FSPOS

FSPOS Vägledning för kontinuitetshantering

Version 6.0, 2024-06-27

FSPOS Arbetsgrupp Kunskapsspridning

2024-06-27

Dokumenthistorik

Utgåva	Datum	Kommentar
1.0	2013-12-16	Första utgåva av FSPOS Vägledning för kontinuitetshantering.
2.0	2014-09-18	Mindre justeringar i huvuddokument. Ny version: Appendix F - Kontinuitetshantering för it-verksamheten. Nytt appendix: Appendix G - Kontinuitetshantering för outsourcad verksamhet. Nytt appendix: Appendix H – Självskattningsformulär.
3.0	2017-01-24	Mindre justeringar i huvuddokument samt kompletterad med senaste versioner av Appendix F - Kontinuitetshantering för it-verksamheten, Appendix G - Kontinuitetshantering för outsourcad verksamhet samt Appendix H – Självskattningsformulär.
4.0	2019-03-14	Inkludering av begreppet ”Produkter och tjänster” som stöd för urval av processer. Komplettering av metod för identifiering och urval av kritiska processer. Beskrivning av begreppet ”Resilience” i relation till risk-, kris- och kontinuitetshantering. Förtydligande beskrivning av Kriteriemodell. Uppdatering av Konsekvensanalys; metodbeskrivning och mallar. Uppdatering av Riskbedömning; metodbeskrivning och mallar. Förtydligande kring begreppen RTO och RPO. Uppdatering av kapitlen *Styrande dokument* och *Analys av verksamheten* till följd av ovanstående ändringar. Redaktionella justeringar i huvuddokument till följd av ovanstående ändringar.

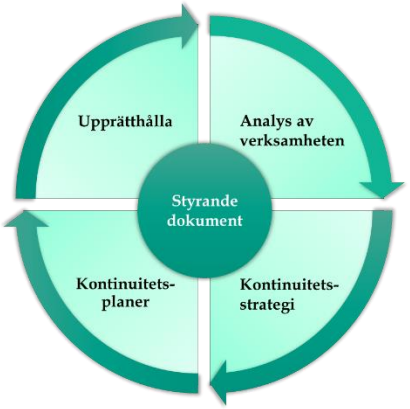
5.0	2021-03-16	Nytt Appendix H - Test av kontinuitetsplaner. Förtydligande beskrivning av begreppen övning och test. Tillägg genomgående i vägledningen om återställningstid även på aktivitetsnivå utifrån uppdateringar i ISO-standard. Ändringar i Appendix E gällande övning och test. Uppdatering av gällande lagstiftningar och standarder. Självskattningsformulär samt begrepps - och referenslista lagda utanför övriga appendix för att göra plats för eventuella nya appendix. Redaktionella justeringar i huvuddokument till följd av ovanstående ändringar.
6.0	2024-06-27	Löpande redaktionella justeringar i samtliga Appendix, inklusive anpassning till FSPOS nya grafiska profil. Uppdatering av gällande lagstiftning och standard. Uppdaterad begreppslista. Nya avsnitt avseende kontinuitetshantering och kopplingen till närliggande discipliner. Revideringar i Appendix B avseende samtliga steg i konsekvensanalys och riskbedömning. Nya avsnitt i Appendix B avseende tillämpning av perspektiv informationssäkerhet. Nytt självskattningsformulär som har uppdaterats och finns publicerat som ett separat Excel-dokument på FSPOS hemsida. Redaktionella justeringar i huvuddokument till följd av ovanstående ändringar.

Sammanfattning

I FSPOS tidigare arbete har ett behov av en vägledning i kontinuitetshantering identifierats. *FSPOS vägledning för kontinuitetshantering* syftar till att tillfredsställa behovet genom att beskriva processen för kontinuitetshantering. Som ytterligare stöd till aktörer i den finansiella sektorn inkluderar vägledningen också metodbeskrivningar, mallar och exempel för arbetet med kontinuitetshantering. Vägledningen baseras på den internationella standarden inom kontinuitetshantering; *ISO 22301– Security and resilience – Business continuity management systems.*

Externa krav på kontinuitetshantering regleras i ett antal föreskrifter från olika tillsynsmyndigheter. Denna vägledning tolkar, beskriver och ger ett stöd för vad som kan göras för att på ett metodiskt sätt uppnå efterlevnad. Med kontinuitetshantering menas kortfattat den process som säkerställer att organisationen har en robusthet och förmåga att driva den kritiska verksamheten på en tolerabel nivå oavsett vilka störningar som inträffar. Syftet med kontinuitetshantering är att identifiera kritiska delar av verksamheten och därefter skapa och säkerställa robusthet i dessa delar, med målsättningen att säkra leveransförmågan vid störningar.

Processen för kontinuitetshantering kan illustreras enligt bilden till höger. Centralt finns **STYRANDE DOKUMENT** som syftar till att utgöra grund för hur organisationen ska arbeta med kontinuitetshantering, till exempel genom tillsättandet av ansvariga individer, definition av syfte och mål, framtagande av en kriteriemodell samt avgränsningar och utgångspunkter.



I steget **ANALYS AV VERKSAMHETEN** identifieras verksamhetens kritiska delar. Tidskrav för hur länge verksamheten kan vara utan dessa delar definieras. Därefter genomförs en riskbedömning för att avgöra huruvida befintliga lösningar är tillräckliga för att möta definierade tidskrav. Analysen kan även innefatta identifiering av informationstillgångar och dess beroenden gentemot informationsbärande resurser. Nästa steg är att definiera **KONTINUITETSSTRATEGIER**. Detta handlar om att upprätta strategier för hur kontinuiteten ska kunna upprätthållas för de identifierade kritiska delarna av verksamheten. I steget **KONTINUITETSPLANER** identifieras och dokumenteras kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner för de kritiska delarna av verksamheten. Kontinuitetslösningarna beskrivs konkret och tydligt för att kunna användas under en störning.

UPPRÄTTHÅLLA handlar om att utbilda, öva, testa, revidera och granska det material och de arbetsprocesser som finns inom ramen för kontinuitetshantering. Dels för att säkerställa att framtaget material är relevant och uppdaterat och dels för att skapa en medvetenhet i organisationen kring kontinuitetshantering.

