FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Regelverk för kontinuitet i it-verksamhet

– Beskrivning av innehåll och tillämpning

2020-12-15
FSPOS Arbetsgrupp Analys

1 Inledning

I denna rapport beskrivs innehåll och tillämpning av utvalda regelverk för kontinuitet i it-verksamheten hos aktörer i den finansiella sektorn. Arbetet med kontinuitet och operativ förmåga[1] inom finansiell sektor är under snabb utveckling och nya regelverk är under utarbetning. Innehållet i denna rapport utgör därmed en beskrivning av de regelverk som bedöms som mest relevanta vid tidpunkten för publicering.

Krav på kontinuitet i it-verksamheten måste alltid utgå från verksamhetens strategi, mål och kravställningar, dvs. hur it-verksamheten ska utformas för att möta verksamhetens krav på kontinuitet och operativ förmåga.

Rapporten beskriver olika krav och områden som påverkar it-verksamhetens arbete med kontinuitet, men gör inte anspråk på att vara heltäckande. Rapporten kan användas i valda delar som ett komplement och stöd i organisationens arbete med kontinuitet i it-verksamheten.

Rapporten riktar sig till personer som ansvarar för eller på annat sätt arbetar med kontinuitet i organisationen.

För information om hur verksamheten praktiskt kan arbeta med kontinuitet i it-verksamheten hänvisas till *FSPOS Vägledning för kontinuitetshantering, Appendix F – Kontinuitetshantering för IT-verksamheten*. Denna rapport utgör inte ett komplement till vägledningen utan kan läsas fristående.

1.1 Syfte och mål

Syftet med denna rapport är att beskriva innehåll och tillämpning av regelverk som berör kontinuitetshantering i it-verksamheten hos aktörer i den finansiella sektorn. Målet är att rapporten kan användas av sektorns aktörer som ett stöd i det egna arbetet med kontinuitet i it-verksamheten.

För att uppnå detta mål har i huvudsak tre frågeställningar behandlats i rapporten; *hur*, *när* och *varför* aktörerna i den finansiella sektorn tillämpar utvalda regelverk i it-verksamhetens kontinuitetsarbete. Genom dessa frågeställningar kan läsaren av rapporten dels avgöra viktiga kravställningars relevans för tillämpning i den egna organisationen, dels dra nytta av andra aktörers erfarenheter av praktisk tillämpning inom området.

---

[1] *I text på engelska används ofta begreppet "operational resilience".*

1.2 Metod och avgränsningar

Metoden för framtagandet av denna rapport innefattar två huvudsakliga delar:

1. beskrivning av regelverk
2. praktisk tillämpning av regelverk genom intervjustudie med utvalda representanter från den finansiella sektorn.

1.2.1 Beskrivning av regelverk

Initialt sammanställdes en bruttolista över regelverk som berör området kontinuitet. Fokus vid urvalet har varit regelverk där kravställningarna direkt berör it-verksamheten och där krav på verksamhetens kontinuitetsarbete har en tydlig koppling till hur it-verksamheten ska utformas för att möta dessa krav.

De regelverk som valts ut har grupperats utifrån antingen utställare eller tillämpningsområde. Denna gruppering har använts genomgående i både kartläggning och intervjustudie i syfte att förse läsaren med en god överblick för att möjliggöra snabb orientering i materialet. I nästa steg har kraven i regelverken som direkt eller indirekt har en anknytning till kontinuitet i it-verksamheten beskrivits.

1.2.2 Praktisk tillämpning av regelverk

En intervjustudie har genomförts för att erhålla kunskap om hur aktörer i den finansiella sektorn tillämpar de utvalda regelverken med syfte att skapa praktisk vägledning för andra aktörer som berörs av dessa. För att studien ska vara relevant för så många organisationer som möjligt, representerar de intervjuade personerna aktörer med olika verksamhetsområden.

1.2.3 Avgränsningar

Då flertalet av de utvalda regelverken är omfattande, har beskrivningarna avgränsats till krav som direkt eller indirekt har anknytning till kontinuitet i it-verksamheten. Övriga krav har utelämnats i kartläggningen av regelverken.

En annan avgränsning är att rapporten inte går på djupet i beskrivningen av olika kontinuitetslösningar för it-verksamheten, exempelvis vid utkontraktering eller tekniska lösningar. Fokus i beskrivningarna ligger på innehållet i regelverken och tillämpningen av dessa. Detta innebär inte att specifika kontinuitetslösningar för it-verksamheten saknar relevans för området, men dessa kräver en mer omfattande beskrivning.

Antal genomförda intervjuer är få, varför resultatet av dessa ska ses som exempel på hur regelverk tillämpas inom några olika verksamhetsområden.

1.2.4 Användning av begrepp i rapporten

Krav på kontinuitet i it-verksamheten måste alltid utgå från verksamhetens strategi, mål och kravställningar. Med ”kontinuitet i it-verksamheten” avses i denna rapport metoder och processer för utformning och styrning av it-miljön som syftar till att skapa robusthet och redundans i it-verksamhetens kritiska system och tjänster.

Genom verksamhetens generella kontinuitetsarbete identifieras organisationens kritiska processer, samt de aktiviteter och resurser som krävs för att de kritiska processerna ska kunna upprätthållas. It-system och andra it-relaterade resurser utgör ofta kritiska stödresurser till finansiella aktörers kritiska processer. De tids- och informationssäkerhetskrav som verksamheten definierat för dessa resurser utgör viktiga ingångsvärden för it-verksamhetens kontinuitetsarbete.

I *FSPOS Vägledning för kontinuitetshantering, Appendix F – Kontinuitetshantering för IT-verksamheten* finns ett antal centrala begrepp inom kontinuitetsområdet beskrivna, samt en beskrivning av hur verksamhetens generella kontinuitetsarbete förhåller sig till it-verksamhetens arbete med kontinuitet.

För att förenkla används ordet ”regelverk” i denna rapport för att beskriva gruppen av regelverk, riktlinjer, föreskrifter, standarder, ramverk och ledningssystem.

2 Beskrivning av regelverk

I följande kapitel beskrivs de regelverk för kontinuitet i it-verksamhet som har valts ut. Regelverken presenteras gruppvis och besvarar frågor som: syfte med regelverken, vilka som berörs av regelverken, hur och varför de ska tillämpas samt vilka krav på kontinuitet i it-verksamheten som ställs, explicit eller implicit, i regelverken.

2.1 EBA guidelines

European Banking Authority (EBA), på svenska: Europeiska bankmyndigheten, är en oberoende tillsynsmyndighet i EU och har som främsta uppgift att bidra till upprättandet av harmoniserade regler för bankverksamhet i Europa, genom att anta bindande tekniska standarder och riktlinjer. Syftet med de gemensamma reglerna är att bidra till att skapa rättvisa förhållanden och ge insättare, investerare och konsumenter ett gott skydd.

I denna rapport har två av EBA:s riktlinjer valts ut:

- Guidelines on outsourcing arrangements (EBA/GL/2019/02)[2]
- Guidelines on ICT and security risk management (EBA/GL/2019/04)[3]

För vilka gäller riktlinjerna?

Riktlinjerna gäller för kreditinstitut, värdepappersföretag, betalningsinstitut och institut för elektroniska pengar inom EU. Finansinspektionen anser även att *Guidelines on outsourcing arrangements* kan fungera som god vägledning för alla slags företag inom finanssektorn – oavsett företagstyp: bank, kreditinstitut, betalningsinstitut, marknadsinfrastrukturbolag, försäkringsföretag[4].

[2] *Riktlinjen finns översatt till svenska: Riktlinjer för utkontraktering (EBA/GL/2019/02).*

[3] *Riktlinjen finns översatt till svenska: Riktlinjer för hantering av IKT-risker och säkerhetsrisker (EBA/GL/2019/04).*

[4] *https://www.fi.se/sv/bank/utlagd-verksamhet/*

Hur ska riktlinjerna tillämpas?

Finansinspektionen följer EBA:s riktlinjer och genomför tillsyn på de företag som omfattas av riktlinjerna[5,6]. Finansinspektionens uppfattning är att riktlinjer från EBA är likvärdiga med svenska allmänna råd. Företag ska därför "med alla tillgängliga medel söka följa riktlinjerna" enligt förordning (EU) nr 1093/2010. Riktlinjerna kan även användas i Finansinspektionens tillsynsaktiviteter.

Guidelines on outsourcing arrangements innehåller krav på interna styrningsarrangemang och riskhantering vid utkontraktering. Omfattas gör alla avtal som ingås eller revideras på eller efter det datum som riktlinjerna trädde i kraft. Finansiella företag bör uppdatera och revidera existerande avtal för att säkerställa att de efterlever de nya riktlinjerna.

Guidelines on ICT and security risk management innehåller krav på informationssäkerhet, inklusive cybersäkerhet, i den mån informationen förvaras i it-system.

Varför ska riktlinjerna tillämpas?

Genom att tillämpa EBA:s riktlinjer bidrar finansiella företag till att möta myndighetens övergripande mål att upprätthålla stabiliteten i det finansiella systemet inom EU samt att skydda banksektorns integritet, effektivitet och korrekta funktion.

2.1.1 Guidelines on outsourcing arrangements

Riktlinjerna syftar dels till att ge en tydlig definition av utkontraktering. Vidare anges kriterier för bedömning av huruvida utkontrakterad verksamhet (aktiviteter, tjänster, processer eller funktioner) är kritisk eller ej, och därigenom vilken påverkan den har på den finansiella aktörens riskprofil eller interna kontrollramverk. Riktlinjerna har varit gällande sedan 30 september 2019.

Vilka krav på kontinuitet ställs?

Riktlinjerna är indelade i ett antal kapitel med olika nyckelteman. I varje kapitel finns krav med kopplingar till kontinuitet utifrån ett flertal viktiga aspekter som alla knyter an specifikt till utkontraktering.

---

[5] *https://www.fi.se/sv/publicerat/nyheter/2019/fi-tillampar-riktlinjer-for-utkontraktering/*

[6] *https://www.fi.se/sv/publicerat/nyheter/2020/fi-tillampar-riktlinjer-for-hantering-av-ikt--och-sakerhetsrisker/*

Proportionalitet

Företag som tillämpar riktlinjerna bör beakta proportionalitetsprincipen som innebär att styrning av utkontraktering ska motsvara den individuella riskprofilen, affärsmodellen och verksamhetens komplexitet.

Proportionalitetsprincipen omfattar även styrningen av kontinuitet i verksamheten. När företagen tillämpar de krav som berör kontinuitet bör de ta hänsyn till de utkontrakterade funktionernas komplexitet, de risker som uppkommer genom utkontrakteringslösningen, hur kritisk eller viktig den utkontrakterade funktionen är samt hur utkontrakteringen potentiellt kan inverka på kontinuiteten i verksamheten.

Bedömning av utkontrakterad verksamhet

Företag som tillämpar riktlinjerna bör fastställa om ett avtal med en tredje part omfattas av definitionen för utkontraktering. När ett arrangemang med en tjänsteleverantör omfattar flera olika funktioner, bör företagen beakta alla aspekter av lösningen i sin bedömning. Vidare bör företag även bedöma huruvida en utkontrakteringslösning gäller en funktion som är kritisk eller viktig för verksamheten.

Ur ett kontinuitetsperspektiv innebär detta att samtliga aspekter som berör styrning och drift av kontinuitetslösningar behöver beaktas samlat. Om tjänsteleverantören exempelvis tillhandahåller maskinvara för datalagring och säkerhetskopiering av uppgifter, bör båda tjänsterna beaktas som en helhet då kontinuitetsarbetet innefattar samtliga aspekter av tjänsteleveransen.

Ramverk för styrning

Företaget bör ha ett heltäckande ramverk för riskhantering som sträcker sig över alla affärsområden och interna enheter. Under denna ram bör företaget identifiera och hantera alla risker, inbegripet risker som orsakas av arrangemang med tredje parter. Vidare bör företaget

- ha en väl definierad styrning med tydliga ansvarsområden för utkontraktering
- upprätta samt regelbundet granska och uppdatera en skriftlig policy för utkontraktering och säkerställa att den genomförs
- bedöma och hantera intressekonflikter som berör dess utkontrakteringslösningar
- upprätthålla och regelbundet pröva lämpliga kontinuitetsplaner när det gäller utkontrakterade kritiska eller viktiga funktioner

- genomföra oberoende granskning av utkontrakterad verksamhet genom internrevision
- på lämpligt sätt dokumentera alla aktuella utkontrakteringslösningar.

Företaget bör även ha regelbundet testade kontinuitetsplaner på plats avseende utkontrakterade kritiska funktioner.

Detta innebär att företaget bör ha ett heltäckande ramverk för kontinuitet som inbegriper identifiering och hantering av alla risker kopplade till utkontraktering i verksamheten och it-verksamheten.

Utkontrakteringsprocessen

Innan ett företag inleder arbetet med en utkontrakteringslösning bör det göra följande:

- bedöma kritisk eller viktig funktion
- bedöma tillsynsvillkoren
- identifiera och bedöma alla relevanta risker
- genomföra företagsbesiktning av den blivande tjänsteleverantören
- identifiera och bedöma intressekonflikter.

I kontraktsfasen ska tjänsteleverantörens rättigheter och skyldigheter tydligt klargöras och fastställas i ett skriftligt avtal. I avtalet bör anges huruvida det är tillåtet att vidare utkontraktera kritiska eller viktiga funktioner, eller väsentliga delar av dem.

Företaget bör även säkerställa att:

- tjänsteleverantörer, när det är relevant, följer lämpliga it-säkerhetsstandarder
- internrevisionsfunktionen kan granska den utkontrakterade funktionen genom ett riskbaserat arbetssätt
- utkontrakteringslösningen uttryckligen tillåter möjligheten för företaget att säga upp lösningen.

Företaget bör även fortlöpande övervaka tjänsteleverantörernas resultat med ett riskbaserat arbetssätt i syfte att säkerställa tillgänglighet, integritet och säkerhet för uppgifter och information. Slutligen bör företaget ha en dokumenterad utträdesstrategi vid utkontraktering av kritiska eller viktiga funktioner.

