FSPOS

Finansiella Sektorns Privat-Offentliga Samverkan

Organisatorisk resiliens

- En överblick

2022-01-26

FSPOS Arbetsgrupp Kunskapsspridning

Innehållsförteckning

1. Inledning

Att den finansiella sektorn är resilient är en förutsättning för finansiell stabilitet och för ett väl fungerande och robust samhälle. Sektorns resiliens bygger i många avseenden på respektive aktörs enskilda förmåga att upprätthålla sin verksamhet vid oväntade händelser. Ömsesidiga beroenden dessa aktörer emellan innebär vidare att en allvarlig störning hos en eller flera aktörer kan sprida sig till övriga delar av det finansiella systemet, med potentiellt förödande konsekvenser för samhället i stort.

Digitaliseringen av den finansiella sektorn, fortsatt globalisering och ett försämrat säkerhetsläge ställer allt högre krav på resiliens. Pandemin och den senaste tidens cyberangrepp är tydliga exempel på vikten av att organisationer besitter en förmåga att anpassa sig till nya utmaningar. Som ett svar på denna utveckling har tillsynsmyndigheter och andra aktörer inlett ett arbete med att ge förslag på nya krav i syfte att stärka sektorns förmåga att hantera oväntade händelser som kan hota finansiell stabilitet. Detta går under samlingsnamnet organisatorisk resiliens.

Denna promemoria beskriver begreppet organisatorisk resiliens (på engelska *operational resilience*) och hur det relaterar till befintligt beredskapsarbete inom finansiell sektor. Promemorian riktar sig till samtliga organisationer inom finansiell sektor inom ramen för FSPOS gemensamma arbete.

Syfte

Syftet med denna promemoria är att beskriva begreppet organisatorisk resiliens och hur det relaterar till befintligt beredskapsarbete inom finansiell sektor, samt att tydliggöra kopplingen mellan organisatorisk resiliens och discipliner som skapar förutsättningar för en robust organisation. Till dessa hör exempelvis intern styrning och kontroll, bolagsstyrning, risk-, kris- och kontinuitetshantering samt informationssäkerhet.

Mål

Målet med denna promemoria är att skapa en gemensam grund och förståelse för hur organisatorisk resiliens relaterar till finansiella sektorns befintliga beredskapsarbete. Detta genom att överblicka befintliga och kommande vägledningar, standarder och regelverk på området samt reflektera över hur dessa kan komma att påverka finansiell sektor i Sverige. Promemorian ska även kunna användas som ett ingångsvärde för kommande FSPOS-aktiviteter inom området.

Metod

Metoden för framtagandet av denna promemoria består av en analys av befintliga publikationer på området organisatorisk resiliens så som vägledningar, standarder och regelverk.

Användning av begrepp i promemorian

Med begreppet organisatorisk resiliens menas i denna promemoria det engelska begreppet "*Operational Resilience*". Det finns för närvarande ingen entydig översättning av begreppet. Promemorian har gjort valet att använda begreppet *organisatorisk resiliens* utifrån ISO Standarden – 22316 - Säkerhet och resiliens - Organisatorisk resiliens – Principer.[1]

Avgränsningar

Denna promemoria är ej ämnad att utgöra ett metodstöd i hur en organisation bygger organisatorisk resiliens. Dokumentet bör istället ses som ett första steg i en analys av begreppet. Litteraturen är för närvarande begränsad och lagstiftare och andra vägledande aktörer inkluderar olika komponenter bakom definitionen av resiliens, detta beroende på vad som önskas åstadkommas. Analysen i denna promemoria har därav begränsats till Baselkommitténs principer om organisatorisk resiliens[2], ISO-standarden 22316[3], Storbritanniens nyligen antagna reglering om organisatorisk resiliens[4], samt EU Kommissionens förslag till förordning om digital operativ motståndskraft i den finansiella sektorn (DORA)[5]. Att notera är att promemorian inte redogör för dessa vägledningar, standarder eller regelverk i sin helhet, utan avser endast beskriva kärnan av vad som önskas åstadkommas samt genom vilka medel. På EU-nivå finns flertalet regelverk och riktlinjer utfärdade av bland andra EBA, EIOPA och ESMA som, när de har implementerats, ökar graden av organisatorisk resiliens. Detta går dock att säga om merparten av regelverken som åligger finansiell sektor, varpå dessa inte kommer att behandlas närmare inom denna promemoria.