Innehållsförteckning

1 Inledning

Denna vägledning har utvecklats av Arbetsgrupp Kunskapsspridning (AG KUN) inom Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS) i syfte att, utifrån god praxis, ge aktörer inom den finansiella sektorn stöd beträffande hur organisationen kan arbeta med utveckling, implementering och uppföljning av kontinuitetsarbetet. Många aktörer i den finansiella sektorn har verksamhet som är samhällsviktig och/eller mycket tidskritisk varför ett strukturerat arbete med kontinuitetshantering är relevant.

I de fall material från denna vägledning används eller visas i andra sammanhang ska källhänvisning göras enligt följande: *FSPOS Vägledning för kontinuitetshantering (2024)*.

Vid eventuella synpunkter på vägledningen finns kontaktinformation på FSPOS hemsida *www.fspos.se*.

1.1 Läsanvisningar

Vägledningen inleds med avsnittet inledning, där bakgrund, utgångspunkt och målgrupp för dokumentet presenteras. Därefter ges en introduktion till kontinuitetshantering, där beskrivningar av nyttan med samt kravställning gällande kontinuitetshantering för olika typer av finansiella aktörer ingår. I avsnittet beskrivs även kopplingen till de närliggande områdena incident-, risk-, och krishantering. Det efterföljande avsnittet beskriver processen för kontinuitetshantering på en övergripande nivå. I Appendix A-E beskrivs därefter respektive steg i kontinuitetshanteringsprocessen på en mer djupgående nivå, genom beskrivning av vad steget innebär och förslag på hur det kan genomföras tillsammans med förslag på mallar och exempel.

Eftersom de flesta aktörerna i den finansiella sektorn har ett starkt beroende till it finns ett specifikt appendix som beskriver hur kontinuitetshantering kan bedrivas för de it-system och -tjänster som verksamheten är beroende av; Appendix F. I Appendix G beskrivs hur aktörerna kan arbeta med kontinuitetshantering vid outsourcing. Appendix H innehåller ett stöd i hur tester av verksamhetens kontinuitetsplaner kan planeras, genomföras och utvärderas.

Som ett komplement till denna vägledning finns ett självskattningsformulär. Självskattningsformuläret kan användas som stöd vid bedömning av nivå av förmåga hos den egna verksamheten. Självskattningsformuläret finns publicerat som ett separat excel-dokument på FSPOS hemsida.

1.2 Utgångspunkt

Behovet av stöd inom kontinuitetshantering har tidigare identifierats inom FSPOS arbetsgrupper, där aktörer i finansiella sektorn har efterfrågat en tydlig och praktisk vägledning inom kontinuitetshantering. För att identifiera sektorns behov av stöd inom kontinuitetshantering samt för att hämta inspiration och goda exempel genomfördes inledningsvis en förstudie. Förstudien baserades på (i) en intervjuundersökning med aktörer inom den finansiella sektorn, (ii) resultatet av en workshop (iii) samt litteraturstudier. Förstudien klargjorde bland annat att sektorns aktörer ser ett behov av tydligare och mer praktisk vägledning inom kontinuitetshantering. Befintliga standarder inom området beskriver ofta *vad* som ska innefattas i arbetet på en övergripande nivå utan konkreta exempel och praktiskt stöd för genomförande. Detta har ofta inneburit att finansiella aktörer antingen saknar nödvändiga verktyg eller själva har utvecklat egna lösningar och tolkningar av standarder, vilket i sin tur medför att sektorns aktörer arbetar på olika sätt.

En central utgångspunkt för vägledningen har därför varit att komplettera befintliga standarder och vägledningar inom området genom att beskriva *hur* arbetet kan genomföras.

Sedan 2012 finns en internationell standard för kontinuitetshantering som beskriver kraven på god kontinuitetshantering, *ISO 22301.*[1] En tillhörande vägledning, *ISO 22313*[2], beskriver något mer konkreta riktlinjer kring genomförandet av kontinuitetshantering. Ytterligare en standard innehåller riktlinjer kring kontinuitetshantering, kopplat till it- och kommunikationsteknologi, *ISO/IEC 27031.*[3]

Denna vägledning utgår från ISO-standarderna för kontinuitetshantering, inklusive den terminologi som standarderna använder. Syftet med FSPOS vägledning är dock inte att vara ett verktyg för hur organisationer kan certifiera sig mot ISO 22301. Även om innehållet i huvudsak överensstämmer med standarden har det främsta syftet varit att stärka finansiella aktörers arbete med utveckling, implementering och uppföljning av kontinuitetshantering.

Initiativ har tagits för att konkretisera standardernas innehåll, såsom *Good Practice Guidelines* (GPG)[4] från Business Continuity Institute. GPG är inte anpassad för någon särskild sektor och innehåller inte exempelmallar och konkreta exempel i någon större utsträckning, såsom efterfrågats av finansiell sektor i ovan nämnda förstudie till denna vägledning. FSPOS vägledning har hämtat viss inspiration från GPG.

1.3 Målgrupp

Målgruppen för FSPOS vägledning är samtliga aktörer inom finansiella sektorn, såväl företag som myndigheter samt såväl stora som små organisationer. Vägledningen är tänkt att kunna användas av samtliga som är involverade i processen för kontinuitetshantering. Vägledningen vänder sig således till verksamhetsansvariga, säkerhetsansvariga, ansvariga för kontinuitetsarbete, men även till aktörernas ledning. Vägledningen är framförallt utformad för de som arbetar med kontinuitetshantering men är även tänkt att kunna utgöra ett underlag för att skapa medvetenhet om kontinuitetshantering och för att förankra behovet av att arbeta med dessa frågor inom organisationen.