Det är viktigt att beakta samtliga aspekter av kontinuitetshantering genom hela utkontrakteringsprocessen. Särskilt viktig är företagsbesiktningen där analysen

bör innefatta tjänsteleverantörens hantering av tillgänglighet och möjlighet för återställning av kritiska system och tjänster. I riskanalysen är det viktigt att identifiera risker förknippade med tjänsteleverantörens hantering och lagring av information samt hur *konfidentialitet*, *riktighet* och *tillgänglighet* för informationen kan säkerställas under alla omständigheter (dvs. alla former av it-relaterade incidenter, inklusive större haverier som kräver återställning av system och tjänster). Detta blir av särskild vikt om tjänsteleverantören i sin tur utkontrakterar delar av tjänsten vidare. Även fysisk plats för serverhallar och lagring av information är av central betydelse för riskanalysen.

Under kontraktsfasen är det viktigt att kontinuitetskraven prioriteras och att leverantörsavtalet omfattar hantering av allvarliga it-relaterade incidenter, inklusive större haverier som kräver återställning av system och tjänster. Även om så kallade standardavtal är relativt vanliga vid utkontraktering bör företaget säkerställa att samtliga krav på kontinuitet finns med i leverantörsavtalet. Särskilt viktigt att beakta är roller och ansvar samt servicenivåer förknippade med återställning av system och tjänster. Andra viktiga aspekter är upprättande av en leverantörsstyrning som omfattar alla kontinuitetskrav samt företagets åtkomst- och revisionsrättigheter gällande tjänsteleverantörens kontinuitetslösningar.

2.1.2 Guidelines on ICT and security risk management

Riktlinjerna syftar till att precisera de riskhanteringsåtgärder som finansinstitut ska vidta för att hantera sina it- och säkerhetsrisker och som ska vidtas av betaltjänstleverantörer i enlighet med PSD2. Dessa riktlinjer inkluderar krav på informationssäkerhet, inklusive cybersäkerhet, i den mån informationen förvaras i it-system. Riktlinjerna har varit gällande sedan 30 juni 2020.

Vilka krav på kontinuitet ställs?

Riktlinjerna omfattar många olika aspekter av kontinuitet, exempelvis inom närliggande områden såsom styrning, organisation, identifiering och klassificering av kritiska funktioner, processer och tillgångar, och även riskhantering, rapportering, revision, etc. Några andra viktiga områden som behandlas är informationssäkerhet och fysisk säkerhet. Riktlinjerna fokuserar särskilt på riskhantering genom att integrera det operativa riskarbetet gentemot nyss nämnda områden.

Proportionalitet

Alla finansinstitut ska efterleva bestämmelserna i dessa riktlinjer på ett sätt som är proportionerligt mot finansinstitutets storlek, interna organisation samt

karaktären, omfattningen, komplexiteten och risknivån på verksamheten. Ur ett kontinuitetsperspektiv innebär detta att tillämpningen av kraven ska vara proportionerlig mot finansinstitutets individuella riskbild.

Strategi och ledning

Ledningsorganet ska tillse att

- finansinstitut har fastställt tillräcklig intern styrning och kontrollramverk
- personalstyrkan är tillräckligt stor och kompetent genom lämplig utbildning
- den tilldelade budgeten är lämplig för att uppfylla kraven
- finansinstitutets it-strategi är fastställd och godkänd för sina it- och säkerhetsrisker.

Vid utkontraktering ska finansinstitut tillse att avtal och servicenivåavtal (både för normala förhållanden och vid störningar i tjänsten) med leverantörer finns, samt kontrollera leverantörers efterlevnad av bl.a. finansinstitutets mål för säkerhet.

Ur ett kontinuitetsperspektiv innebär detta att

- finansinstitutet ska ha en heltäckande styrning och ramverk för kontinuitet
- nyckelpersoner som tilldelats en aktiv roll i kontinuitetsarbetet har fått tillbörlig utbildning och övrig personal har erhållit en allmän medvetenhetshöjande utbildning inom kontinuitet
- en budget finns allokerad för kontinuitetsarbetet
- en kontinuitetsstrategi är fastställd och godkänd av ledningen.

Vid utkontraktering är det viktigt att beakta samtliga kontinuitetsrelaterade aspekter genom hela utkontrakteringsprocessen (se *EBA Guidelines on outsourcing arrangements* för fler detaljer).

Ramverk för hantering av operativa risker och säkerhetsrisker

Finansinstitut bör identifiera och hantera sina it- och säkerhetsrisker genom fastställda ramverk, lämpliga processer och kontroller, samt tilldela ansvaret för hantering av dessa risker. Finansinstitut bör även kartlägga sina verksamhetsfunktioner, roller och stödprocesser för att identifiera inbördes beroenden avseende it- och säkerhetsrisker. Vidare bör samtliga informationstillgångar kartläggas och klassificeras. Finansinstitut bör därefter identifiera de it- och säkerhetsrisker som påverkar identifierade och

klassificerade verksamhetsfunktioner, stödprocesser och informationstillgångar utifrån dess kritikalitet. Med utgångspunkt i riskbedömningarna bör åtgärder fastställas för att reducera de identifierade riskerna. Riskbedömningens resultat bör därefter rapporteras till ledningsorganet. Finansinstitutets styrning, samt dess system och processer för it- och säkerhetsrisker ska periodiskt granskas genom revision.

Detta innebär att finansinstitutet bör ha ett heltäckande ramverk för kontinuitet, samt genomföra analys av it-verksamheten (aggregering av resurser identifierade av verksamheten, konsekvensanalys och riskbedömning) i enlighet med *FSPOS Vägledning för kontinuitetshantering, Appendix F – Kontinuitetshantering för IT-verksamheten*. Genom att kartlägga och klassificera samtliga informationstillgångar *innan* analys av it-verksamheten påbörjas erhåller verksamheten viktig kännedom om de tillgänglighetskrav och andra informationssäkerhetsrelaterade krav som gäller för informationstillgångarna. Detta resulterar i högre kvalitet på resultatet från analys av it-verksamheten. Se *MSB:s Metodstöd för systematiskt informationssäkerhetsarbete*[7] för en mer utförlig beskrivning av kartläggning och klassificering av informationstillgångar.

Informationssäkerhet

Finansinstitut bör utarbeta och dokumentera en informationssäkerhetspolicy som ska definiera principer och regler med hög kravnivå för att skydda konfidentialiteten, integriteten för, och tillgängligheten till, finansinstitutets och deras kunders data och information. Policyn ska bland annat inkludera en beskrivning av informationssäkerhetsledningens viktigaste roller och ansvarsområden. Med utgångspunkt i informationssäkerhetspolicyn bör finansinstitut ta fram och införa säkerhetsåtgärder för att reducera de it- och säkerhetsrisker som de utsätts för. Finansinstitut bör definiera, dokumentera och införa rutiner för

- logisk åtkomstkontroll (identitets- och åtkomsthantering)
- fysisk säkerhet (skydd av lokaler och datacentraler)
- säkerhet för it-verksamhet (förhindra säkerhetsincidenter i system och tjänster)
- säkerhetsövervakning (upptäcka avvikande aktiviteter som kan påverka finansinstituts informationssäkerhet)
- översyn, bedömning och test av informationssäkerhet.

[7] *https://www.informationssakerhet.se/metodstodet/*

Finansinstitut bör även ta fram ett utbildningsprogram för all personal och alla uppdragstagare för att säkerställa att kompetens finns för att genomföra de aktuella arbetsuppgifterna och skyldigheterna.

Finansinstitutets informationssäkerhetspolicy bör således innehålla ett avsnitt som beskriver principer och regler för kontinuitet i it-verksamheten. Detta bör beskriva hur konfidentialiteten, integriteten för, och tillgängligheten till, finansinstitutets system och tjänster bevaras under den dagliga driften samt vid allvarliga it-relaterade incidenter, inklusive större haverier som kräver återställning av system och tjänster. Även de roller som har ett ansvar inom kontinuitet i it-verksamheten bör beskrivas, som exempelvis kontinuitetsansvarig eller IT Service Continuity Manager. Med utgångspunkt i informationssäkerhetspolicyn bör finansinstitut ta fram och införa säkerhetsåtgärder kopplade till kontinuitet i it-verksamheten. Dessa åtgärder dokumenteras lämpligen som en del i övriga säkerhetsåtgärder inom informationssäkerhet. De rutiner som definieras, dokumenteras och införs enligt punktlistan i föregående stycke bör även beakta åtkomsthantering av backuper och fysiskt skydd av datacenter vid ett haveri. Utbildningsprogrammet bör säkerställa att all personal med ett ansvar för kontinuitet i it-verksamheten får lämplig utbildning för att kunna utföra sina arbetsuppgifter.

Hantering av it-verksamhet

Finansinstitut bör hantera sin it-verksamhet utifrån dokumenterade och införda processer och rutiner godkända av ledningen. Denna uppsättning av dokument ska definiera hur finansinstitut driver, övervakar och kontrollerar sina system och tjänster. Dessa processer och rutiner bör bland annat innefatta

- kapacitetshantering
- loggning och övervakning
- förteckning över it-tillgångar
- livscykelhantering för it-tillgångar
- säkerhetskopiering och återställande av data och it-system
- incident- och problemhantering.

Detta innebär att finansinstitutet bör dokumentera och införa processer för kontinuitet i it-verksamheten, samt identifiera beroenden gentemot övriga processer (enligt bland annat punktlistan ovan) och sammankoppla dessa. För att underlätta detta arbete rekommenderas finansinstitutet att införa och tillämpa ett standardiserat ramverk för hantering av it-verksamhet, exempelvis ITIL 2011, där samtliga nödvändiga processer och dess beroenden finns definierade. Det är även nödvändigt att definiera roller och ansvarsområden kopplade till dessa

processer och rutiner. Särskild vikt bör läggas vid incident- och problemhantering då dessa processer är helt avgörande för en fungerande hantering av störningar eller längre avbrott.

It-projektledning och ändringshantering

Finansinstitut bör utarbeta och införa en process som styr anskaffning, utveckling och underhåll av system och tjänster. Denna process ska planeras med hjälp av en riskbaserad metod. Ett finansinstitut bör bland annat tillse att

- de funktionella och icke-funktionella kraven är tydligt definierade och godkända
- en fastställd metodik finns för test och godkännande av it-system före första användning
- testa it-system och åtgärder för informationssäkerhet
- införa separata it-miljöer för test och produktion
- införa åtgärder för att skydda integriteten av källkoder för internt utvecklade it-system
- processer finns för anskaffning och utveckling av it-system.

Finansinstitut bör även ta fram och införa en process för ändringshantering för att säkerställa att alla ändringar i system och tjänster registreras, testas, bedöms, godkänns, införs och verifieras på ett kontrollerat sätt.

Finansinstitut bör således säkerställa att arbetet med kontinuitet i it-verksamheten är integrerat med processen som styr anskaffning, utveckling och underhåll av system och tjänster. Särskilt viktigt är att verksamheten definierar krav på tillgänglighet, kapacitet, mål för återställningstid (RTO)[8] och mål för återhämtningspunkt (RPO)[9]. Metodiken för test och godkännande av system och tjänster ska beakta kontinuitetskraven och genomförda tester ska säkerställa att kontinuitetslösningarna fungerar och uppfyller verksamhetens krav.

Finansinstitutet bör även analysera vad kraven på separata it-miljöer för test och produktion innebär ur ett kontinuitetsperspektiv, särskilt vid test av kontinuitetslösningar. Exempel på frågor som bör beaktas är om alla former av test kan genomföras i testmiljön, om data kan flyttas till och hanteras i testmiljön

---

[8] *Recovery Time Objective (RTO), dvs. den maximala tiden inom vilken ett system eller en process ska återställas efter en incident.*

[9] *Recovery Point Objective (RPO), dvs. den maximala tiden inom vilken dataförlust är acceptabel vid en incident.*

utan att bryta mot informationssäkerheten eller andra regelverk, om kapaciteten i testmiljön ligger nära eller långt ifrån produktionsmiljön för att testa exempelvis återställningstider, etc. För ändringshantering är det också viktigt att säkerställa att ändringar i system och tjänster analyseras och hanteras i processen. Kontroller bör utformas för att fånga upp kontinuitetsrelaterade aspekter vid ändringar i system och tjänster.

Hantering av verksamhetens driftskontinuitet

Finansinstitut bör ta fram en sund process för kontinuitetshantering (BCM). Som en del av sund kontinuitetshantering bör finansinstitut bland annat

- utföra konsekvensanalys (BIA), samt att kvantitativt och kvalitativt bedöma deras potentiella konsekvenser (riskbedömning)
- ta fram och dokumentera kontinuitetsplaner, samt fastställa dessa planer för att säkerställa att de uppfyller uppsatta mål för återställningstid (RTO) och mål för återhämtningspunkt (RPO)
- utarbeta återställningsplaner som fokuserar på återställande av driften av kritiska verksamhetsfunktioner, stödprocesser, informationstillgångar och deras inbördes beroenden
- beakta och införa kontinuitetsåtgärder för att motverka fel hos tredjepartsleverantörer som har avgörande betydelse för kontinuiteten av ett finansinstituts it-tjänster
- periodiskt testa sina kontinuitetsplaner för att visa att företaget kan hållas levande tills kritiska verksamheter kan återupprättas, och i synnerhet
    - tillse att kontinuitetsplaner för kritiska verksamhetsfunktioner, stödprocesser, informationstillgångar och deras inbördes beroenden testas minst en gång om året
    - använda en lämplig uppsättning av allvarliga men samtidigt möjliga scenarier, och i förekommande fall testa tjänster som tillhandahålls av tredje parter
    - utforma tester för att utmana förutsättningarna för kontinuitetsplanerna, inklusive styrnings- och kriskommunikationsplaner
    - verifiera förmågan hos personalen, uppdragstagarna, systemen och tjänsterna att hantera dessa scenarier
- uppdatera kontinuitetsplaner minst en gång om året utifrån testresultaten, aktuella underrättelser om hot och erfarenheter från tidigare händelser
- tillse att effektiva kriskommunikationsåtgärder är fastställda vid aktivering av kontinuitetsplaner.

Det är av central betydelse att it-verksamheten är delaktig i att utarbeta processen för kontinuitetshantering för att skapa robusthet och redundans i it-verksamhetens kritiska system och tjänster. It-verksamheten ska betraktas som en del av verksamheten och ska därför vara delaktig i konsekvensanalys, riskbedömning, utveckling av kontinuitetsplaner och återställningsplaner, samt övning och test av dessa planer.