---

[1] Svensk Standard – SS-ISO 22316:2020 - Säkerhet och resiliens - Organisatorisk resiliens – Principer.

[2] Basel Committee on Banking Supervision - Consultative Document: Principles for operational resilience - August 2020.

[3] Svensk Standard – SS-ISO 22316:2020 - Säkerhet och resiliens - Organisatorisk resiliens – Principer.

[4] PRA CP29/19: Operational resilience: impact tolerances for important business services, FCA CP19/32: Building operational resilience: impact tolerances for important business services and feedback to DP18/04, Bank CP Operational Resilience: Central counterparties, Bank CP Operational Resilience: Central securities depositories and Bank CP Operational Resilience: Recognised Payment Systems and Specified Service providers.

[5] Europaparlamentets och Rådets förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014.

2. Vad är organisatorisk resiliens?

I följande kapitel redogörs för hur begreppet organisatorisk resiliens definieras av olika vägledande aktörer samt vad som i slutändan förväntas åstadkommas med den regulatoriska utvecklingen.

Begreppet organisatorisk resiliens har under de senaste åren blivit allt mer förekommande i publicerade konsultationer samt förslag på regleringar och krav ämnade till att stärka sektorns förmåga att hantera oväntade händelser. Begreppet som sådant är inte nytt och kan ses som en beskrivning av, på ett eller annat sätt, förmågan att stå emot och klara av en förändring, samt återhämta sig och vidareutvecklas.[6] Ur ett beredskapsperspektiv är begreppet nära förknippat med vad ett samordnat risk-, kris- och kontinuitetshantersarbete syftar till.

Baselkommittén är ett exempel på en aktör som under de senaste åren har arbetat vidare med att beskriva organisatorisk resiliens. I "*Principles for Operational Resilience*" definieras organisatorisk resiliens som bankers förmåga att upprätthålla kritisk verksamhet under ett avbrott. Denna förmåga menar Kommittén skapar *förutsättningar för aktörer att identifiera och skydda sig mot hot och eventuella störningar, att kunna hantera och anpassa sig till, samt återhämta och lära sig av inträffade händelser*.[7] För att stärka en organisations resiliens förespråkar kommittén ett principbaserat tillvägagångssätt med grund i tidigare publicerade principer om god hantering av operativa risker, bolagsstyrning, outsourcing, kontinuitetshantering och vägledningar inom riskhantering.

Internationella standardiseringsorganisationen (ISO) har utarbetat en internationell standard om organisatorisk resiliens. Organisatorisk resiliens definieras i standarden som en *organisations förmåga att ta till sig och anpassa sig till en föränderlig miljö så att den når sina målsättningar, säkrar sin fortsätta existens samt har framgång*. Likt Baselkommitténs vägledning fastställer standarden principer för organisatorisk resiliens och presenterar egenskaper samt aktiviteter som tillsammans stärker en organisations resiliens. Resiliens ses här som *resultatet av en god verksamhet och en effektiv riskhantering*, som *påverkas av ett unikt samspel mellan samt en kombination av strategiska och operativa faktorer*. [8] Som exempel på faktorer kan nämnas förekomsten av en kultur som förespråkar resiliens eller förekomsten av samordnande och ändamålsenliga ledningsprinciper (exempelvis risk-, kris- och kontinuitetshantering).