Många av sektorns aktörer har sedan länge arbetat med kontinuitetshantering och har ett väl implementerat arbetssätt för området. För dessa organisationer kan denna vägledning bidra med inspiration, eller användas för att jämföra sig mot. Andra finansiella aktörer har ännu inte uppnått samma mognad. För dessa organisationer kan vägledningen användas för att från grunden utveckla, implementera och följa upp kontinuitetsarbetet. Vägledningen försöker ge stöd till organisationer med olika behov och mognad inom kontinuitetshantering. I vägledningen ges stöd och exempel på hur kontinuitetshanteringen kan byggas gradvis. Detta då ambitionsnivå och möjlighet till mogna inom kontinuitetshantering skiljer sig mellan olika organisationer.

---

[1] *ISO 22301 - Security and resilience – Business continuity management systems – Requirements.*

[2] *ISO 22313 - Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301.*

[3] *ISO/IEC 27031 - Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.*

[4] *Business Continuity Institute (BCI)- Good Practice Guidelines– Global edition.*

2 Introduktion till kontinuitetshantering

Drivkrafterna till varför en organisation arbetar med kontinuitetshantering kan vara många och kan vara internt drivna av exempelvis organisationens egen ambition och mål. Drivkrafterna kan även vara externa krav från bland annat lagkrav, kundkrav, rykte eller förändringar i marknad och omvärld.

Detta avsnitt beskriver vad kontinuitetshantering är och vilken nytta som kan uppnås genom ett effektivt arbete inom området. Exempelvis beskrivs hur organisationens måluppfyllnad stöds av en effektiv kontinuitetshantering, genom att verksamheten kan upprätthållas på en acceptabel nivå oavsett vilka störningar som inträffar. Därigenom kan organisationen i förlängningen skydda intressenter, rykte, varumärke och värdeskapande aktiviteter.

Avsnittet beskriver även ett antal förväntningar som ställs på finansiella aktörer avseende kontinuitetshantering, genom exempelvis avtal, föreskrifter, lagkrav och allmänna råd.

Avslutningsvis söker avsnittet beskriva skillnader och samband mellan kontinuitetshantering och ett antal besläktade discipliner, såsom risk-, incident- och krishantering. Även kontinuitetshanteringens kopplingar mot informationssäkerhet, totalförsvar och organisatorisk resiliens beskrivs i avsnittet. Dessa discipliner kan upplevas som överlappande och kan ibland vara svåra att separera från varandra.

2.1 Vad är kontinuitetshantering?

Förenklat kan kontinuitetshantering beskrivas som den process som säkerställer att organisationen kan driva sin kritiska verksamhet på tolerabel nivå, oavsett vilka störningar som inträffar.[5] Med detta menas att organisationen minskar sin sårbarhet och ökar sin motståndskraft mot olika händelser som kan påverka den kritiska verksamheten. Aktuell vägledning kommer att utgå från denna definition, samt även i så stor utsträckning som möjligt använda begrepp och definitioner från ISO 22301.

2.2 Nyttan med kontinuitetshantering

Nyttan med kontinuitetshantering kan dels beskrivas genom den effekt som arbetet kan få på organisationens förmåga att upprätthålla verksamheten och därigenom tillgodose sina mål. Nyttan kan också beskrivas i termer av vilka fördelar kontinuitetshantering har som process och metod, genom ett systematiskt och strukturerat arbetssätt.

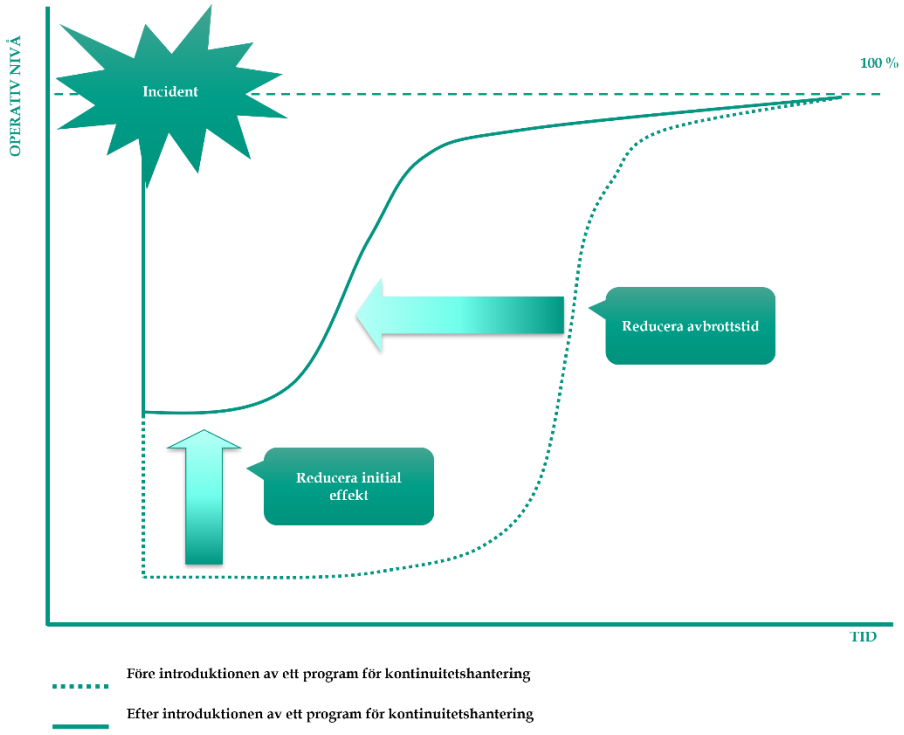
Det övergripande syftet med kontinuitetshantering är att identifiera kritiska delar av verksamheten, såsom kritiska produkter och tjänster eller processer, och därefter skapa och säkerställa robusthet i dessa delar, med målsättningen att säkra leveransförmågan vid störningar.

Ökad robusthet medför förbättrad förmåga att förebygga, bemöta och återhämta sig från störningar och avbrott. Arbetet med kontinuitetshantering syftar därmed till att skapa en handlingsberedskap och kontinuitetsförmåga inom organisationen, det vill säga att säkerställa att organisationen har tillräcklig kunskap för att förebygga och hantera avbrott i verksamheten.