2.2 *EIOPA guidelines*

European Insurance and Occupational Pension Authority (EIOPA), på svenska: Europeiska försäkrings- och tjänstepensionsmyndigheten, är en oberoende tillsynsmyndighet i EU som bland annat arbetar med att utforma tillsynen över försäkringsföretag med verksamhet i flera länder genom att ta fram riktlinjer och tekniska standarder, främja lika tillämpning av EU-regler hos tillsynsmyndigheter i olika länder, samt fördjupa samarbetet mellan tillsynsmyndigheter i olika länder.

I denna rapport har två av EIOPA:s riktlinjer valts ut:

- Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)[10]
- Guidelines on Information and Communication Technology security and governance (EIOPA-BoS-19-526)

Båda dessa riktlinjer är baserade på EBA:s motsvarande riktlinjer som beskrivs i kapitel 2.1. Därför beskrivs kraven i detta kapitel genom att belysa dessa likheter och i övrigt referera till motsvarande avsnitt i EBA:s riktlinjer.

För vilka gäller riktlinjerna?

Riktlinjerna kompletterar Solvens II-direktivet och gäller för alla försäkrings- och återförsäkringsföretag inom EU.

Hur ska riktlinjerna tillämpas?

Finansinspektionen följer EIOPA:s riktlinjer och genomför tillsyn på de företag som omfattas av riktlinjerna[11]. Finansinspektionens uppfattning är att riktlinjer

---

[10] *Riktlinjen finns översatt till svenska: Riktlinjer om uppdragsavtal med molntjänstleverantörer (EIOPA-BoS-20-002).*

[11] *https://www.fi.se/sv/publicerat/nyheter/2020/fi-kommer-tillampa-eu-riktlinjer-om-uppdragsavtal-med-molntjanstleverantorer/*

från EIOPA är likvärdiga med svenska allmänna råd. Företag ska därför "med alla tillgängliga medel söka följa riktlinjerna" enligt förordning (EU) nr 1093/2010. Riktlinjerna kan även användas i Finansinspektionens tillsynsaktiviteter.

Guidelines on outsourcing to cloud service providers innehåller krav på interna styrningsarrangemang, inklusive sund riskhantering, som kreditinstitut, värdepappersbolag, betalningsinstitut och institut för elektroniska pengar bör tillämpa vid utkontraktering.

Guidelines on Information and Communication Technology security and governance innehåller krav på informationssäkerhet, inklusive cybersäkerhet, i den mån informationen förvaras i it-system.

Varför ska riktlinjerna tillämpas?

Genom att tillämpa EIOPA:s riktlinjer bidrar finansiella företag till att möta myndighetens övergripande mål att verka för finansiell stabilitet och förtroende på försäkrings- och pensionsmarknaderna inom EU.

2.2.1 Guidelines on outsourcing to cloud service providers

Riktlinjerna syftar till att harmonisera nationell reglering och tillsyn, samt ge tydlighet och transparens till marknadsaktörer för användning av molntjänster (*eng: cloud outsourcing*). EIOPA har eftersträvat att, i möjligaste mån, harmonisera dessa riktlinjer med *EBA Guidelines on outsourcing arrangements*. Dessa riktlinjer är dock inte lika omfattande då de enbart omfattar uppdragsavtal om molntjänster. Riktlinjerna träder i kraft den 1 januari 2021.

Vilka krav på kontinuitet ställs?

Riktlinjerna består av 16 specifika områden som regleras. Nedan har dessa områden grupperats på ett sådant sätt att de harmoniserar med *EBA Guidelines on outsourcing arrangements*, vilket möjliggör korsreferenser mellan riktlinjerna.

Se motsvarande avsnitt i kapitel 2.1.1 för fler detaljer.

- *Proportionalitet*: Proportionalitetsprincipen gäller vid uppdragsavtal om molntjänster.
- *Bedömning av utkontrakterad verksamhet*: Ett flertal bedömningar ska göras innan utkontrakteringsprocessen inleds.
- *Ramverk för styrning*: Styrning och policy med tydliga ansvarsområden ska finnas vid uppdragsavtal om molntjänster.

- *Utkontrakteringsprocessen*: Innan överenskommelser ingås med molntjänstleverantörer ska företaget genomföra ett flertal olika analyser och bedömningar, inklusive företagsbesiktning.

2.2.2 *Guidelines on information and communication technology (ICT) security and governance*

Riktlinjerna syftar till att harmonisera nationell reglering och tillsyn, samt ge tydlighet och transparens till marknadsaktörer för att fastställa en basnivå inom it- och informationssäkerhetsområdet. Riktlinjerna är på övergripande nivå liknande de krav som beskrivs i *EBA Guidelines on ICT and security risk management*. Riktlinjerna träder i kraft den 1 juli 2021.

Vilka krav på kontinuitet ställs?

Riktlinjerna består av 24 specifika områden som regleras. Nedan har dessa områden grupperats på ett sådant sätt att de harmoniserar med *EBA Guidelines on ICT and security risk management*, vilket möjliggör korsreferenser mellan riktlinjerna.

Se motsvarande avsnitt i kapitel 2.1.2 för fler detaljer.

- *Proportionalitet*: Proportionalitetsprincipen gäller vid hantering av it- och säkerhetsrisker.
- *Strategi och ledning*: En strategi, styrning och kontrollramverk ska finnas för hantering av it- och säkerhetsrisker.
- *Ramverk för hantering av operativa risker och säkerhetsrisker*: Ett ramverk och processer för hantering av it- och säkerhetsrisker ska finnas.
- *Informationssäkerhet*: En informationssäkerhetspolicy och funktion som hanterar informationssäkerheten ska finnas.
- *Hantering av it-verksamhet*: Företaget ska hantera it- och säkerhetsrisker med hjälp av de införda processerna.
- *It-projektledning och ändringshantering*: Processer som styr anskaffning, utveckling, underhåll av system och tjänster, och ändringshantering ska finnas.
- *Hantering av verksamhetens driftskontinuitet*: En kontinuitetspolicy ska finnas (detta krav finns inte angivet i *EBA Guidelines on ICT and security risk management*). Konsekvensanalys och riskbedömning ska genomföras, kontinuitetsplaner och återställningsplaner ska tas fram, och planerna ska testas regelbundet. Effektiv kriskommunikation ska finnas.

2.3 CPMI-IOSCO guidelines

Committee on Payments and Market Infrastructures (CPMI) och International Organization of Securities Commissions (IOSCO) är två internationella organisationer som samarbetar avseende frågor rörande den finansiella infrastrukturen. Samarbetet syftar till att förbättra koordineringen för utveckling och fastställande av standarder och riktlinjer som berör clearing, avveckling och rapportering för finansiella marknadsinfrastrukturer (FMI:er) runt om i världen.

I denna rapport har två av CPMI-IOSCO:s riktlinjer valts ut:

- Principles for financial market infrastructures (PFMI)
- Guidance on cyber resilience for financial market infrastructure

För vilka gäller riktlinjerna?

CPMI-IOSCO:s riktlinjer gäller för alla FMI:er i Sverige och internationellt, exempelvis handelsplatser, värdepapperscentraler, betalningssystem och centrala motparter. På Riksbankens hemsida finns en översikt över den finansiella infrastrukturen samt vilka företag som räknas som FMI:er i Sverige[12].

Hur ska riktlinjerna tillämpas?

Finansinspektionen tillämpar CPMI-IOSCO:s riktlinjer i sin tillsynsverksamhet. Riksbanken tillämpar CPMI-IOSCO:s riktlinjer i sin övervakning av FMI:er. Alla FMI:er ska således följa dessa riktlinjer.

Principles for financial market infrastructures (PFMI) ska tillämpas av alla FMI:er och tillsynsmyndigheter. Tillsynsmyndigheterna ska dessutom utvärdera sig själva och publicera utfallet av denna utvärdering. Utvärderingen görs av myndigheternas internrevisionsfunktion, som är organisatoriskt separerad från tillsyns- och övervakningsverksamheten[13].

Guidance on cyber resilience for financial market infrastructure är ett tillägg till PFMI och ska tillämpas av alla FMI:er och tillsynsmyndigheter. Finansinspektionen

[12] *https://www.riksbank.se/en-gb/financial-stability/the-financial-system/the-financial-infrastructure/*

[13] *https://www.fi.se/sv/publicerat/nyheter/2014/tillsynen-av-finansiell-infrastruktur-fungerar-val/*

och Riksbanken använder detta tillägg som underlag för sin tillsynsverksamhet respektive övervakning[14].

Varför ska riktlinjerna tillämpas?

Genom att tillämpa CPMI-IOSCO:s riktlinjer bidrar FMI:er till att möta följande mål för dessa riktlinjer:

- skydda investerare
- säkerställa att finansmarknaden är rättvis, effektiv och transparent
- minska systemrisker.

2.3.1 Principles for financial market infrastructures

Riktlinjerna fastställer 24 principer som måste följas av alla FMI:er. Dessa principer innefattar viktiga områden som exempelvis generell organisation, hantering av kredit- och likviditetsrisker, hantering av affärsrisker och operativa risker, tillgänglighet, effektivitet och transparens. PFMI är utformat för att säkerställa hög säkerhet, effektivitet och resiliens hos de infrastrukturer som stödjer den globala finansmarknaden, vilket ställer krav på att dessa riktlinjer tillämpas fullt ut på ett korrekt sätt. Riktlinjerna har varit gällande sedan april 2012.

Vilka krav på kontinuitet ställs?

Av riktlinjens 24 principer är det i huvudsak en princip som ställer explicita krav inom kontinuitetsområdet.

Princip 17: Operativ risk

En FMI ska identifiera de resurser som utgör operativ risk, både interna och externa, och reducera påverkan av dessa risker genom att använda ändamålsenliga system, riktlinjer, procedurer och kontroller. System ska utformas för att säkerställa en hög grad av säkerhet och operativ tillförlitlighet, och ska ha adekvat, skalbar kapacitet. Kontinuitetshantering ska syfta till snabb återställning av verksamheten och uppfyllande av FMI:ers skyldigheter, även i händelse av ett storskaligt eller större avbrott.

---

[14] *Financial Infrastructure Report 2017, sid. 8, publicerad av Riksbanken. https://www.riksbank.se/en-gb/press-and-published/publications/other-former-publications/financial-infrastructure-report/*

En FMI ska ha en kontinuitetsplan som adresserar händelser som utgör en signifikant risk för avbrott i verksamheten. Kontinuitetsplanen ska innefatta användning av en sekundär inrättning[15]. Den ska utformas så att kritiska system och tjänster kan återställas senast inom två timmar efter ett avbrott (två timmar RTO). Planen ska utformas så att en FMI kan göra avveckling senast i slutet av samma dag då ett avbrott sker, även under extrema förhållandena. En FMI ska testa kontinuitetsplanen regelbundet.

Därutöver ställs ett flertal detaljerade krav för utformning av kontinuitetsplaner och förmåga till återställning. Dessa krav ligger helt i linje med ISO 22301 och ITIL 2011. Ett krav som särskilt sticker ut är att en FMI ska genomföra en jämförande riskanalys av den sekundära inrättningen. Den sekundära inrättningen ska i princip vara opåverkad vid en händelse som påverkar den primära inrättningen, med undantag för en koordinerad attack. Varje inrättning ska ha en robust resiliens baserad på duplicering av mjukvara och hårdvara. Teknologi ska finnas för att replikera data mellan tillgängliga inrättningar, och uppfylla uppsatta mål för återhämtningspunkt (RPO).

Sammanfattningsvis har PFMI högt uppställda krav inom kontinuitet som genererar kostsamma kontinuitetslösningar. Tillämpning av ISO-standarder (exempelvis ISO 22301) och ramverk för it-styrning (exempelvis ITIL 2011) är därför en förutsättning för att kunna uppfylla kraven i PFMI.

2.3.2 Guidance on cyber resilience for financial market infrastructure

Riktlinjerna är ett tillägg till *Principles for financial market infrastructures (PFMI)* och syftar till att förse FMI:er med vägledning i arbetet med att förbättra dess förmåga inom cyberresiliens. Målet med riktlinjerna är att begränsa de eskalerande risker för stabiliteten i det finansiella systemet som cyberhot utgör. Riktlinjerna har varit gällande sedan juni 2016.

Vilka krav på kontinuitet ställs?

Riktlinjerna omfattar fem riskkategorier och tre övergripande områden som ska tillämpas i ett ramverk för cyberresiliens hos en FMI. Riskkategorierna är: styrning, identifiering, skydd, detektering, hantering och återställning. De övergripande områdena är: test, situationsmedvetenhet, inlärning och utveckling.

---

[15] *Inrättning i detta fall syftar på kontor, datacenter, eller andra inrättningar som är nödvändiga för den operativa driften av verksamheten.*

Styrning

En FMI ska

- ha ett heltäckande ramverk för cyberresiliens som omfattar både it, människor och processer, samt inbegriper risker inom hela ekosystemet[16]
- säkerställa att ramverken för cyberresiliens och ERM[17] är konsekventa
- tillämpa internationella och nationella standarder för cyberresiliens
- genomföra revisioner och mäta compliance
- skapa en företagskultur och bygga kunskap som gynnar cyberresiliens
- förankra ägandeskap och ansvar i organisationen, inklusive styrelsen och högsta ledningen.

Dessa krav ska integreras i företagets arbete med kontinuitet i it-verksamheten.

Identifiering

En FMI ska

- identifiera verksamhetens funktioner och stödjande processer
- identifiera informationstillgångar och tillgång till dessa
- regelbundet genomföra granskning och uppdateringar
- identifiera beroenden som inbegriper hela ekosystemet.

Dessa krav berör direkt konsekvensanalys, riskbedömning, granskning och uppdatering inom kontinuitetsarbetet. För att främja samarbete inom organisationen ska ovanstående arbete även innefatta cyberresiliens.

Skydd

En FMI ska

- tillämpa *resilience by design*, dvs. bygga in säkerhet i teknik- och systemutveckling från ett tidigt stadium av konceptualisering och design
- en design från grunden som innefattar hela ekosystemet
- tillämpa kraftfulla kontroller för it som skydd mot cyberhot
- tillämpa övervakning och detektering av cyberhot inom it-miljön
- hantera risker som inbegriper hela ekosystemet

---

[16] *Med ekosystem i detta sammanhang avses deltagare, andra sammankopplade FMI:er, tjänsteleverantörer, andra leverantörer och dess produkter, etc.*

[17] *Enterprise Risk Management (ERM), dvs. företagets övergripande riskhantering.*

- hantera insiderhot genom säkerhetsanalys, bakgrundskontroll på anställda och tillämpa fysisk och logisk åtkomstkontroll
- utbilda personal i cybersäkerhet och hantering av risker.