Andra aktörer som tidigt arbetat med organisatorisk resiliens är de brittiska tillsynsmyndigheterna Bank of England, Financial Conduct Authority och Prudential Regulation Authority som i nära samarbete med landets finansiella sektor var först ut i Europa med att föreslå ett nytt regelverk på området. Myndigheterna definierar organisatorisk resiliens som *finansinstitut, infrastrukturleverantörer och sektorns förmåga att förebygga, anpassa sig till, hantera, återhämta sig och lära sig av driftavbrott*.[9] Utgångspunkten, enligt ovan aktörer, är att allvarliga störningar kommer att inträffa, vilket kan resultera i stora konsekvenser för slutkonsumenter, finansmarknader och det finansiella systemet som sådant. Organisationer behöver därför planera därefter.

---

[6] MSB - Resiliens: begreppets olika betydelser och användningsområden - Publikationsnummer MSB569 – 2013.

[7] Basel Committee on Banking Supervision - Consultative Document: Principles for operational resilience - August 2020.

[8] Svensk Standard – SS-ISO 22316:2020 - Säkerhet och resiliens - Organisatorisk resiliens – Principer.

[9] Bank of England, Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA) - Discussion Paper: Building the UK financial sector's operational resilience.

Det traditionella synsättet och inställningen som präglat den finansiella sektorn har varit att allvarliga störningar inte ska kunna inträffa, vilket inte längre kan anses tillräckligt. Regelverket innebär ett skifte då den egna verksamhetens överlevnad inte längre står i fokus för beredskapsarbetet. Att upprätthålla enskilda processer blir på så sätt mindre intressant och ersätts i regelverket med att upprätthålla tillhandahållandet av viktiga produkter och tjänster (*Important Business Services*), detta ur ett konsumentperspektiv. Myndigheterna ämnar på så sätt att åstadkomma en förändring där aktörer kontinuerligt och på ett mångfacetterat sätt arbetar med att säkerställa en hög förmåga att leverera de produkter och tjänster som samhället är beroende av, när oväntade störningar väl inträffar. [10]

Såväl Baselkommittén som de brittiska tillsynsmyndigheterna nämner cyberhot som ett relevant område för arbetet med organisatorisk resiliens, men är samtidigt tydliga med att andra risker likväl ska kunna hanteras. Europeiska kommissionen har valt att inleda resan mot en mer robust finansiell sektor genom att fokusera på digital resiliens. I sitt förslag till en förordning om digital operativ motståndskraft i den finansiella sektorn (DORA-förordningen) definieras detta som *finansiella företags förmåga att tillförsäkra operativ integritet ur ett tekniskt perspektiv för att säkerheten i nätverk och informationssystem ska kunna upprätthållas*.[11] Definitionen särskiljer sig markant från ovan nämnda definitioner, och så av naturliga skäl. Kommissionen ämnar åstadkomma en stärkt förmåga att hantera informations- och kommunikationsrelaterade störningar och hot i den finansiella sektorn genom att harmonisera nuvarande reglering på området. I förordningen återfinns krav på styrning, riskhantering, rapportering och testning samt en tillsynsram för leverantörer av IKT-tjänster som traditionellt sett inte hamnat under myndigheternas tillsyn.

Utifrån ovan definitioner och resonemang kommer organisatorisk resiliens fortsättningsvis i denna promemoria att beskrivas som *resultatet* av ett integrerat beredskapsarbete som sträcker sig över samtliga berörda beredskapsdiscipliner och genomsyrar hela organisationen, där ägandeskapet på ett tydligt sätt ligger på ledningsnivå. Skiftet är viktigt – när fokus ligger på *resultat* istället för *regeluppfyllnad*, så tillkommer en högre grad av flexibilitet där organisationer på ett mer effektivt sätt kan anpassa sig i en konstant föränderlig miljö. Kommissionens syn på organisatorisk resiliens särskiljer sig i och med ovan diskuterat syfte och ämnar inte på samma sätt åstadkomma ett skifte i tankesätt eller en hög grad av flexibilitet. Samtidigt delar ovan aktörer många grundläggande principer om hur organisatorisk resiliens ska uppnås genom verksamhetsstyrning, testning och riskhantering.