---

[5] *SS-EN ISO 22301 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Krav.*

Ett sätt att visualisera nyttan med kontinuitetshantering illustreras i diagrammet nedan. Som visas i bilden är det främst två effekter som uppnås genom arbete med kontinuitetshantering. Konsekvenserna som organisationen drabbas av i händelse av en störning minskar, dels genom att minimera störningens påverkan på den operativa nivån, och dels genom att korta ner avbrottstiden.



Även om det övergripande målet med kontinuitetshantering är att minska konsekvenserna av avbrott och avbrottstider bör det påpekas att målsättningen i förlängningen är att skydda organisationens intressenter, rykte, varumärke och värdeskapande aktiviteter. På så vis kan nyttan med kontinuitetshantering innebära stärkt uppfyllnad av ett stort antal mål som satts upp av verksamheten, såsom efterlevnad av lagar och krav, finansiella mål samt egna mål för exempelvis kundnöjdhet.

Ekonomisk nytta uppnås bland annat genom att mitigera risker och att investeringar i robusthetshöjande åtgärder kan optimeras. Genom minskade kostnader i samband med avbrott och störningar stärks lönsamheten. Ytterligare ekonomisk nytta kan ges genom lägre försäkringspremier för organisationer som kan påvisa arbete med kontinuitetshantering.

En stor risk för många organisationer är störningar i kassaflöde, som är beroende av att produkter och tjänster är tillgängliga. Genom att skapa robusthet i de processer som stödjer verksamhetens kritiska produkter och tjänster, stärks därmed även organisationens kassaflöde.

Arbetet med kontinuitetshantering kan utgöra en värdefull signal till kunder och andra intressenter för att stärka förtroendet för den egna organisationen. Därutöver är det oftast billigare att behålla kunder genom förebyggande och bättre hantering av avbrott än att vinna tillbaka förlorade kunder. En stärkt förmåga med stöd av kontinuitetshantering kan innebära fördelar i en konkurrenssituation.

En utmaning för många aktörer inom sektorn är även att säkerställa kritiska leveranser från leverantörer och tredjepart. Kontinuitetshantering understryker behovet av externa beroenden och försöker säkerställa sådana leveranser genom upprättande av lämpliga strategier och avtal för att kunna säkerställa kontinuitet.

Ett annat kritiskt område är säkerställande av personal. Kontinuitetshanteringen kan exempelvis inbegripa upprättande av beredskapsavtal för säkerställande av personal i händelse av avbrott.

Nyttan med kontinuitetshantering ligger även i arbetssättet som sådant. Arbetet ger fördelar i form av; [6]

- **TRYGGHET** – ett systematiskt tillvägagångssätt minskar risken för att missa viktiga detaljer
- **EFFEKTIVITET** – investeringar i säkerhet och kontinuitet optimeras i förhållande till hur viktig en process är för verksamheten i stort
- **TRANSPARENS** – ledningen tvingas fatta beslut och kommunicera organisationens riskacceptans, det vill säga viljan att ta risker
- **ANSVAR** – genom ett strukturerat arbete tydliggörs ansvaret för kritiska delar av verksamheten

Genom att arbeta systematiskt med kontinuitetshantering kan kontinuitet säkerställas i de kritiska processerna. Kontinuitetshantering skapar mervärde till organisationen genom att bidra till stärkt måluppfyllnad, detta med hjälp av ett strukturerat och effektivt arbetssätt som tydliggör ansvar samt möjliggör optimeringar avseende investeringar.

2.3 *Krav och förväntningar på kontinuitetshantering*

Kontinuitetshantering är en process som ofta drivs av organisationens egna mål, i syfte att upprätthålla den kritiska verksamheten. Viktigt att notera är samtidigt att olika externa krav ställs på att finansiella aktörer ska arbeta med kontinuitetshantering. I vissa fall är inriktningen obligatorisk, medan den i andra fall utgör rekommendationer.

I detta avsnitt noteras ett antal föreskrifter, lagkrav och allmänna råd. Det bör dock beaktas att lagar, föreskrifter och råd utvecklas och uppdateras löpande och att de som beskrivs i denna vägledning endast är ett urval. Finansiella aktörer bör därför hålla sig uppdaterade kring förändringar i olika regelverk. Viktigt att notera är även att krav på kontinuitetshantering kan vara styrda av avtal med kunder, partners, leverantörer eller myndigheter, såsom RIX-regelverk, BG-avtal, Euroclear-avtal och Nasdaq-avtal. Vidare bör beaktas att andra krav kan ställas på organisationen när den verkar inom andra länder än Sverige.

För myndigheter under regeringen ger Myndigheten för samhällsskydd och beredskap (MSB) allmänna råd om att identifiera och hantera behovet av kontinuitet för behandling av information, samt öva förmåga att upprätthålla identifierat behov av kontinuitet för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet.[7]

---

[6] *Krisberedskapsmyndigheten - Kontinuitetsplanering – en introduktion.*

[7] *MSB - Föreskrifter om informationssäkerhet för statliga myndigheter.*

Därutöver har MSB i samverkan med andra aktörer tagit fram ett behovsanpassat stöd i form av en digital verktygslåda för att underlätta arbetet med kontinuitetshantering både hos offentliga och privata aktörer. [8]

Förordningen (2022:524) om statliga myndigheters beredskap, även kallad Beredskapsförordningen, ersatte förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, även kallad Krisberedskapsförordningen. Förordningen innehåller bestämmelser om vilka uppgifter som statliga myndigheter under regeringen har inför, samt vid fredstida krissituationer och höjd beredskap.[9]

För så kallade Financial Market Infrastructures (FMI), som faciliterar clearing, avveckling och registrering av ekonomiska och andra finansiella transaktioner, har CPSS/IOSCO[10] fastställt principer som bland annat ställer krav på kontinuitetsplaner. Planerna ska behandla händelser som utgör en betydande risk för större avbrott och ska även omfatta användning av en sekundär site samt att kritiska it-system kan återuppta verksamheten inom två timmar efter avbrott. Planen bör utformas så att organisationen kan fullfölja avvecklingen vid slutet av dagen, även vid extrema omständigheter.[11]

Under 2013 antog Europaparlamentet och rådet ett nytt direktiv[12] och en förordning[13] som syftar till att införa Basel 3 i bindande rättsakter inom EU gällande kapitaltäckningsregler. Rättsakterna bygger på de tre pelarna; grundläggande kapitalkrav, tillsyn samt riskbedömning och informationskrav. EU-regleringen omfattar alla banker, kreditmarknadsföretag och värdepappersföretag i EU:s medlemsstater. I betänkandet SOU 2013:65 föreslås lagändringar för anpassning av gällande svensk rätt till den nya EU-regleringen.