Resilience by design ska även innefatta kontinuitetslösningar som hanterar avbrott eller andra störningar till följd av tekniska eller mänskliga fel, inte enbart till följd av cyberattacker. Övervakning och detektering ska även innefatta tillgänglighets- och kapacitetshantering.

Detektering

En FMI ska

- etablera förmåga till ständig övervakning av cyberhot som innefattar samtliga intressenter
- kunna upptäcka, hantera och analysera cyberhot.

Betydelsen av cyberhot ska även innefatta hot och sårbarheter kopplade till kontinuitet och backuphantering. En cyberattack kan leda till ett avbrott som behöver hanteras genom återställning av system och tjänster eller data.

Hantering och återställning

En FMI ska

- kunna återställa kritisk it senast inom två timmar efter en cyberattack,
- utveckla beredskapsplaner (*eng: contingency plans*) för oförutsedda händelser
- utveckla och testa procedurer för hantering, återställning och återgång till normal drift
- tillämpa design av system, processer och kontroller som är integrerade med verksamheten
- skydda känslig data genom backuphantering och återställning, samt säkerställa att kraven för både riktighet och tillgänglighet alltid uppfylls
- planera för kriskommunikation vid cyberattacker.

Givet kravet på två timmar RTO för kritiska system och tjänster är det av största vikt att kontinuitetslösningar även innefattar hantering av olika cyberhot. Av denna anledning ska ansvariga för kontinuitet och cyberresiliens tillsammans verka för att uppnå en hög grad av robusthet hos kritiska system och tjänster.

Test

En FMI ska

- etablera ett testprogram i syfte att validera effektiviteten av ramverket
- använda standardiserade metoder och praxis för test (sårbarhetstester, scenariobaserade tester, penetrationstester, etc.)
- genomföra koordinerade tester som innefattar hela ekosystemet och samtliga intressenter.

Även inom området för test ska ansvariga för kontinuitet och cyberresiliens tillsammans verka för att uppnå en hög mognadsgrad i syfte att säkerställa robustheten hos kritiska system och tjänster. Då cyberattacker kan leda till intermittenta avbrott eller störningar är det viktigt att säkerställa att dessa kan hanteras genom återställning (exempelvis genom flytt till sekundär inrättning), och att detta även testas.

Situationsmedvetenhet

En FMI ska

- tillämpa *Cyber Threat Intelligence (CTI)*, dvs. information som genom bearbetning, analyser och bedömningar förädlas till kunskap
- tillämpa informationsdelning till andra parter.

Det är viktigt att föra kunskapen vidare och göra personal, ledningsfunktioner och andra intressenter medvetna om potentiella risker och dess konsekvenser på verksamhetens kontinuitet till följd av cyberattacker.

Inlärning och utveckling

En FMI ska

- tillämpa lärande och ständiga förbättringar inom arbetet med cyberresiliens
- tillämpa mätetal och mognadsmodeller för att utvärdera arbetet med cyberresiliens.

Lärande och ständiga förbättringar ska tillämpas i symbios mellan cyberresiliens och kontinuitet för att erhålla största möjliga effekt av arbetet. Robusthet uppnås genom att omfatta alla former av hot och risker som kan påverka *konfidentialitet*, *riktighet* eller *tillgänglighet* hos system och tjänster eller data.

2.4 *Finansinspektionens föreskrifter*

Finansinspektionens föreskrifter och allmänna råd fungerar som komplement till lagar och förordningar. Medan föreskrifterna är obligatoriska för företagen att följa, är de allmänna råden rekommendationer för hur aktörerna kan gå tillväga för att följa de bindande bestämmelserna.[18]

I denna rapport har två av Finansinspektionens föreskrifter valts ut:

- FFFS 2014:4 – Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker
- FFFS 2014:5 – Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem

För vilka gäller föreskrifterna?

Föreskrifterna FFFS 2014:4 och FFFS 2014:5 gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, kreditmarknadsföreningar, och värdepappersbolag.

Hur ska föreskrifterna tillämpas?

Föreskrifterna förväntas tillämpas genom att den finansiella aktören inför samtliga av de obligatoriska krav som finns i föreskrifterna. De allmänna råden om omnämns i föreskrifterna är inte bindande regler utan en rekommendation för hur aktören kan göra för att följa de bindande bestämmelser som råden anknyter till.

FFFS 2014:4 innehåller bestämmelser om hur ett företag ska hantera sina operativa risker. Det ställs ett flertal krav på verksamhetens generella kontinuitetshantering.

FFFS 2014:5 innehåller bestämmelser om hur ett företag ska hantera informationssäkerhet, it-verksamhet och insättningssystem.

Varför ska föreskrifterna tillämpas?

De lagar och regler som utvecklats för finansmarknaden, däribland FFFS 2014:4 och FFFS 2014:5, lägger ett stort ansvar på företagen att själva motverka osund verksamhet och risker mot stabiliteten. Därför åligger ansvaret aktören själv att tillämpa föreskrifterna i verksamheten. Finansinspektionen bedriver sedan

[18] *https://www.fi.se/sv/bank/regler/*

tillsyn för att säkerställa att lagar och regler efterlevs av aktören som således har ett egenintresse i att undvika sanktioner eller andra straffåtgärder.

2.4.1 FFFS 2014:4 – Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker

Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker reglerar bland annat styrelsens och den verkställande direktörens ansvar, hanteringen av operativa risker i verksamheten, bland annat i fråga om processer, legala risker, personal, säkerhet, process för godkännande samt kontinuitetshantering. Reglerna omfattar även krav på företagens värdepappersrörelse och valutahandel. Föreskrifterna har varit gällande sedan 1 juni 2014.

Vilka krav på kontinuitet ställs?

FFFS 2014:4 ställer ett flertal krav på verksamheters kontinuitetshantering. Dessa berör interna regler, analys av konsekvenser och planering för återställning, kommunikation och utbildning, samt uppdatering och test av planer, och påverkar därför kontinuitetsarbetet inom it-verksamheten. Föreskriften anger även särskilda krav för it-system.

Interna regler, analys av konsekvenser och planering för återställning

Metoder, rutiner, ansvariga (roller och befattningar) ska anges för kontinuitetshantering. Den längst tillåtna tiden för avbrott ska fastställas, liksom kravet att konsekvenserna av sådana avbrott ska analyseras regelbundet på alla affärsenheter och stödfunktioner i företaget. Föreskriften anger även krav på att dokumentera beredskapsplaner, kontinuitetsplaner och återställningsplaner.

Kommunikation och utbildning

Ett företag ska ha rutiner för att hantera sin interna och externa kommunikation i samband med ett avbrott eller en större verksamhetsstörning, inklusive dess dotterbolag och filialer. Detta innebär att tydliga rutiner behövs för att kommunicera avbrott i it-miljön till den berörda verksamheten. Vad gäller utbildning ska ett företag regelbundet utbilda och informera sin personal om hur den ska använda beredskapsplaner, kontinuitetsplaner och återställningsplaner.

Uppdatering och test av planer

Ett företag ska regelbundet uppdatera och testa sina beredskapsplaner, kontinuitetsplaner och återställningsplaner, samt utse en ansvarig person eller funktion för uppdatering och test av varje sådan plan. Verksamheten ska även

ange vilka typer av tester som ska utföras, samt hur ofta testerna ska utföras. Det innebär att samtliga planer för system och tjänster som stöttar kritisk verksamhet, eller processer av väsentlig betydelse, ska uppdateras och testas på motsvarande sätt i nära samarbete med den övriga verksamheten. Vidare ska it-organisationen ta fram motsvarande testplan innefattande vilka typer av tester som ska utföras för respektive it-system, samt hur ofta testerna ska utföras. Beredskapsplaner, kontinuitetsplaner och återställningsplaner för verksamhetens kritiska processer eller processer av väsentlig betydelse, samt de system och tjänster som stöttar dessa processer, ska som minimum testas årligen.

It-system

Ett företag ska identifiera operativa risker i sina produkter, tjänster, funktioner, processer och it-system, samt beskriva vilka it-system som stödjer processen i processdokumentationen. För att möjliggöra detta krävs att konsekvensanalys och riskbedömning görs på ett korrekt sätt inom ramen för kontinuitetsarbetet, med särskilt fokus på de it-system som stödjer processen. Ett företag ska även ha en process för att godkänna nya eller väsentligt förändrade produkter, tjänster, marknader, processer, it-system samt för större förändringar i företagets verksamhet och organisation. Det innebär att kontinuitetsplaner och återställningsplaner ska granskas vid större förändringar.

Ett företag ska se till att dess huvudsakliga it-driftställe finns på ett tillräckligt stort geografiskt avstånd från den plats där företaget förvarar sina säkerhetskopior. För samtliga bestämmelser avseende hur ett företag ska hantera it-system hänvisar föreskriften till FFFS 2014:5 om informationssäkerhet, it-verksamhet och insättningssystem.

2.4.2 FFFS 2014:5 – Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem

Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem omfattar bland annat krav på att företagen ska arbeta strukturerat och metodiskt med informationssäkerhet. De reglerar även styrning och processer för it-verksamheten samt ställer krav på säkerheten för insättningssystem. Föreskrifterna har varit gällande sedan 1 juni 2014.

Vilka krav på kontinuitet ställs?

FFFS 2014:5 tar höjd utifrån ett informationssäkerhetsperspektiv och berör därigenom både direkta och indirekta krav på kontinuitet i it-verksamheten. Dessa krav är indelade i tre olika områden: informationssäkerhet, it-verksamhet och insättningssystem.

Informationssäkerhet

Ett företag ska arbeta strukturerat och metodiskt med informationssäkerhet genom att använda sig av ett ledningssystem. Kopplat till detta krav följer ytterligare krav på att

- mål och inriktning för informationssäkerheten ska dokumenteras och att ett tydligt ansvar för informationssäkerheten säkerställs
- företaget klassificerar sin information så att rätt skyddsnivå erhålls utifrån *konfidentialitet*, *riktighet* och *tillgänglighet* i verksamheten
- genomföra riskanalys årligen (och vid förändringar i verksamheten) och därefter besluta om åtgärder utifrån dessa analyser och inträffade incidenter
- fastställa interna regler för sitt arbete med informationssäkerhet.

Dessa krav medför ett särskilt fokus på bevarandet av informationens *konfidentialitet*, *riktighet* och *tillgänglighet*. Ett företag ska arbeta strukturerat och metodiskt med kontinuitet. Detta innefattar

- dokumentation av mål och inriktning
- säkerställande av tydligt ansvar för kontinuitetsarbetet
- it-verksamhetens säkerställande av att informationens skyddsnivåer för *konfidentialitet*, *riktighet* och *tillgänglighet* kan bevaras under alla omständigheter (dvs. alla former av it-relaterade incidenter, inklusive större haverier som kräver återställning av system och tjänster)
- genomförande av konsekvensanalys och riskbedömning för verksamhetens kritiska system och tjänster
- fastställda interna regler för informationssäkerhet som inkluderar krav på kontinuitet.

It-verksamhet

Ett företag ska ha dokumenterade övergripande mål och strategier för sin it-verksamhet. Ett företag ska också säkerställa att det är tydligt vem som ansvarar för de olika delarna av företagets it-verksamhet. För varje it-system ska företaget utse en person eller funktion som ansvarar för företagets krav på systemet. Ett företag ska ha ändamålsenliga processer för hantering av sina it-system. Ett företag ska även ha dokumentation över varje enskilt it-system som är av betydelse för verksamheten. För bestämmelser om uppdragsavtal hänvisas till 10 kap. FFFS 2014:1 om styrning, riskhantering och kontroll i kreditinstitut och 9 kap. FFFS 2007:16 om värdepappersrörelse.

Dessa krav medför att it-verksamheten ska ha dokumenterade övergripande mål och strategier för kontinuitetsarbetet, samt säkerställa att en kontinuitetsansvarig person finns utsedd. Ett it-systems ansvariga person har även ansvar för att uppfylla verksamhetens definierade krav på systemets tillgänglighet, återställning och backup-hantering. Företaget ska ha en ändamålsenlig process för hanteringen av kontinuitet och dokumentation av it-systemets återställningsplan och annan teknisk dokumentation nödvändig för återställningen av systemet.

För bestämmelser om uppdragsavtal är Finansinspektionens föreskrifter inte uttömmande. I stället hänvisas till *EBA Guidelines on outsourcing arrangements* respektive *EIOPA Guidelines on outsourcing to cloud service providers* för mer konkreta kravställningar inom kontinuitet avseende uppdragsavtal.

Insättningssystem

För företag som tar emot eller avser att ta emot insättningar som omfattas av insättningsgaranti enligt lagen (1995:1571) om insättningsgaranti gäller särskilda krav för att bevara informationens riktighet, integritet, konfidentialitet och tillgänglighet hos de it-system som företaget använder för att hantera sin information om insättare och deras insättningar. Dessa krav gäller riskanalys, funktioner och rutiner för informationssäkerhet, dokumentation, granskning och rapportering.

De särskilda kraven för insättningssystem medför att ett antal kontinuitetsrelaterade krav särskilt behöver beaktas. Det ska finnas tekniska funktioner och administrativa rutiner för att säkerställa att aktiviteter och ändringar i dessa it-system är spårbara och kan analyseras i syfte att utröna hur de påverkar systemets drift, tillgänglighet och förmåga till återställning efter ett avbrott. Dessutom ska åtkomstkontroll, systemintegritet och informationens riktighet kunna bevaras under och efter ett avbrott.

2.5 ISO-standarder

Internationella ISO-standarder inom kontinuitetshantering syftar till att ge företag, oavsett storlek, ett stöd för systematiskt arbete i sin kontinuitetshantering. Genom att tillämpa dessa standarder säkerställs att företaget följer ett etablerat arbetssätt som kan förstås och tolkas av leverantörer, kunder och andra intressenter.

I denna rapport har två ISO-standarder valts ut:

- ISO 22301:2019 – Business continuity management systems – Requirements
- ISO 27031:2011 – Guidelines for information and communication technology readiness for business continuity

För vilka gäller standarderna?

ISO-standarderna gäller för alla slags företag inom finanssektorn oavsett företagstyp, exempelvis bank, kreditinstitut, betalningsinstitut, marknadsinfrastrukturbolag, försäkringsföretag, med flera.

Hur ska standarderna tillämpas?