Operational resilience (…) is an outcome. It is a step change, where we expect you to be forward looking and making decisions today that help prevent harm tomorrow.[12]

[10] Financial Conduct Authority - The view from the regulator on Operational Resilience - Speech by Megan Butler, Executive Director of Supervision.

[11] Regeringskansliet - Faktapromemoria 2020/21: FPM16 - Förordning om digital operativ motståndskraft i den finansiella sektorn.

[12] Financial Conduct Authority - The view from the regulator on Operational Resilience - Speech by Megan Butler, Executive Director of Supervision.

3. Kopplingen mellan organisatorisk resiliens och befintligt beredskapsarbete

Organisatorisk resiliens kan enligt ovan sammanfattas som resultatet av ett integrerat, systematiskt och strukturerat arbete inom ett flertal discipliner med syfte att bygga en robust organisation.

En sådan disciplin är intern styrning och kontroll. Ägandeskapet för verksamhetens organisatoriska resiliens bör ligga på styrelse- och ledningsnivå, ett tydligt krav i samtliga ovan diskuterade regelverk. Finansinspektionen föreskriver att företag ska ha en dokumenterad riskstrategi och förespråkar även en strategi för kontinuitetshantering. Strategier är ett viktigt verktyg för att i rimlig grad *säkerställa att bankens riskexponering är i linje med den fastställda riskaptiten*[13] och som samtidigt ger verksamheten en tydlig bild av önskad förmåga. Den interna styrningen behöver vidareutvecklas för att även inkludera en strategi för organisatorisk resiliens enligt samma struktur. Styrelsens och ledningens godkännande och engagemang kan tillika ses som en förutsättning för att åstadkomma en företagskultur som präglas av resiliens. Interna kontrollmekanismer kommer som ett resultat av detta att behöva inkludera nya funktioner och processer i syfte att säkerställa att arbetet bedrivs på ett ändamålsenligt och effektivt sätt.

Nära besläktad med ovan disciplin är bolagsstyrning som utgör en viktig komponent i beredskapsarbetet. Tydliga roller och ansvar samt delegering till såväl ämnesansvariga som operativt ansvariga i verksamheten skapar goda förutsättningar för förmåga och regelefterlevnad. En vanlig förekommande utmaning är dock att åstadkomma ett samordnat och integrerat arbetssätt - en förutsättning för organisatorisk resiliens. En tydlig bolagsstyrning som förhindrar silostrukturer är en förutsättning för organisatorisk resiliens. Uppkomsten av befattningen *Resilience Manager* med ett samlat ansvar för strategiska och taktiska resiliensfrågor är ett exempel på hur detta har hanterats internationellt.

Befintligt arbete med risk-, kris- och kontinuitetshantering får likt ovan discipliner ny innebörd. För att säkerställa en integrerad och välfungerande beredskapskedja behöver resultatet av det ena på ett tydligt sätt födas in och tas om hand i det andra, vilket bland annat förutsätter funktioner samt processer för informationsdelning, kunskapsöverföring och samverkan. Att som organisation kunna anpassa sig till nya utmaningar ställer exempelvis krav på förmågan att förutse och hantera förändringar i risklandskapet. Arbetet med riskhantering blir som ett resultat av detta mer omfattande och behöver involvera fler perspektiv. Risker med låg sannolikhet men hög konsekvens behöver i större utsträckning tas om hand och samverkan med, samt övervakning av kritiska tredjepartsleverantörer behöver förstärkas. Systematiska uppdateringar i riskbedömningar får i sin tur konsekvenser på arbetet med kontinuitetshantering där befintliga kontinuitetslösningar följdriktigt behöver utvärderas. Coronapandemin är ett tydligt exempel på händelse där en snabb förändring i risklandskapet med brutna leveranskedjor, smittspridning och en snabb omställning till hemarbete kommit att ställa nya krav på befintliga lösningar, i synnerhet ur ett tidsperspektiv.