I betänkandets bilaga 2 återfinns direktivet (som nämns ovan) där det under kapitlet om granskningsprocesser och tekniska kriterier för organisation och riskhantering står att *"de behöriga myndigheterna ska se till att det finns beredskaps- och affärskontinuitetsplaner för att säkerställa ett kreditinstituts förmåga att fortlöpande bedriva sin verksamhet och begränsa förlusterna vid en allvarlig störning i verksamheten"*[14].

Krav på kontinuitetshantering hos kredit- och värdepappersinstitut återfinns även i EBA:s (European Banking Authority) riktlinjer gällande intern styrning och kontroll (GL11). Där ställs bland annat krav på att instituten ska upprätta kontinuitetshantering, inklusive framtagande av kontinuitetsplaner, för att säkerställa sin förmåga att upprätthålla verksamheten och begränsa förluster vid allvarliga störningar. [15]

---

[8] *MBS - Verktygslåda för kontinuitetshantering. https://www.msb.se/kontinuitetshantering*

[9] *Förordning om statliga myndigheters beredskap.*

[10] *CPSS (The Committee on Payment and Settlement Systems) är en kommitté inom Bank for International Settlement (BIS), IOSCO (International Organization of Securities Commissions) är en organisation för tillsynsmyndigheter.*

[11] *CPSS/IOSCO. Principles for financial market infrastructures, Principle 17.*

[12] *Direktiv 2013:36/EU (ofta benämnt CRD 4).*

[13] *Förordning (EU) nr 575/2013 (ofta benämnt CRR).*

[14] *SOU 2013:65, Bilaga 2 - Europaparlamentet och rådets direktiv 2013/36/EU, Avdelning VII - Tillsyn, Kapitel 2 - Granskningsprocesser, Avsnitt II - Styrformer, processer och rutiner i institut, Underavsnitt 2 - Tekniska kriterier för organisation och riskhantering, Artikel 85 - Operativ Risk.*

[15] *EBA - Guidelines on Internal Governance (GL 11).*

Baserat bland annat på Basel 3 och GL 11, har Finansinspektionen tagit fram föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4) och om styrning, riskhantering och kontroll (FFFS 2014:1) i kreditinstitut. Dessa föreskrifter berör ett flertal aktörer i den finansiella sektorn.[16] I föreskrifterna noteras att berörda aktörer ska ha *"en väl fungerande kontinuitetshantering för att säkerställa att dess viktigaste information och funktioner bevaras samt att dess verksamhet upprätthålls vid ett avbrott eller en större verksamhetsstörning"*.[17] Det arbetssätt som beskrivs i denna vägledning ligger i linje med de krav i FFFS 2014:4 som berör kontinuitetshantering.

För försäkrings- och återförsäkringsorganisationer ställer Solvens II[18] krav på att bolaget vidtar rimliga åtgärder för att säkerställa kontinuitet i verksamheten. Detta innebär som minst att organisationen upprättar system, resurser och rutiner för kontinuitetshantering, samt att kontinuitetsplaner utvecklas.[19]

Som framgår vid en närmare studie av aktuella texter är kraven och råden sällan särskilt specifika, utan formulerade på en övergripande nivå. Detta innebär att varje organisation ofta utformar detaljerna i sitt kontinuitetshanteringsarbete själva. Då lagkrav och råd företrädelsevis fokuserar på vad som ska göras lämnas ansvaret för hur kontinuitetshanteringen ska genomföras i hög grad till respektive aktör.

Den 1 januari 2023 trädde lagen (2022:1568) om Sveriges riksbank (riksbankslagen) i kraft. Riksbankslagen ger Riksbanken rätt att genom föreskrifter peka ut vilka företag som bedriver verksamhet som är av särskild betydelse för betalningar samt fastställa företagens skyldigheter avseende arbete med planering och förberedelser samt utbildnings- och övningsverksamhet. Riksbankens föreskrifter och allmänna råd (RBFS 2023:3) om företag av särskild betydelse för genomförandet av betalningar under fredstida krissituationer och vid höjd beredskap trädde i kraft den 1 februari 2024. Föreskrifterna riktar sig till sådana företag som Riksbanken har bedömt bedriver verksamhet som är av särskild betydelse för genomförandet av betalningar. Dessa företag ska planera och förbereda för att kunna upprätthålla sin betalningsverksamhet under fredstida krissituationer och vid höjd beredskap samt bedriva intern utbildnings- och övningsverksamhet. Företagen ska även delta i det gemensamma arbete med planering och förberedelser som Riksbanken leder samt delta i de gemensamma utbildningar och övningar som Riksbanken genomför. Företagen ska därutöver planera och förbereda för att kunna ingå i den ledningsfunktion för samordning och information som Riksbanken leder under fredstida krissituationer och vid höjd beredskap.

Förordningen om digital operativ motståndskraft för den finansiella sektorn, den så kallade DORA-förordningen, trädde i kraft i början av 2023. Den syftar till att säkerhet i nätverk och informationssystem som stöttar i att affärsprocesser inom finansiell sektor upprätthålls.[20] Aktörer

---

[16] *FFFS 2014:1 gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, och kreditmarknadsföreningar. Även värdepappersrörelsen i dessa företag berörs av föreskrifterna.*
FSSS 2014:4 gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, kreditmarknadsföreningar och värdepappersbolag.