ISO-standarderna tillämpas genom att företaget inför de strukturer, processer och kontroller som beskrivs i standarderna, samt bygger upp nödvändiga förmågor i form av personal, styrning och tillämpliga verktyg. Att tillämpa ISO-standarderna innebär som regel en stor investering för företaget, vilket ställer krav på tydliga mål med införandet. Målet kan vara att företaget arbetar i enlighet med standarden, eller en certifiering[19] på längre sikt.

De ISO-standarder som kartläggs i denna rapport har olika syften och tillämpas därför på olika sätt.

ISO 22301:2019 är en standard för ledningssystem som fastställer krav för kontinuitetshantering i verksamheten, inklusive it-verksamheten. Standarden kan även tillämpas för att bedöma en organisations förmåga att uppfylla sina egna krav på och förpliktelser om kontinuitetshantering.

ISO 27031:2011 är en vägledning för kontinuitetsberedskap inom informations- och kommunikationsteknologi (*eng: ICT – Information and Communication Technology)* och tillämpas som stöd för en bredare ledningssystemsstandard som beskrivs i ISO 22301.

Varför ska standarderna tillämpas?

Genom att tillämpa de strukturer och krav som beskrivs i ISO-standarderna byggs en förmåga i företaget att hantera avbrott och störningar i verksamheten, inklusive it-verksamheten, på ett standardiserat sätt. Standarderna skapar möjlighet att arbeta med kontinuitet enligt internationellt etablerad *best practice*, och formar samtidigt ett gemensamt språk, vilket förenklar kommunikation både

[19] *Enbart ISO 22301 är certifieringsbar i nuläget.*

internt och externt. Därmed blir det lättare att upprätthålla kompetens och förmåga inom kontinuitet över tid.

2.5.1 ISO 22301

ISO 22301 är en internationell ledningssystemsstandard som innehåller krav och ledningsstrukturer som ligger till grund för att kunna upprätthålla kontinuiteten hos verksamhetens leverans av produkter och tjänster under en störning eller avbrott i verksamhetsprocessen. ISO 22301, som är certifieringsbar, ligger även som grund för de övriga standarderna inom kontinuitetshantering.

Internationella ledningssystemsstandarder följer samma struktur eller kapitelindelning, vilket förenklar integrering av flera ledningssystem. Den första versionen av denna standard kom ut 2012 och en reviderad version publicerades 2019.

Vilka krav på kontinuitet ställs?

ISO 22301 innehåller sju kapitel med olika kravställningar som tillsammans utgör hela ledningssystemet för verksamhetens kontinuitetshantering och operativa förmåga.

Organisationens sammanhang

Vid etablering av kontinuitetsledningssystem ska organisationen identifiera sakägare och deras krav, etablera och upprätthålla en process för att identifiera rättsliga och regulatoriska krav, och säkerställa att dessa krav omhändertas. Organisationen ska identifiera de delar av organisationen, dess produkter och tjänster, som ska ingå i kontinuitetsledningssystemet.

Detta innebär att organisationen behöver identifiera samtliga system och tjänster, inklusive deras ägare, som organisationen är beroende av inom de funktioner som ingår i kontinuitetsledningssystemet, samt förstå och hantera de rättsliga och regulatoriska krav som ställs på dessa system och tjänster.

Ledarskap

Högsta ledningen ska säkerställa att det finns en policy och mål som är i linje med organisationens strategiska riktning. Vidare ska organisationen

- etablera kraven för kontinuitetsledningssystemet som en integrerad del av verksamhetsprocessen
- allokera nödvändiga resurser för kontinuitetsledningssystemet
- leda och understödja de personer som bidrar i tillämpningen av kontinuitetsledningssystemet

- säkerställa att policyn är fastställd och kommunicerad
- säkerställa att roller och ansvar inom kontinuitetsledningssystemet är definierade, tillsatta och kommunicerade.

Detta innebär att kraven för kontinuitetsledningssystemet behöver innefatta även it-verksamheten. Vid allokering av resurser är det viktigt att nyckelpersoner (kontinuitetsansvariga) inom både verksamheten och it-verksamheten utses, samt att nödvändiga kontaktytor etableras. Dessa personer behöver i sin tur leda och understödja andra resurser som tillsammans bidrar i tillämpningen av kontinuitetsledningssystemet. Vid fastställande av policy, roller och ansvar är det viktigt att både verksamheten och it-verksamheten samverkar.

Planering

Vid planering av kontinuitetsledningssystemet ska risker och möjligheter fastställas och adresseras i syfte att säkerställa målen med kontinuitetsledningssystemet. Åtgärder för dessa risker och möjligheter ska införas och utvärderas. Mål för kontinuitetsarbetet ska även fastställas för relevanta funktioner och nivåer i organisationen. Dessa mål ska sedan omsättas till planer som beskriver hur dessa mål ska nås. Organisationen ska också avgöra hur förändringar som påverkar kontinuitetsledningssystemet ska hanteras och planeras.

Det är av största vikt att all hantering av risker och möjligheter även inbegriper it-verksamheten som ska ses som en leverantör av viktiga tjänster till verksamheten.

Stödverksamhet

Organisationen ska

- tillsätta nödvändiga resurser för kontinuitetsledningssystemet
- avgöra vilken kompetens som behövs för personer som arbetar med kontinuitet
- säkerställa att all personal blir medvetna om policy, och deras roller och ansvar i kontinuitetsledningssystemet
- avgöra krav (vad, när, till vem, hur, av vem, etc.) på kommunikation kopplat till kontinuitetsledningssystemet
- dokumentera kontinuitetsledningssystemet, inklusive ändringshantering och behörighetskontroll på dokumentationen.

Även it-verksamheten förväntas genomföra samtliga punkter ovan då it-verksamhetens arbete med kontinuitet är en integrerad del av kontinuitetsledningssystemet.

Operativ hantering

Organisationen ska

- planera, införa och kontrollera kontinuitetsprocessen som en förutsättning för att uppfylla kraven för kontinuitetsledningssystemet
- genomföra konsekvensanalys för att avgöra maximalt tolerabel avbrottsperiod (MTPD)[20] och återställningstid (RTO) för verksamhetsprocessens prioriterade aktiviteter, och identifiera prioriterade resurser som stödjer aktiviteterna
- genomföra riskbedömning för att identifiera risker kopplade till avbrott i verksamhetsprocessens prioriterade aktiviteter och resurser
- identifiera och välja kontinuitetsstrategier och lösningar för att möta kraven på MTPD och RTO
- identifiera krav på prioriterade resurser, inklusive system och tjänster, och införa utvalda kontinuitetslösningar.

Organisationen ska införa och resurssätta en process och struktur för att kunna hantera operativa incidenter/avbrott och kommunicera detta till relevanta intressenter. För hantering av incidenterna ska särskilda team ha ansvar och ha genomgått utbildning. Organisationen ska dokumentera och upprätthålla kontinuitetsplaner och procedurer för att kunna hantera incidenter/avbrott i verksamheten. Även återställning och återgång till normal verksamhet ska dokumenteras. Organisationen ska slutligen införa ett program för övning och test av kontinuitetsplaner, samt utvärdera alla genomförda aktiviteter ovan enligt planerade intervall, vid inträffade incidenter eller vid större förändringar.

Det är av största vikt att samtliga aktiviteter ovan genomförs i samverkan mellan verksamheten och it-verksamheten. Det är av särskild vikt att beakta risker kopplade till it-verksamhetens beroenden gentemot leverantörer och tredjepartsleverantörer. För detta ändamål hänvisas till *EBA Guidelines on outsourcing arrangements* respektive *EIOPA Guidelines on outsourcing to cloud*

[20] *Maximum Tolerable Period of Disruption (MTPD), dvs. den maximala tiden som processen/aktiviteten kan vara otillgängligt innan oacceptabla konsekvenser uppstår.*

service providers för mer konkreta kravställningar avseende uppdragsavtal där kontinuitetshantering ingår.

Utvärdering av prestanda

Organisationen ska

- övervaka, mäta, analysera och utvärdera kontinuitetsledningssystemet och dess resultatet
- genomföra internrevision (*eng: internal audit*) inom ramen för ett etablerat program för detta ändamål
- genomföra ledningens genomgång (*eng: management review*) med jämna intervall.

Då kontinuitetsarbetet omfattar hela företagets it-miljö blir utvärdering av prestanda hos it-verksamheten särskilt viktig då risker som utvärderas blir hela företagets angelägenhet. Därför behöver resultatet från it-verksamhetens utvärdering av prestanda kommuniceras till samtliga berörda intressenter inom organisationen.

Förbättringar

Organisationen ska

- upptäcka möjligheter till förbättringar
- upptäcka avvikelser (*eng: nonconformities*) och vidta nödvändiga åtgärder
- utvärdera och genomföra ständiga förbättringar (*eng: continual improvements*) baserat på kvalitativa och kvantitativa mätetal.

Ovanstående aktiviteter genomförs av både verksamheten och it-verksamheten.

2.5.2 ISO 27031

ISO 27031 är en internationell standard som beskriver ett ledningssystem för *ICT Readiness for Business Continuity (IRBC)* som fokuserar på företagets förmåga att kunna återställa it-tjänster (*eng: IT disaster recovery*) efter en störning eller ett större haveri. Standarden innefattar koncept och principer för informations- och kommunikationsteknologi och formar ett ramverk för metoder och processer för att identifiera och specificera samtliga aspekter i syfte att uppnå en höjd it-beredskap.

ISO 27031, som inte är certifieringsbar, används och tillämpas av vissa aktörer som ett komplement till ISO 22301 för hantering av kontinuitet och återställning av it-tjänster.

Vilka krav på kontinuitet ställs?

IRBC är ett ledningssystem som kompletterar och stödjer organisationers kontinuitets- och/eller informationssäkerhetsprogram. IRBC baseras på följande huvudprinciper:

- Förebygga att incidenter inträffar.
- Upptäcka incidenter så tidigt som möjligt.
- Besvara incidenter på ett effektivt sätt.
- Återställa system, tjänster och data på ett korrekt sätt.
- Genomföra förbättringar efter inträffade incidenter.

De viktigaste beståndsdelarna inom IRBC är

- människor
- fysiska inrättningar
- teknologi – inklusive hårdvara, nätverk och mjukvara
- data
- processer
- leverantörer.

Genom att tillämpa IRBC kan it-verksamheten på ett meningsfullt sätt värdera sin förmåga att stödja målen för kontinuitetsledningssystemet. I stället för att besvara frågan ”hur säker är vår it-miljö?” kan den viktigare frågan ”har it-verksamheten kapaciteten att besvara incidenter?” besvaras.

Processen för IRBC bygger på principen för *Plan-Do-Check-Act (PDCA)*[21]:

- *Plan* – här ingår verksamhetens konsekvensanalys och dess kravställningar, skriva IRBC policy, och genomföra gap-analys. Här ingår även formulering av strategier för färdigheter och kunskap, fysiska inrättningar, teknologi, data och leverantörer.
- *Do* – här ingår införande av strategierna för beståndsdelarna inom IRBC, samt den operativa hanteringen. Bland annat ska kontinuitets- och återställningsplaner utvecklas, medvetenhets- och kunskapshöjande utbildningar genomföras, samt en dokumenterad procedur för operativ hantering av incidenter tas fram, där även återställning och återgång till normal drift ingår.

---

[21] *Plan-Do-Check-Act (PDCA), även kallad Deming cycle, är en iterativ ledningsprocess i fyra steg för att erhålla kontroll och ständiga förbättringar i verksamhetens produkter och tjänster.*

- *Check* – här ingår övervakning och granskning, övning och test, samt revision. Detta steg innefattar bland annat övervakning av fysiska inrättningar, ändringshantering, företagsbesiktning, avveckling av system och tjänster, hotbildsanalys, prestandamätning, etc. Ett övnings- och testprogram ska etableras som omfattar all operativ hantering. Olika former av revision ska genomföras, bland annat intern- och externrevision.
- *Act* – här ingår ledningens genomgång och ständiga förbättringar, som i sin tur leder till nya krav på IRBC som hanteras genom nästa PDCA-cykel.

ISO 27031 ger ytterligare praktiskt stöd inom it-verksamhetens kontinuitetsarbete genom Annex A-C, där följande områden behandlas:

- Operativ hantering av incidenter, där även återställning och återgång till normal drift ingår.
- Hög tillgänglighet för system och underliggande infrastruktur.
- Bedömning av felscenarion och risker.

2.6 Ramverk för it-styrning

It-styrning är en del av den allmänna styrningen av ett företag och syftar till att tillföra så stort värde som möjligt för verksamheten. Ramverk för it-styrning finns för att skapa en struktur som säkerställer att it-verksamheten uppfyller målen för it-styrningen, och därigenom verksamhetens övergripande mål. Behovet av ramverk för it-styrning är tydligt tack vare en stadigt ökande reglering av it-verksamheten inom finanssektorn.

I denna rapport beskrivs två ramverk för it-styrning:

- ITIL 2011 – Information Technology Infrastructure Library[22]
- COBIT 2019 – Control Objectives for Information and Related Technologies

[22] *En ny, omarbetad version, ITIL4, finns tillgänglig sedan 2019 och greppar ett mer holistiskt perspektiv för att stödja organisationen i en it-miljö som kännetecknas av ledord som Agile, DevOps and Lean. Rapporten fokuserar på föregående version, ITIL 2011, då den är betydligt mer vanligt förekommande.*

För vilka gäller standarderna?

Ramverk för it-styrning gäller för alla slags företag inom finanssektorn oavsett företagstyp, exempelvis bank, kreditinstitut, betalningsinstitut, marknadsinfrastrukturbolag, försäkringsföretag, med flera.

Hur ska standarderna tillämpas?

Genom att tillämpa ett standardiserat ramverk för it-styrning, kan företaget producera mätbara resultat som ligger till grund för utvärdering av it-verksamhetens strategi och mål, och kan jämföras med andra företag inom samma sektor. Att införa ett ramverk för it-styrning innebär som regel en stor och kostsam förändring som inbegriper samtliga delar av it-organisationen, varför ett sådant införandeprogram bör genomföras stegvis med tydligt uppsatta delmål.

De ramverk för it-styrning som kartläggs i denna rapport har olika syften och tillämpas därför på olika sätt.

ITIL 2011 fokuserar på ”hur man uppnår” en funktionell it-styrning genom konkreta tips, råd, rekommendationer, processer, mallar, teorier, metoder och modeller.