[13] Finansinspektionen - FI-tillsyn - Bankernas kontinuitetshantering - Nr 18 - 9 juni 2020.

Digitaliseringen av den finansiella sektorn och det växande cyberhotet innebär att informationssäkerhet utgör ytterligare en viktig disciplin för skapandet av organisatorisk resiliens. Likt ovan förändringar i arbetssätt och metodik förutsätter en resilient organisation ett systematiskt informationssäkerhetsarbete med avstamp i en tydlig strategi, där man som organisation arbetar förebyggande och i synergi med övriga discipliner, samt där skyddet anpassas kontinuerligt utifrån identifierade behov.

Befintlig ISO-standard om organisatorisk resiliens sammanfattar ovan diskussion väl:

Det finns inte ett enskilt tillvägagångssätt för att stärka en organisations resiliens. Det finns etablerade ledningsdiscipliner som gemensamt bidrar till resiliens, men var och en för sig räcker de inte för att garantera en organisations resiliens. Organisatorisk resiliens är resultatet av ett samspel mellan egenskaper och aktiviteter, och av bidrag från annan teknisk och vetenskaplig expertis.[14]

[14] Svensk Standard – SS-ISO 22316:2020 - Säkerhet och resiliens - Organisatorisk resiliens – Principer.

4. Avslutande reflektioner

Efter en överblick av befintliga och kommande vägledningar, standarder och regelverk inom organisatorisk resiliens kan konstateras att det inte finns en entydig syn på begreppet, eller hur organisationer uppnår en viss grad av resiliens. Men genom närmare analys av syfte och mål kan utrönas att organisatorisk resiliens är resultatet av ett integrerat beredskapsarbete som sträcker sig över flera olika discipliner, genomsyrar hela organisationen, där ägandeskapet på ett tydligt sätt åligger organisationers toppskikt.

Hur den regulatoriska utvecklingen kan komma att påverka beredskapsarbetet i den svenska finansiella sektorn är för närvarande svårt att förutsäga. Kommande DORA-förordning ligger närmast i tiden och förväntas harmonisera nuvarande reglering på IKT-området. Förordningen som sådan ställer långtgående krav på finansiella företag och kommer att innebära en stor förändring i hur beredskapsarbete bedrivs inom ett specifikt område, men innebär samtidigt inte ett skifte i tankesätt likt det som de brittiska tillsynsmyndigheterna ämnar åstadkomma.

Ett snabbt föränderligt risklandskap och lagstiftares motreaktion under de senaste åren kan dock ses som ett tydligt tecken på att fler regleringar är att vänta. Flera av de förbättringsbehov som Finansinspektionen har identifierat avseende bankers kontinuitetshantering, så som styrning och kontroll, tester och rapportering[15] kan möjligen hanteras genom ovan diskuterade regelverk och principer. Ett bra första steg för en aktör inom finansiell sektor bör vara att redan nu börja förbereda sig på vad detta skulle kunna innebära för den egna organisationen. För att identifiera gap i befintlig resiliens ställer ovan diskuterade regelverk krav på mer komplex övningsverksamhet med scenarion som utmanar hela beredskapskedjan. Värt att notera är att det redan nu finns många goda exempel på sådana aktiviter hos aktörer inom finansiell sektor. Vidare kommer ett systematiskt och strukturerat arbete med bland annat kontinuitetshantering, riskhantering (inkl. tredjepartsrisker) och förmågeutveckling tillsammans med ledningens godkännande och engagemang i form av mandat, stöd och resurstilldelning bädda för en allt mer resilient organisation.

[15] Finansinspektionen - FI-tillsyn - Bankernas kontinuitetshantering - Nr 18 - 9 juni 2020.