[17] *Finansinspektionen - Föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut, 2 kap 8 §, s. 4. (FFS 2014:1)*

[18] *Solvens II är ett direktiv från Europeiska kommissionen, med syfte att skapa en bättre konkurrens mellan försäkringsbolagen, genom att reglerna blir lika för alla aktörer, dels ett förstärkt konsumentskydd för försäkringstagarna.*

[19] *European Commission - Solvency II (2009/138/EC).*

[20] *REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.*

verksamma inom finanssektorn, men även kritiska tredjepartsleverantörer och molntjänstleverantörer, berörs. DORA innebär högre krav på bland annat hur organisationer detekterar, skyddar mot och förebygger angrepp, att det finns kontinuitetsplaner på plats och att det finns tillgång till backuper och metoder för att återställa information. Kraven på testning av digital motståndskraft ökar också. Bolag som berörs har fram till början av 2025 på sig att uppfylla kraven. EU:s finansiella tillsynsmyndigheter (ESA) får befogenhet att begära information, utföra inspektioner samt utfärda rekommendationer, administrativa sanktioner och avhjälpande åtgärder för identifierade kritiska tredjeparter. Lokala tillsynsmyndigheter kommer att utöva tillsyn över de finansiella företag som omfattas av reglerna i respektive medlemsstat. Den nya regleringen kommer innebära en närmare samverkan inom Europa och mellan leverantörer, vilket stärker en gemensam europeisk säkerhet på marknaden.[21]

2.4 Koppling till andra discipliner

En vanlig frågeställning kring kontinuitetshantering är hur området förhåller sig till angränsande discipliner. Svårigheten att separera de olika disciplinerna beror på att de ofta är överlappande och på en övergripande nivå syftar till att förebygga och hantera oönskade händelser som äventyrar organisationens måluppfyllnad. I efterföljande avsnitt ges en beskrivning över kopplingen mot andra discipliner så som risk, incident, - och krishantering. Kopplingar görs även mot disciplinerna informationssäkerhet, totalförsvar och organisatorisk resiliens.

I FSPOS Vägledning för krishantering presenteras disciplinernas koppling mot krishantering.

En fråga som ofta förekommer i detta sammanhang är huruvida särskilda processer behövs för de olika disciplinerna, eller om kontinuitetshanteringen inbegriper samtliga. Ett kortfattat svar på dessa frågor är att områdena delvis har olika fokus och angreppssätt, vilket kräver olika metoder och kompetenser. I mindre organisationer kan ansvar ligga hos samma person, medan hos de större organisationerna är ansvaret delegerat till olika personer i skilda delar av organisationen. Utgångspunkten bör dock vara att kontinuitetshantering betraktas som en egen disciplin men med flertalet gränsytor till andra discipliner. Arbetet med kontinuitetshantering bör därför alltid integreras för att inte utföras i stuprör.

2.4.1 Kontinuitetshantering och incidenthantering

En incident definieras av ISO 22301 som en händelse som kan vara eller skulle kunna leda till avbrott, förlust, nödläge eller kris[22]. Med andra ord menas med incidenter händelser som ännu inte utmynnat i allvarliga avbrott eller kriser. En organisation hanterar typiskt sett ett stort antal incidenter i förhållande till kriser. Incidenter kan vara mindre avbrott eller händelser som hanteras i det ordinarie arbetet och som inte kräver stöd av krisledning eller kontinuitetsplaner.

I detta sammanhang kan nämnas att it normalt hanterar många incidenter i den dagliga verksamheten för att återställa tjänster till normalläge. It-standarden ITIL[23] definierar en incident

---

of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC).
No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[21] *MSB - Policyöversikt: Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete.*

[22] *SS-EN ISO 22301 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering – Krav.*

[23] *Information Technology Infrastructure Library (ITIL).*

som *"ett oplanerat avbrott i en it-tjänst eller sänkt kvalitet på en it-tjänst. Konfigurationsfel som ännu inte har påverkat tjänsten är också en incident, till exempel fel vid spegling av en disk."*

En liknande definition ges i en annan it-standard, ISO 20000[24], där incidenter beskrivs som *"en händelse som inte är en del av den normala driften av en tjänst och som orsakar eller kan orsaka avbrott eller en minskning av kvaliteten på tjänsten"*.

De händelser som fångas upp av incidenthanteringen behöver inte nödvändigtvis hanteras inom ramen för organisationens kris- och kontinuitetshantering. Med en effektiv incidenthantering kan organisationen undvika att händelser utvecklas till kriser och/eller större avbrott i verksamheten. För att säkerställa att bolagets incidenter kan hanteras på ett effektivt sätt upprättas tydliga rutiner för larm och eskalering, samt en enhetlig analysmetodik. Vid analys av incidenter bedöms sedan om krisledning eller kontinuitetsplaner bör aktiveras.

2.4.2 Kontinuitetshantering och riskhantering

Riskhantering handlar om att hantera osäkerheter genom att systematiskt identifiera, analysera, utvärdera och behandla[25] de risker som påverkar organisationens mål. Riskhantering utgör en central del i den strategiska styrningen av organisationen. Riskhanteringen fokuserar på ett bredare urval av risker än kontinuitetshantering.

En vanlig utgångspunkt i riskhantering är att först identifiera potentiella händelser/hot och därefter analysera deras sannolikhet och konsekvens, för att slutligen planera för åtgärder/behandlingar för att minska sannolikhet för eller konsekvens av risken.

Kontinuitetshantering utgår i stället från kännedom om den kritiska verksamheten, dess beroenden och konsekvenserna av avbrott. Inom kontinuitetshantering analyseras risker mer på en operativ nivå, då kontinuitetshantering i större utsträckning fokuserar på avbrott i kritiska processer, aktiviteter och resurser. Risker och sårbarheter som identifieras inom kontinuitetshantering är endast sådana som har en direkt koppling till organisationens kritiska aktiviteter och där riskerna kan leda till oacceptabla avbrott.

Risk- och kontinuitetshanteringen har en nära koppling och de två områdena bör koordineras noga. Organisationens riskacceptans, den risknivå som en organisation är villig att acceptera, fastställs övergripande på en strategisk nivå och denna bör vara konsekvent mellan risk- och kontinuitetshanteringsarbetet.

Identifiering, analys och behandling av risker inom ramen för kontinuitetshanteringen bör även komplettera den mer övergripande riskhanteringen och vice versa.