COBIT 2019 fokuserar på ”vad som måste uppnås” genom att tillhandahålla konkreta verktyg för att mäta mognadsgraden för varje processområde inom organisationen.

2.6.1 ITIL 2011

ITIL är världens mest använda ramverk för it-styrning med samlad praxis för hur it-verksamheten på bästa sätt kan gå tillväga för att säkra en effektiv och kundorienterad tjänsteleverans. Ramverket beskriver en mängd processer och funktioner som kan användas som stöd och hjälp i styrningen av it-verksamheten. Första versionen av ITIL togs fram mellan 1989 och 1995, och har sedan dess uppdaterats ett flertal gånger. ITIL 2011 är en uppdaterad version av ITIL3.

ITIL-livscykeln består av 5 olika steg:

1. ITIL service strategi
2. ITIL service design
3. ITIL serviceövergång
4. ITIL serviceoperation
5. ITIL kontinuerlig serviceförbättring

Vilka krav på kontinuitet ställs?

I denna rapport ligger fokus på processen för *IT Service Continuity Management (ITSCM)* som återfinns i steget för ITIL service design. ITSCM syftar till att hantera risker som kan påverka it-tjänster allvarligt. Processen säkerställer att en intern eller extern leverantör av en it-tjänst under alla omständigheter kan leverera en minsta överenskommen tjänstenivå (SLA[23]) genom att reducera riskerna för allvarliga avbrott eller katastrofer till en acceptabel nivå, samt planera för återställning av it-tjänsten om katastrofen är ett faktum. ITSCM är en stödjande process till verksamhetens kontinuitetsprocess.

ITSCM är en livscykelbaserad process som består av 5 olika steg:

1. Initiering.
2. Kravställning och strategi.
3. Fastställande.
4. Operativ hantering.
5. Aktivering.

Initiering

I detta processteg ska

- en policy fastställas och kommuniceras så att all personal är medveten om och förstår roller och ansvar i arbetet med ITSCM
- omfattningen av ITSCM bestämmas genom konsekvensanalys och riskbedömning
- en struktur definieras för operativ hantering av incidenter som stödjer kontinuitetsprocessen
- ett projekt initieras för införande av ITSCM och resurser tillsättas
- kvalitativa och kvantitativa mätetal definieras för införandet.

Policyn ska åtminstone förtydliga ledningens intentioner och mål med ITSCM, samt definiera roller och ansvar. När omfattningen av ITSCM ska bestämmas är det viktigt att inte enbart utgå från verksamhetens förväntningar, utan även ta hänsyn till anmärkningar från genomförda revisioner, och compliance gentemot regulatoriska krav, kundkrav, försäkringskrav och informationssäkerhetskrav. Vid allokering av resurser är det viktigt att bygga kunskap inom företaget och inte enbart förlita sig på kunskap hos leverantörer. Kvalitativa och kvantitativa

[23] *Service Level Agreement (SLA).*

mätetal ska fånga upp prestandan inom ITSCM genom nyckeltal som svarar upp mot verksamhetens övergripande mål och strategier.

Kravställning och strategi

I detta processteg ska

- konsekvensanalys och riskbedömning genomföras för samtliga verksamhetsprocesser som omfattas av ITSCM
- mål för återställningstid (RTO) och mål för återhämtningspunkt (RPO) definieras för samtliga it-tjänster i konsekvensanalysen
- riskbedömningen särskilt fokusera på händelser som berör exempelvis
    - förlust, skada eller nekad åtkomst till infrastrukturtjänster
    - fel eller brister hos leverantörer av kritiska it-tjänster
    - förlust eller förvanskning av viktig information
    - sabotage, utpressning eller spioneri
    - infiltrering eller cyberattack på informationssystem
- strategier för kontinuiteten i it-tjänsterna beskrivas baserat på verksamhetens behov, i syfte att reducera de identifierade riskerna.

Vid riskbedömningen ska de risker som faller utanför organisationens riskaptit behandlas. Ett riskbeslut ska då tas om vilka risker som de facto kan elimineras beroende på nettorisk; här gäller att hitta en balans mellan acceptabel risknivå och kostnaden att reducera risken. Om bortfall av en it-tjänst resulterar i hög konsekvens för verksamheten, bör högre tillgänglighet för it-tjänsten övervägas. Fokusera alltid på *single point of failures (SPOF)*[24] vid konsekvensanalys och riskbedömning. Dessa utgör i regel alltid en hög risk för verksamheten och bör därmed elimineras helt, om möjligt. Strategier för kontinuiteten i it-tjänster ska alltid innefatta backuphantering, återställning och återgång till normal drift.

Fastställande

I detta processteg ska

- kontinuitetsplaner utvecklas och fastställas, inklusive procedurer för återställning och återgång till normal drift
- organisatorisk planering genomföras i händelse av ett allvarligt avbrott eller en katastrof

[24] *Single point of failure (SPOF) avser den svagaste länken i ett givet system, ofta där redundans saknas.*

- kontinuitetslösningar fastställas baserade på strategierna beskrivna i föregående steg, i syfte att reducera de identifierade riskerna
- kontinuitetslösningar övas och testas initialt så att de fungerar som det är tänkt.

Vid utveckling av kontinuitetsplaner för it-verksamheten, utgå alltid ifrån att en eller flera nyckelpersoner inte finns på plats. Utgå från en rimlig nivå på kunskap hos de personer som ska utföra procedurerna i planerna. Säkerställ att alla nödvändiga.

Planerna bör innehålla all nödvändig information som behövs efter aktivering, exempelvis

- uppgifter om mål för återställningstid (RTO) och mål för återhämtningspunkt (RPO)
- detaljer för backuphantering, återställning och återgång till normal drift
- beroenden till andra system och tjänster
- referenser till andra planer och rangordning mellan dessa (undvik att upprepa samma information i flera dokument)
- hårdvaru- och mjukvarukrav för återställning och återgång till normal drift, exempelvis detaljer för licenshantering och konfiguration
- checklistor för validering efter genomförd återställning.

It-organisationen ska även bidra i utvecklingen av verksamhetens kontinuitetsplaner. Reservrutiner, återställningsrutiner och återgångsrutiner för verksamheten kan med fördel beskrivas även i kontinuitetsplaner för it-verksamheten, tillsammans med procedurer för återställning och återgång av infrastruktur. Övning och test av kontinuitetslösningar ska genomföras i nära samarbete med verksamheten; samtliga berörda processer och kontinuitetsplaner ska ingå med siktet inställt på en verklig katastrof. Olika former av övning och test kan användas, se *FSPOS Vägledning för kontinuitetshantering, Appendix H – Test av kontinuitetsplaner* för fler detaljer. Definiera tydliga mål och kritiska framgångsfaktorer vid all planering av övning och test; allt kan inte övas eller testas.

Operativ hantering

I detta processteg ska regelbundet

- utbildning, medvetenhetshöjande och andra kunskapsbyggande aktiviteter genomföras
- granskning och revision genomföras

- övning och test av kontinuitetslösningar genomföras, samt efter större förändringar
- ändringar i kontinuitetslösningar hanteras och kontinuitetsplaner uppdateras därefter.

Nyckelpersoner som har tilldelats en aktiv roll i kontinuitetsarbetet ska erhålla tillbörlig utbildning och övrig personal ska erhålla en allmän medvetenhetshöjande utbildning inom kontinuitet. Granskning och revision av kontinuitetsarbetet inom it-verksamheten ska innefatta samtliga beroenden, inklusive leverantörer. Kritiska kontinuitetslösningar ska övas och testas minst årligen, eller efter större förändringar i organisation eller teknologi. Inkludera alltid verksamheten och krishanteringsfunktionen för dessa test.

Aktivering

I detta processteg ska kontinuitetsplaner aktiveras i händelse av ett allvarligt avbrott eller en katastrof. Det är av avgörande betydelse att kontinuitetsplaner har testats innan aktivering. En aktivering kan medföra stora kostnader, särskilt om en extern lösning eller tjänst används för återställning. Därför ska beslut att aktivera tas av en ledningsfunktion eller krishanteringsfunktion. För kritiska it-tjänster behöver ofta ett snabbt beslut tas för att inte riskera att överskrida it-tjänstens mål för återställningstid (RTO). För dessa it-tjänster rekommenderas att definiera en tidslinje som anger tidpunkt för när ett beslut att aktivera senast ska fattas.

Utgå alltid från att

- beslut att aktivera kan behöva tas när som helst under dygnet, när som helst under året
- det föreligger vissa ledtider under proceduren för återställning, exempelvis inställelse av personal
- allvarliga avbrott eller katastrofer sker när det resulterar i störst konsekvens för verksamheten, och när inte all personal finns på plats
- återställning av it-tjänster innebär hög aktivitet i organisationen med långa arbetspass som resultat, planera därför för 3-skift av personal.

Kom ihåg att

- säkerställa att kontinuitetsplaner alltid finns tillgängliga för berörd personal, även på backupmedia
- återställning av it-tjänster betraktas som en sista utväg när inga andra möjligheter återstår.

2.6.2 COBIT 2019

COBIT är ett allmänt accepterat ramverk som adresserar moderna teknologier, trender och säkerhetskrav för organisationen. Ramverket knyter ihop verksamhetens och it-verksamhetens mål för att överbrygga gap och undvika silos inom organisationen. Fokus ligger på förbättringar inom organisationens it-styrning och harmoniserar med ITIL 2011 och andra ramverk och standarder. COBIT finns även till för att stödja utveckling av policys.

COBIT tillhandahåller verktyg, baserat på *best practice*, som kan anpassas för att mäta mognadsgraden för varje processområde inom organisationen. Dessa processområden är planering och organisation, förvärv och införande, leverans och support, samt övervakning och utvärdering. COBIT har skapats av Information Systems Audit and Control Association (ISACA) och släpptes första gången 1996. Den för närvarande tillgängliga versionen är COBIT 2019.

Vilka krav på kontinuitet ställs?

I denna rapport ligger fokus på processen för *Managed Continuity* då den knyter direkt an till kontinuitet i it-verksamhet. Processen syftar till att etablera och upprätthålla en kontinuitetsplan som möjliggör för verksamheten och it-verksamheten att besvara incidenter och snabbt anpassa sig till avbrott i verksamheten.

COBIT erbjuder möjlighet att mäta mognadsgraden inom *Managed Continuity* och andra processer genom verktyg som kan anpassas efter organisationens behov. Genom att jämföra nuvarande nivå av förmågor i processen mot förväntad nivå erhåller organisationen ett mått på mognadsgrad.

Nedan presenteras de övergripande kraven för alla subprocesser inom *Managed Continuity*. Till varje krav anges referenser till ISO 22301 (kapitel 2.5.1) och ITIL 2011 (kapitel 2.6.1) där motsvarande kvar beskrivs mer i detalj och hur de knyter an till kontinuitetsarbetet i it-verksamheten. COBIT beskriver även *best practices*, vilka inte presenteras här.

Fastställ policy, mål och omfattning

Policy och omfattningen av kontinuitetsarbetet ska fastställas så att de harmoniserar med företagets mål, strategi och dess intressenter. Se avsnitten för *organisationens sammanhang* och *ledarskap* enligt ISO 22301, samt avsnittet för *initiering* enligt ITIL 2011.

Upprätthåll verksamhetens resiliens

Utvärdera olika valmöjligheter för verksamhetens resiliens och välj kostnadseffektiva strategier för kontinuitet och återställning i händelse av ett avbrott eller andra störningar. Se avsnitten för *planering* och *operativ hantering* enligt ISO 22301, samt avsnittet för *kravställning och strategi* enligt ITIL 2011.

Utveckla och fastställ kontinuitetsplaner

Utveckla kontinuitetsplaner och återställningsplaner baserade på strategin. Planerna ska innehålla procedurer och information nödvändiga för kontinuiteten i företagets kritiska aktiviteter. Se avsnitten för *planering* och *operativ hantering* enligt ISO 22301, samt avsnittet för *fastställande* enligt ITIL 2011.

Öva, testa och granska kontinuitetsplaner

Öva och testa kontinuitetsplaner och återställningsplaner regelbundet. Jämför mot förutbestämda resultat och uppmuntra till utveckling av innovativa kontinuitetslösningar för att upprätthålla verksamhetens resiliens över tid. Se avsnittet för *operativ hantering* enligt ISO 22301, samt avsnittet för *operativ hantering* enligt ITIL 2011.

Granska, upprätthåll och förbättra kontinuitetsplaner

Ledningen ska regelbundet granska kontinuitetshanteringsförmågan i syfte att upprätthålla dess ändamålsenlighet, lämplighet och effektivitet. Hantera ändringar enligt en ändringsprocess så att planerna alltid är uppdaterade i enlighet med verksamhetens krav. Se avsnitten för *utvärdering av prestanda* och *förbättringar* enligt ISO 22301, samt avsnittet för *operativ hantering* enligt ITIL 2011.

Genomför utbildningar

Utbilda relevanta interna och externa intressenter regelbundet i procedurer och deras roller och ansvar vid ett avbrott eller andra störningar. Se avsnittet för *stödverksamhet* enligt ISO 22301, samt avsnittet för *operativ hantering* enligt ITIL 2011.

Hantera lösningar för backup

Upprätthåll tillgängligheten av affärskritisk information inom ramen för informationssäkerhetsarbetet. Se avsnitten för *planering* och *operativ hantering* enligt ISO 22301, samt avsnittet för *fastställande* enligt ITIL 2011.

Utför granskning efter aktivering

Bedöm lämpligheten i kontinuitetsplaner och återställningsplaner efter återgång till normal drift i verksamhetsprocesser och tjänster efter ett avbrott. Se avsnitten

för *utvärdering av prestanda* och *förbättringar* enligt ISO 22301, samt avsnitten för *operativ hantering* och *aktivering* enligt ITIL 2011.

2.7 Regelverkens gemensamma nämnare

Det finns en tydlig uppdelning mellan de beskrivna regelverken i denna rapport: de obligatoriska regelverk som upprättas av myndigheter och som aktörer måste följa, och de stödjande regelverk som kan tillämpas av aktörer för standardisering och it-styrning i syfte att nå regelefterlevnad.

Det som förenar de beskrivna regelverken är att samtliga syftar till att hantera den underliggande operativa risken i verksamheten. Det blir tydligt även när kontinuitet i it-verksamheten fokuseras; samtliga grundläggande krav inom kontinuitet för policy, styrning, process och organisation återfinns, explicit eller implicit, i samtliga beskrivna regelverk.

