitetshantering marknadsförs som en konkurrensfördel gentemot företagets intressenter (kunder, leverantörer, aktieägare osv) *
26. Kontinuitetshanteringens processer bidrar till strategisk utveckling *
27. Det finns metoder och verktyg som används för kontinuerlig utvärdering av kontinuitetsprogrammets effektivitet och lämplighet * *Om det finns några få metoder och verktyg; Välj en lägre siffra och vice versa*
28. Det finns ett översiktligt kontinuitetsprogram som sträcker sig över en flerårsperiod * *Ett kontinuitetsprogram syftar till att skapa en omfattande och effektiv kontinuitetshantering. Ett sådant program håller en mycket hög prioritering för ledningen*
29. Det finns en specifik enhet inom kontinuitetshantering som samarbetar nära andra avdelnings- och enhetschefer. * *Om enheten endast samarbetar med några få avdelningschefer - Välj en lägre siffra*
30. Externa intressenter (partners, leverantörer, kunder, myndigheter osv) deltar i gemensamma övningar av olika krisscenarion *
31. Övrigt att tillägga * *Har du övriga kommentarer eller funderingar kring ämnet, denna enkät eller tankar kring kontinuitetshantering?*

BILAGA 4 - Beräkningsexempel för mognadsnivå

För att räkna ut mognadsnivån för ett företag beräknas medeltalet av svaren för varje nivå (nedan visas resultatet för Banker på nivå 3):

	8. Det finns en gemensam terminologi inom kontinuitetshantering som används av samtliga avdelningar som är involverade i företagets kontinuitetshantering	9. Det finns ett styrprogram för avdelningar (vilka är involverade i kontinuitetshantering) som upprätthåller, åtminstone i begränsad utsträckning, efterlevnad gentemot gemensamma policys, standarder och "best practices" av företagets kontinuitetshantering.	10. Det finns ett träningsprogram som ökar medvetenheten av kontinuitetshantering för avdelningar som är involverade i företagets kontinuitetshantering	11. Det finns etablerade krav på återhämtningstider och återställningspunkter av kritiska funktioner vid inträffandet av en kris	
Kategori	Nivå 3	Nivå 3	Nivå 3	Nivå 3	Företagssnitt
Bank	6	6	5	4	5,25
Bank	0	0	2	5	1,75
Bank	9	2	2	9	5,5
Bank	8	8	5	7	7

Snitt:

Bank	5,75	4	3,50	6,25	4,88
------	------	---	------	------	------

Därefter beräknas genomsnittet för företagskategorin för varje nivå:

Kategori	Nivå 1	Nivå 2	Nivå 3	Nivå 4	Nivå 5	Nivå 6
Banker	10	6,71	4,88	5,85	4,59	3,75

För att underlätta för våra respondenter när det skulle besvara enkäten, valde vi att (i samråd med vår handledare) låta svarsalternativen vara mellan 0-10 istället för 0-100. Vi väljer dock i analysen att presentera svaren som procentsatser då det blir lättare att föra en diskussion då.

För att sedan räkna ut den genomsnittliga mognadsnivån, summeras genomsnittet från samtliga nivåer och divideras med högsta svarsalternativet (10). Detta ger följande mognadsnivå för Banker:

	Mognadsnivå
Banker	3,578

Förtydligande beräkningsexempel:
Om samtliga påståenden i alla nivåer besvaras med högsta svarsalternativet (10), skulle det summerande genomsnittet alltså bli 60 och mognadsnivån skulle således då bli 6