2.4.3 Kontinuitetshantering och krishantering

Krishantering är den process som säkerställer att organisationen har en fastställd organisation (krisledning) samt fastställda rutiner för hantering av en krishändelse. Kriser är ofta händelser som inte kunnat hanteras av incidenthantering eller av organisationens kontinuitetsplaner, utan eskaleras till krisledningen.

Inom krisledningen finns därför särskild kompetens och tillräckliga mandat för att hantera krishändelser på en övergripande strategisk nivå.

---

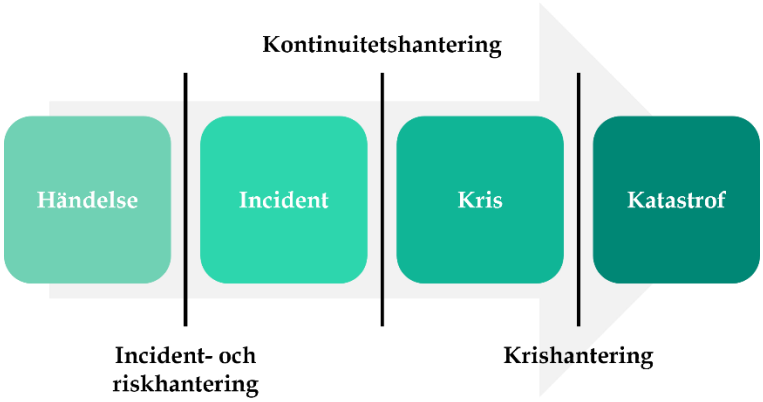
[24] *ISO 20000 – International IT Service Management Standard.*

[25] *SS-ISO 31000 Riskhantering – Vägledning.*

En kris är en händelse som är mer allvarlig än en incident och som hotar att skada, eller har skadat organisationen, eller relevanta intressenter, exempelvis kunder eller allmänheten. Kriser kan, men behöver inte nödvändigtvis innebära, att den kritiska verksamheten är avbruten och avviker från vad som anses vara en tolerabel nivå. En kris kan således vara ett avbrott i verksamheten men det kan även vara händelser som inte direkt medför avbrott i verksamheten, såsom exempelvis en förtroendekris. Krishanteringen har en nära koppling till kontinuitetshanteringen genom att krisledningen i varje kris bör beakta hur den kritiska verksamheten påverkas och om kontinuitetsplaner har aktiverats eller behöver aktiveras.

2.4.4 Incident-, risk-, kris- och kontinuitetshantering

Organisationer bör arbeta med såväl incident-, risk, och- krishantering, som kontinuitetshantering i förebyggande syfte, det vill säga med avsikt att undvika oönskade händelser. Områdena skiljer sig dock åt avseende vid vilken typ av situationer som planer och rutiner aktiveras, se nedanstående illustration.



De olika områdena kan också förklaras i termer av vilken typ av oönskade händelser de fokuserar på att hantera, i termer av sannolikhet och påverkan. Riskhantering handlar om att identifiera risker och arbetet med att hantera dessa. Kontinuitetshantering är ett kompletterande arbetssätt som ska hantera även den typ av händelser som inte kan förutses av olika anledningar, men som kan få stora konsekvenser för organisationen. Detta sker genom att, som ovan beskrivits, identifiera de kritiska delarna av verksamheten och därefter arbeta för att skapa robusthet i dessa delar. Riskhantering och kontinuitetshantering är komplement till varandra och organisationen behöver arbeta med båda.

Incidenthantering tjänar som en första barriär innan kontinuitetsplaner eller krisledningsorganisationen behöver aktiveras. Incidenthanteringen ger även ingångsvärden till organisationens riskhantering, genom att inträffade händelser ger stöd vid riskanalyser.

Krishanteringen utgör ett komplement till övriga områden genom att en särskild organisation, med särskilda kompetenser, mandat och rutiner, behöver sättas in då inte incident-, risk- och kontinuitetshantering är tillräckligt stöd för att hantera situationen.

2.4.5 Kontinuitetshantering och informationssäkerhet

Informationssäkerhet handlar om att skydda en organisations data och information från obehörig åtkomst, manipulation och förlust. En god struktur för informationssäkerhet är viktigt eftersom

brister i denna kan leda till allvarliga konsekvenser, exempelvis dataintrång, förlust av känslig information, ekonomiska förluster, juridiska konsekvenser och skada på organisationens rykte.

Kontinuitetshantering är en viktig del av informationssäkerhet, och informationssäkerhetskrav kopplat till kontinuitet finns i standardserien *ISO 27000*[26] som är etablerad i Sverige och internationellt. Standarden ställer krav på säkerhetsåtgärder för planering, upprätthållande och testning av informationssäkerhet under en störning, samt planering, upprätthållande och testning av IKT-kontinuitet (informations- och kommunikationsteknik) baserat på mål och krav inom kontinuitet.[27]

Enligt MSB[28] är kontinuitetshantering en viktig del av informationssäkerheten, då informationshantering har en avgörande roll i de flesta verksamhetsprocesser. Att ha en tydlig kartläggning av hårdvara och it-resurser kopplat till informationshantering underlättar arbetet att övergå till alternativa arbetssätt under ett avbrott.

Utifrån ett riskhanteringsperspektiv är det helt avgörande att knyta ihop risker från informationssäkerhetsarbetet med kontinuitetshantering för att erhålla en effektiv och adekvat hantering av säkerhetsrisker. Att kontinuerligt återkoppla från informationssäkerhetsarbetet till konsekvensanalys och riskbedömning gör det möjligt för organisationer att upprätthålla en adaptiv och målinriktad kontinuitetsstrategi för att möta nya och föränderliga hotlandskap.

Baserat på dessa faktorer är det av yttersta vikt att upprätthålla en kontinuerlig dialog med ansvariga funktioner för informationssäkerhet för att säkerställa att kontinuitetsplaner integreras tydligt med informationssäkerhetsstrategin. Genom denna dialog kan potentiella hot och sårbarheter som kan påverka både kontinuitets- och informationssäkerhet identifieras och adresseras, vilket stärker organisationens förmåga att effektivt hantera störningar samt skydda kritiska processer och informationstillgångar.