Kartläggningen visar att EBA:s och EIOPA:s riktlinjer överensstämmer i mycket stor utsträckning avseende såväl innehåll som struktur. CPMI-IOSCO:s riktlinjer skiljer sig en del i innehåll och struktur då dessa i större utsträckning utgår från andra globala standarder.

En gemensam nämnare för samtliga regelverk är att de beskriver kraven för kontinuitetshantering utifrån samma referensram, d.v.s. att de följer ett standardiserat sätt att styra och hantera kontinuitetsarbetet. Däremot kan terminologin skilja mellan regelverken.

Finansinspektionens föreskrifter preciserar inte de kontinuitetsrelaterade kraven på samma detaljnivå som övriga regelverk, även om de grundläggande kraven finns beskrivna.

ISO 22301 och ISO 27031 har gemensamt att de kompletterar varandra och därigenom skapar ett mer komplett ledningssystem för informations- och kommunikationsteknologi.

ITIL 2011 och COBIT 2019 skapar tillsammans en helhet genom att ITIL fokuserar på it-styrning genom processer, medan COBIT tillhandahåller konkreta verktyg för hur verksamheten och it-verksamheten ska knytas samman och sträva efter gemensamma mål.

Gemensamt för ISO-standarder och ramverk för it-styrning är att de kan tillämpas samtidigt eller i urval utifrån den gemensamma referensramen. Därigenom kan organisationen välja att tillämpa det eller de stödjande regelverk som är mest relevanta utifrån den egna organisationens verksamhet och förutsättningar.

3 Praktisk tillämpning av regelverk

I detta kapitel beskrivs praktisk tillämpning av regelverken i föregående kapitel hos några aktörer med finansiell verksamhet. Detta kapitel belyser respondenternas bild av *hur*, *när* och *varför* regelverken tillämpas i respektive organisation, samt vilken påverkan de har på det dagliga arbetet med kontinuitet i it-verksamheten.

Totalt har tre intervjuer genomförts med fem respondenter som representerar verksamheter inom försäkring, värdepapper och clearing. Respondenternas huvudsakliga arbetsuppgifter varierar något, även om deras roller och ansvar ryms inom kontinuitetsområdet. En av respondenterna ansvarar för kontinuitetsprocessen för hela organisationen, en ansvarar för verksamhetens riskramverk och utför kontroller, en är högsta ansvarig för cyberresiliens och säkerhetsskydd, en är regelverks- och kontinuitetsansvarig inom ett affärsområde, och en är kontinuitetsansvarig för it-verksamheten och arbetar även med verksamhetens krishantering.

Beskrivningen av tillämpning hos aktörer är strukturerad efter samma gruppering av regelverk som används i föregående kapitel. Intervjuunderlaget innehåller ett antal grundfrågor som gäller samtliga regelverk för att möjliggöra jämförelse, samt fördjupande frågor som anpassats efter respektive grupp av regelverk.

3.1 Resultat av intervjuer

Hur tillämpas regelverken?

Respondent A, organisation med verksamhet inom försäkring

Organisationen har en central GRC-funktion (Governance, Risk management, Compliance) på koncernnivå som ansvarar för utformning av de interna regelverken och genomför omvärldsbevakning. Därutöver har koncernen en funktion som ansvarar för internrevision. Vidare har varje företag i koncernen, inklusive it-organisationen, en egen GRC-funktion som är kontrollerande. Organisationen har även interna diskussionsforum som syftar till att omvärldsbevaka och lyfta fram olika regelverk och diskutera tillämpning. Genom detta upplägg beskrivs organisationen ha en god överblick över aktuella regelverk, deras tolkning och tillämpning.

Regelverk från EBA, EIOPA och ISO lyfts fram som de med störst betydelse för arbetet med kontinuitet i it-verksamheten. De osäkerheter som finns i tolkningen av de nya regelverken, särskilt från EIOPA, sätts upp som risker och hanteras

genom omvärldsbevakning, vilket bedöms vara det enda möjliga i nuläget. It-organisationen har inrättat en särskild funktion för sourcing-frågor som ansvarar för samtliga faser i sourcing-processen, samt säkerställer att samtliga avtalskonstruktioner klassificeras korrekt enligt EBA:s riktlinjer. Även EIOPA:s riktlinjer taktar in i arbetet med sourcing där Finansinspektionens tolkning av EIOPA:s riktlinjer[25] bidrar i det arbetet. Senast i slutet av 2022 måste organisationens samtliga leverantörsavtal ha omförhandlats i enlighet med EIOPA:s nya riktlinjer, vilket bedöms vara en stor utmaning för organisationen.

Ett exempel på konsekvens av EIOPA:s nya riktlinjer för utkontraktering är synen på hur backupdata ska hanteras. Tidigare har failover-tester varit ett vanligt sätt att testa kritiska it-system, men i och med EIOPA:s nya riktlinjer kommer enbart skarp återläsning av data från backup att godkännas. Då Finansinspektionen inte explicit har angivit hur detta krav ska tolkas, kan det i slutändan innebära att samtliga leverantörsavtal behöver omförhandlas av denna anledning. Effekten av sådana tester kan innebära att särskilda GDPR-säkrade testmiljöer behöver byggas upp, vilket kan komma att bli mycket kostnadsdrivande.

Beträffande Finansinspektionens föreskrifter tar organisationens GRC-funktion del av publicerade tillsynsrapporter, sätter upp internkontroller och förbereder åtgärder inför tillsynsmyndighetens inspektioner. FFFS 2014:1 hanteras, tillämpas och kontrolleras av organisationens GRC-funktion, medan FFFS 2014:4 hanteras, tillämpas och kontrolleras av BCM-funktionen. Identifierade kontinuitetsrelaterade risker hamnar hos respondenten för hantering. Även genomförda internkontroller kan leda till åtgärder som behöver hanteras inom ramen för kontinuitet. Finansinspektionens föreskrifter anses betona vikten av och ge ännu större tyngd i arbetet med kontinuitet i it-verksamheten.

ISO 22301 och ISO 27031 bevakas och granskas av organisationens GRC-funktion. ISO-standarderna följs fullt ut och formar processen för kontinuitet. Ett av koncernens företag är certifierat enligt ISO 27001, vilket är ett krav från en av företagets kunder. Resterande företag inom koncernen arbetar i enlighet med ISO 27001, vilket medför att även it-verksamheten arbetar i enlighet med ISO 27001. Standarderna är väl integrerade i verksamheten samtidigt som respondenten poängterar att organisationen fortfarande brottas med samma utmaning som

[25] *https://www.fi.se/sv/publicerat/nyheter/2020/fi-kommer-tillampa-eu-riktlinjer-om-uppdragsavtal-med-molntjanstleverantorer/*

många andra: styrningen finns på plats men den tid som avsätts för tillämpningen av standarderna är inte tillräcklig.

ITIL och COBIT tillämpas i huvudsak som stödjande verktyg i arbetet med kontinuitet i it-verksamheten. Organisationen har sedan tidigare arbetat enligt ITIL3 men denna anses inte längre tillämpbar i och med att ITIL4 släpptes i februari 2019. ITIL4 används främst till att orientera sig och få praktiska råd i tillämpningen av kontinuitet i it-verksamheten. COBIT, å andra sidan, tillämpas främst för att tolka olika regelverk. Detta exemplifieras av arbetet med ISO 22301, där COBIT används för att erhålla svar på frågor som exempelvis hur styrning och samarbete med andra delar i organisationen ska gå till, vilka intressen som är viktiga att beakta i andra delar av organisationen ur ett kontinuitetsperspektiv samt hur viktiga frågeställningar ska bedrivas och få genomslag.

Respondent B, organisation med verksamhet inom värdepapper

Organisationen har en central funktion som ansvarar för interna regelverk. Denna funktion gör omvärldsanalys och tar del av utgivna rapporter och uppdateringar från EBA och andra aktuella regelverk, och anpassar de interna regelverken därefter.

Då utkontraktering är av central betydelse för organisationen, pågår i detta nu ett arbete att anpassa ramverket för utkontraktering baserat på EBA:s riktlinjer. De krav och uppdateringar som gäller kontinuitet analyseras och införs i form av processer och instruktioner som beskriver hur organisationen genomför aktiviteter kopplade till utkontraktering. Exempel på detta är leverantörs- och riskbedömningar, utformning av viktiga frågeställningar kring det praktiska genomförandet, med mera. När kraven i regelverken anpassas till interna kravställningar blir referenserna till EBA:s riktlinjer mindre konkreta, men genom att de interna processerna utformas tillsammans med konkreta nyckeltal, säkerställs att kraven införs korrekt. Införandet av EBA:s riktlinjer är ett pågående arbete i organisationen, där huvudprinciperna redan finns på plats. Sett till ett treårsperspektiv har stora förändringar redan uppnåtts i organisationen genom det förändrade arbetssättet och hanteringen av utkontraktering. För varje år ökar medvetenheten i organisationen, och därigenom mognadsgraden i hanteringen av utkontraktering.

Organisationen berörs inte av Finansinspektionens föreskrifter, men däremot av EU-förordningen Central Securities Depositories Regulation (CSDR) som är motsvarande föreskrift för värdepapperscentraler. CSDR har påskyndat målsättningen och tidplanen för uppfyllande av de övriga regelverken. Tack vare att organisationen är en del av en internationell koncern, har samtliga CSDR-krav

samlats i koncernens gemensamma interna regelverk. Därigenom kan organisationen dra nytta av koncernens stordriftsfördelar och konsumera it-tjänster som lyder under koncernens gemensamma interna regelverk. Organisationen berörs även av CPMI-IOSCO då verksamheten räknas som en finansiell marknadsinfrastruktur (FMI).

Beträffande ISO-standarder tillämpas i första hand ISO 22301 och ISO 27031 för hanteringen av kontinuitet i it-verksamheten. Även ISO 27001 har stor betydelse för hanteringen av informationssäkerhet. Organisationen har genomfört en fullständig anpassning till ISO 27001, även om en del arbete återstår ur ett medvetande- och mognadsperspektiv. ISO-standarderna tillämpas och kommuniceras via policys, riktlinjer och procedurer. I dagsläget är organisationen inte certifierad i någon av ISO-standarderna.

Organisationen har antagit ett ramverk som kallas Technology Framework. Detta innefattar en anpassning av verksamhetens arbetssätt enligt de processer som COBIT förhåller sig till, även om COBIT ännu inte är helt och hållet integrerat i verksamheten. Technology Framework har fått stor betydelse för styrningen av it-verksamheten, som därigenom har fått en ny verktygslåda att förhålla sig till och som är enkel att kommunicera. Respondenten lyfter fram Technology Framework som en viktig förändring i synsättet på it-organisationen; från att se it-organisationen som ett rent cost-center till att bli en leverantör av affärsnytta. I förändringsarbetet behövs en kommunikationsplattform och i det sammanhanget lämpar sig COBIT särskilt väl att luta sig mot.

Kravställningarna inom Technology Framework utgår ifrån bland annat ISO 27001, medan it-styrningen är helt och hållet anpassad efter COBIT. Medan COBIT är styrande i arbetet med kontinuitet i it-verksamheten, anser respondenten att ITIL är mer av en informell vägledning för styrning av it-tjänster och dess utformning, och används därmed inte för formell it-styrning inom organisationen. Anpassningen till ISO 27001 har dock kommit längre än införandet av Technology Framework.

Organisationen använder FFIEC (Federal Financial Institutions Examination Council) som referensramverk för att utvärdera sina kontroller inom ramen för informationssäkerhetsarbetet. Där ingår bland annat kontroller för incidenthantering, återställning av system och tjänster, återgång till normal drift, samt backuphantering.

Respondent C, organisation med verksamhet inom clearing

Organisationen har en central risk- och compliance-funktion som ansvarar för interna regelverk. De interna regelverken genererar de krav, inom ramen för

kontinuitet, som organisationen behöver förhålla sig till och följa. De interna regelverken är väl integrerade i verksamheten, även om de hanteras hos olika avdelningar och roller inom organisationen. Den centrala risk- och compliance-funktionen genomför internrevision på arbetet med kontinuitet, till viss del tas även hjälp av externa revisorer. Genom detta förfarande säkerställs att de interna regelverken, som VD har fastställt, följs. Den centrala risk- och compliance-funktionen ansvarar även för att göra omvärldsanalys och ta del av utgivna rapporter och uppdateringar för de aktuella regelverken.

EBA, CPMI-IOSCO och Finansinspektionens föreskrifter anges vara viktiga regelverk för organisationens verksamhet. Särskilt CPMI-IOSCO:s riktlinjer anges vara kravställande i arbetet med kontinuitet. Beträffande Finansinspektionens föreskrifter, är FFFS 2014:4 direkt omsatt i de interna regelverken då dessa explicit refererar till dessa föreskrifter. FFFS 2014:5 däremot ligger till grund för de interna regelverken men saknar explicit referens.

ISO 22301 och ISO 27031 ligger också till grund för de interna regelverken även om de inte, i likhet med FFFS 2014:5, refereras till explicit. I de interna regelverken står att organisationen ska tillämpa standarder för ledningssystem på ett för organisationen lämpligt och effektivt sätt. Målet är att uppnå full compliance med ISO 22301 och ISO 27031 på sikt. Organisationen bedömde sig inte kunna nå full compliance med ISO-standarder på egen hand, då it-organisationen var relativt liten. Detta ledde till ett beslut att utkontraktera it-driften till leverantörer som har ISO-certifieringar, och därigenom stärka förmågan till leverantörsstyrning av dessa. I dagsläget är organisationen inte certifierad i någon av ISO-standarderna.

ITIL 2011 används för de flesta relevanta processer och ansvariga har utsetts till dessa. I rollen som kontinuitetsansvarig för it-verksamheten ingår även processansvar för IT Service Continuity Management och Capacity Management. Vidare är it-verksamhetens SIAM-organisation[26], inom vilken ansvaret för organisationens kontinuitet i it-verksamheten ingår, i sin helhet utformad efter ITIL 2011. Tidigare tillämpade it-verksamheten främst processerna för Incident Management, Problem Management och Change Management, men i samband med att it-verksamheten introducerade SIAM-organisationen, togs beslutet att tillämpa ITIL:s samtliga processer och roller inom organisationen.

[26] *Service Integration and Management (SIAM), en metod för styrning av flera leverantörer av affärs- och it-tjänster, där dessa integreras och tillsammans skapar en affärsmässig it-verksamhet.*

När tillämpar ni regelverken?

Respondent A, organisation med verksamhet inom försäkring

Organisationen tillämpar de interna regelverken kontinuerligt. De interna regelverken är skrivna på en förhållandevis allmän och hög nivå, vilket skapar ett visst tolkningsutrymme och spelrum i hur och när de ska tillämpas. Utkontrakteringsprocessen lyfts återigen fram som ett exempel på när regelverken används som ett praktiskt verktyg i den dagliga verksamheten.

Utträdeskraven i EBA:s och EIOPA:s riktlinjer nämns som ett särskilt fokusområde, där respondenten tillsammans med organisationens jurister går igenom hur kontinuiteten kan garanteras under ett utträde. Mycket fokus riktas mot dessa krav ur ett process- och styrningsperspektiv för att minimera risken för ett krisläge om organisationen byter leverantör av kritiska it-tjänster. De RFI:er (Request For Information) som skickas ut till leverantörer idag innehåller frågeställningar direkt kopplade till regelverken. Organisationens bidrag är att avgöra vilka krav som ska anses vara skall- eller börkrav. Om det finns ett gap mellan organisationens önskemål och leverantörens förmåga, hanteras detta gap genom riskhantering.

ISO 22301 ligger till grund för den årliga översynen av kontinuitetsprocessen samt för kravställning på framtagande av exempelvis övnings- och testprotokoll. ISO-standarderna generellt har även bidragit till att organisationen de facto använder systemens och tjänsternas återställningsplaner vid allvarliga incidenter.

Respondent B, organisation med verksamhet inom värdepapper

Återigen betonas EBA:s riktlinjer för utkontraktering vara av central betydelse för organisationen då huvuddelen it-tjänsterna driftas av leverantörer. Generellt finns en stor komplexitet i EBA:s riktlinjer när företag inom en koncern har olika förutsättningar. Ett sådant exempel är riktlinjer för riskbedömningar, som inte kan hanteras enbart inom det egna företaget, utan behöver hanteras i en större kontext. Givet organisationens affärsmodell, förekommer även situationer när EBA:s riktlinjer inte anses vara tillräckliga vid riskbedömningar, och då krävs en mer utvecklad analysmodell än vad som kravställs i riktlinjerna.

ISO 27001 är tillämpbar för samtliga medarbetare som arbetar aktivt med informationssäkerhet eller teknologi, då standarden är bred i sin tillämpning. ISO 27001 har sin tyngd i de tekniska verksamheterna i allmänhet och it-organisationen i synnerhet. De kontroller som avser kontinuitet hanteras av verksamhetens ansvariga för resiliens, som säkerställer att verksamheten har

identifierat sina kritiska processer, samt att de tekniska verksamheterna, inklusive it-verksamheten, uppfyller kravställningarna. Till stöd för kontinuitetsarbetet finns även kontinuitetskoordinatorer ute i verksamheten.

COBIT anses också vara tillämpbar i det dagliga arbetet då den syftar till att it-verksamheten är i linje med verksamhetens strategi, mål och behov; därmed blir it-verksamheten en uttalad service-organisation.

Respondent C, organisation med verksamhet inom clearing

Finansinspektionens föreskrifter har stor betydelse för organisationens hantering av deltagarkrav. Organisationens skyldigheter gentemot regering och myndigheter för säkerställande att deltagarna följer deltagarkraven, leder till ytterligare krav på den egna it-verksamheten, i egenskap av ägare och förvaltare av en kritisk tjänst inom sektorn. Dessa krav innefattar bland annat hantering och utvärdering av deltagarnas kontinuitet som görs regelbundet och riskbaserat.

Internt följer it-verksamheten upp hanteringen av kontinuitet genom årliga leverantörsuppföljningar, där leverantörerna åläggs att förklara hur de har byggt upp och säkrat sin egen kontinuitet. Det finns även möjlighet för it-verksamheten att erhålla hjälp genom extern revision av en leverantör om det finns särskilda skäl. It-verksamhetens huvudsakliga roll, ur ett kontinuitetsperspektiv, är att styra och övervaka leverantörerna, vilket är både resurs- och kostnadskrävande.

Varför tillämpar ni regelverken?

Respondent A, organisation med verksamhet inom försäkring

Övergripande, menar respondenten, handlar det främst om regelefterlevnad och av konkurrensskäl. Lägg därtill lika delar värdegrund, där företaget vill vara ”bäst i klassen”, och grundläggande ”hygienfaktorer” genom den typ av reglerad verksamhet som organisationen bedriver. Förtroendet och anseendet hos kunder, leverantörer och branschkollegor står i centrum; de regulatoriska kraven måste helt enkelt uppfyllas. Ett negativt nedslag från en tillsyn, som kommer ut i media, vore mycket olyckligt och kostsamt.

ISO 22301, ITIL4 och COBIT betonas vara avgörande instrument i arbetet för respondenten, då samtliga utgör viktiga hjälpmedel och verktygslådor som används i det dagliga arbetet med kontinuitet i it-verksamheten. Utan ISO-standarderna hade det varit svårt att utforma en fungerande kontinuitetprocess och samtidigt hävda vikten av kontinuitetsarbetet.

Respondent B, organisation med verksamhet inom värdepapper

Givet den verksamhet som organisationen bedriver och beroendet av it-tjänster, är EBA:s riktlinjer för utkontraktering särskilt viktiga, då tydliga riktlinjer behövs för arbetet med utkontraktering och kontinuitet. Genom att tillämpa dessa regelverk uppnås målet att erhålla hög resiliens i verksamheten. Vidare anses en organisation, som kan beskrivas genom välkända regelverk, ha lättare att förhålla sig till de kontroller som förväntas vara införda. I slutändan är syftet med regelverken att kunna hantera verksamhetens operativa risker.

Respondent C, organisation med verksamhet inom clearing

ITIL 2011 tillämpas i verksamheten då det är en erkänd standard som bland annat beskriver hur it-verksamheten ska utformas till en beställarorganisation som inrymmer ett flertal leverantörer. It-verksamheten har valt att tillämpa ITIL 2011 fullt ut i syfte att underlätta den operativa hanteringen och styrningen av leverantörer, då ITIL 2011 även tillämpas av leverantörerna. ITIL 2011 främjar arbetet med kontinuitet i it-verksamheten genom att det blir tydligt vilka interna roller som ska kommunicera med vilka externa roller hos leverantören. Det blir även tydligt vilka andra it-processer som kontinuitetsprocessen behöver interagera med. ITIL 2011 anses ha höjt organisationens förmåga inom kontinuitet avsevärt.

4 Avslutande reflektioner

Regelverken som beskrivs i denna rapport har stor betydelse för arbetet med kontinuitet i it-verksamheten för aktörer i den finansiella sektorn. De nya regelverken från EBA, EIOPA och CPMI-IOSCO är särskilt betydelsefulla då dessa ligger till grund för utformningen av de interna regelverken. ISO-standarderna har stor betydelse för utformning av processer och kontrollramverk. ITIL lämpar sig för alla typer av organisationer som eftersträvar en standardiserad och leverantörsgemensam it-förvaltning. COBIT används mer för praktisk it-styrning i det dagliga arbetet och säkerställer att it-organisationen stödjer verksamhetens strategi och mål.

De nya regelverken har medfört en ökad tydlighet i kraven för exempelvis informationssäkerhet och utkontraktering. En generell utmaning med de nya regelverken är hur kraven ska tolkas och omsättas i praktisk tillämpning, särskilt eftersom regelverken i viss utsträckning överlappar varandra. En utmaning som lyfts fram i intervjuerna är konsekvensen av de nya kraven inom utkontraktering, som innebär att gamla leverantörsavtal behöver skrivas om i enlighet med de nya kraven. För finansiella marknadsinfrastrukturer (FMI:er) har Europeiska centralbanken (ECB) tagit fram ett omfattande stöd för tolkning av regelverk, *Cyber resilience oversight expectations for financial market infrastructures (CROE)*[27], som utgår från och konkretiserar CPMI-IOSCO:s riktlinjer, ISO 27001, COBIT 5, med flera regelverk.

En generell trend inom reglering av it-verksamhet är att regelverken blir både fler och mer detaljerade. Ytterligare regelverk som berör områdena it- och cybersäkerhet för finanssektorn är under framtagning. EU-kommissionen har hösten 2020 presenterat ett förslag till förordning *Digital Operational Resilience for the Financial Sector (DORA)*[28] som är en åtgärd som ryms inom kommissionens strategi *Digital Finance Strategy*[29]. Denna riktar sig till ett stort antal finansiella företag och ställer omfattande krav på bland annat organisation och styrning av it-risker, hantering och rapportering av it-incidenter, genomförande av tester av förmågan att hantera störningar och cyberangrepp samt krav på tredjeparts leverantörer. När förordningen genomförs kommer den ligga till grund för utformning av nya riktlinjer, så kallade ”tekniska standarder”, som de

[27] *https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr181203_1.en.html*

[28] *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2020:595:FIN&from=EN*

[29] *https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en*

europeiska tillsynsmyndigheterna för bank-, försäkrings- och värdepappersverksamhet kommer att utarbeta.

Betydelsen av kontinuitet i it-verksamheten inom finanssektorn växer i takt med ökade krav på cyberresiliens, vilket bekräftas av de nya regelverken. Samtidigt sker teknikutvecklingen i snabb takt med ett tilltagande fokus på automation och virtualisering, vilket medför ytterligare utmaningar för ansvariga inom kontinuitetsområdet. En positiv trend är verksamhetens förändrade förhållningssätt från att se it-verksamheten som en kostnad till att bli en leverantör av affärsnytta. Detta innebär ökade möjligheter att integrera it-verksamheten i i den övergripande verksamheten för att skapa affärsnytta genom att upprätthålla kontinuiteten i organisationens kritiska processer.

Det kan konstateras att olika organisationer har valt olika angreppssätt i arbetet med kontinuitet i it-verksamheten, där både organisatorisk tillhörighet och ansvarsfördelning skiljer sig åt. Gemensamt bland respondenterna är uppfattningen att funktioner med ansvar för kontinuitet i it-verksamheten bör placeras centralt inom organisationen.

Givet komplexiteten till följd av den ökade mängden regelverk och den snabba teknikutvecklingen inom området, blir vikten av rätt kompetens inom kontinuitetsarbetet allt viktigare. Det räcker inte med kunskap om innehåll och tolkning av regelverken, kraven behöver kunna omsättas i praktisk tillämpning där processer, kontroller och åtgärder är integrerade med verksamhetens riskhantering.

Bilaga A – Referenslista

Kartlagda regelverk

- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)
- EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)
- EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)
- EIOPA Guidelines on Information and Communication Technology security and governance (EIOPA-BoS-19-526)
- CPMI-IOSCO Principles for financial market infrastructures (PFMI)
- CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure
- FFFS 2014:4 – Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker
- FFFS 2014:5 – Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem
- ISO 22301:2019 – Business continuity management systems – Requirements
- ISO 27031:2011 – Guidelines for information and communication technology readiness for business continuity
- ITIL 2011 – Information Technology Infrastructure Library
- COBIT 2019 – Control Objectives for Information and Related Technologies

Övriga regelverk, lagar och förordningar

- FSPOS Vägledning för kontinuitetshantering, Appendix F – Kontinuitetshantering för IT-verksamheten
- FSPOS Vägledning för kontinuitetshantering, Appendix H – Test av kontinuitetsplaner

- PSD2-direktivet (Revised Payment Services Directive)
- Solvens II-direktivet (om upptagande och utövande av försäkrings- och återförsäkringsverksamhet)
- FFFS 2007:16 – Finansinspektionens föreskrifter om värdepappersrörelse
- FFFS 2014:1 – Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut
- Lag (1995:1571) om insättningsgaranti
- Förordning (EU) nr 1093/2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten)
- EU-förordning General Data Protection Regulation (GDPR)
- EU-förordning Central Securities Depositories Regulation (CSDR)
- EU-förordning Digital Operational Resilience for the Financial Sector (DORA)
- Cyber resilience oversight expectations for financial market infrastructures (CROE) – utgiven av Europeiska centralbanken (ECB)
- MSB:s Metodstöd för systematiskt informationssäkerhetsarbete
- FFIEC (Federal Financial Institutions Examination Council) Cybersecurity Framework
- ISO 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

Länkar

- Finansinspektionens frågor och svar om utlagd verksamhet
  https://www.fi.se/sv/bank/utlagd-verksamhet/
- Finansinspektionens nyheter: FI tillämpar riktlinjer för utkontraktering, 2019-07-04
  https://www.fi.se/sv/publicerat/nyheter/2019/fi-tillampar-riktlinjer-for-utkontraktering/

- Finansinspektionens nyheter: FI tillämpar riktlinjer för hantering av IKT- och säkerhetsrisker, 2020-05-26
https://www.fi.se/sv/publicerat/nyheter/2020/fi-tillampar-riktlinjer-for-hantering-av-ikt--och-sakerhetsrisker/

- MSB:s Metodstöd för systematiskt informationssäkerhetsarbete
https://www.informationssakerhet.se/metodstodet/

- Finansinspektionens nyheter: FI tillämpar EU-riktlinjer om avtal med molntjänstleverantörer, 2020-08-20
https://www.fi.se/sv/publicerat/nyheter/2020/fi-kommer-tillampa-eu-riktlinjer-om-uppdragsavtal-med-molntjanstleverantorer/

- Riksbankens översikt över den finansiella infrastrukturen
https://www.riksbank.se/en-gb/financial-stability/the-financial-system/the-financial-infrastructure/

- Finansinspektionens nyheter: Tillsynen av finansiell infrastruktur fungerar väl, 2014-03-27
https://www.fi.se/sv/publicerat/nyheter/2014/tillsynen-av-finansiell-infrastruktur-fungerar-val/

- Riksbankens publicering av Financial Infrastructure Report
https://www.riksbank.se/en-gb/press-and-published/publications/other-former-publications/financial-infrastructure-report/

- Finansinspektionens översikt över regler för olika företagstyper
https://www.fi.se/sv/bank/regler/

- Europeiska centralbankens pressmeddelande: ECB publishes the cyber resilience oversight expectations, 2018-12-03
https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr181203_1.en.html

- EU-kommissionens förslag till förordning Digital Operational Resilience for the Financial Sector (DORA)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2020:595:FIN&from=EN

- EU-kommissionens publicering av Digital finance package
https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en