2.4.6 Kontinuitetshantering och totalförsvar

Sverige behöver ha en beredskap för att kunna hantera olika typer av hot mot vår säkerhet. Det gäller förberedelse för att hantera fredstida kriser, som till exempel pandemier eller naturkatastrofer, säkerhetspolitiska kriser och ytterst ett väpnat angrepp.

Då kontinuitetshantering handlar om att säkerställa att organisationen kan driva sin kritiska verksamhet på tolerabel nivå under fredstid har totalförsvar ett bredare perspektiv och omfattar både civila och militära åtgärder för att skydda landet mot yttre hot. Civil beredskap är ett samlingsnamn för krisberedskap och civilt försvar, det vill säga planering för fredstida krissituationer såväl som höjd beredskap och krig.

---

[26] *ISO 27000-serien innefattar ett flertal standarder för informationssäkerhet, cybersäkerhet och integritetsskydd, bland annat. ISO 27001 – Informationssäkerhet - Cybersäkerhet och integritetsskydd - Ledningssystem för informationssäkerhet – Krav. ISO 27002 - Informationssäkerhet – Cybersäkerhet och integritetsskydd – Informationssäkerhetsåtgärder.*

[27] *Dessa krav återfinns i säkerhetsåtgärderna 5.29 Informationssäkerhet vid störning, samt 5.30 Kontinuitetsberedskap inom IKT.*

[28] *MSB - Vägledning för processorienterad informationskartläggning.*

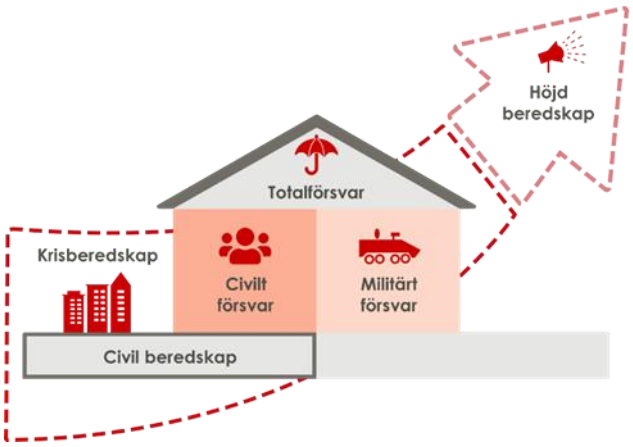


Illustration av hur krisberedskap, civilt försvar, och totalförsvar hänger ihop (MSB).

Civila organisationer som omfattas av totalförsvaret ska inneha en god förmåga att kunna upprätthålla verksamhet av betydelse för totalförsvaret i händelse av krig eller krigsfara. Detta görs genom arbete med civil beredskap, där kontinuitetshantering är en central utgångspunkt. De viktiga samhällsfunktionerna inom finansiell sektor innefattar: Betalningsförmedling, Försäkring, Sparande, finansiering, finansiell riskhantering och Finansiell stabilitet.

En stor del av alla samhällsviktiga verksamheter bedrivs av privata aktörer. Samhällsviktig verksamhet av betydelse för totalförsvaret behöver kunna fortsätta bedrivas även under krigsfara och krig. En väl fungerande privatoffentlig samverkan är därför en viktig förutsättning för den civila beredskapen.

Totalförsvaret ska vara krigsavskräckande, det vill säga minska risken för angrepp och påtryckningar mot Sverige och därmed värna vår säkerhet, frihet, självständighet och handlingsfrihet. Målet för totalförsvaret i händelse av ett väpnat angrepp är att ha förmågan att försvara Sverige och upprätthålla verksamhet av betydelse för totalförsvaret. I krig eller krigsfara kan regeringen besluta om höjd beredskap. Under högsta beredskap är totalförsvar all samhällsverksamhet som då skall bedrivas (lagen om totalförsvar och höjdberedskap 1§). Vid höjd beredskap ska samhällsviktig verksamhet av betydelse för totalförsvaret[29] anpassa sin organisation till de särskilda krav som råder. [30]

I arbetet med totalförsvarsplanering kan en organisation använda sig av befintligt beredskapsarbete som utgångspunkt, t.ex. kontinuitetshantering. Genom att komplettera arbetet med kontinuitetshantering med t.ex. förändrade avbrottstider, uthållighetsaspekter i kontinuitetslösningar och scenarios av höjd beredskap kan perspektivet i kontinuitethanteringen breddas till att inkludera även krig eller krigsfara.

Svenska Institutet för Standarder har tagit fram en handbok för kontinuitetshantering.[31] I denna återfinns ett särskilt kapitel som beskriver tilläggsrekommendationer avseende hur en organisation kan inkludera perspektivet höjd beredskap i en process för kontinuitetshantering.

---

[29] *MSB/FM - Handlingskraft och i Riksbankens föreskrifter.*

[30] *FSPOS - PM: Aktuella planeringsförutsättningar för finansiella sektorns arbete med civilt försvar.*

[31] *SS 22304–2023 – Säkerhet och resiliens- Ledningssystem för kontinuitetshantering - Handbok för kontinuitetshantering.*

2.4.7 Kontinuitetshantering och organisatorisk resiliens

Med begreppet organisatorisk resiliens menas i denna vägledning det engelska begreppet ”Operational Resilience”. Det finns för närvarande ingen entydig översättning av begreppet.

Vägledningen har gjort valet att använda begreppet organisatorisk resiliens utifrån ISO Standarden – 22316 - Säkerhet och resiliens - Organisatorisk resiliens – Principer[32] samt utifrån FSPOS framtagna promemoria Organisatorisk resiliens - En överblick.[33]

Begreppet syftar på förmågan att stå emot och hantera förändringar samt att återhämta sig och utvecklas.[34] Inom beredskapsperspektivet är det nära relaterat till risk-, kontinuitets- och krishantering.

Organisatorisk resiliens kan sammanfattas som resultatet av integrerat, systematiskt och strukturerat arbete inom flera discipliner för att skapa en robust organisation. Detta inkluderar intern styrning och kontroll, där ägandeskapet för resiliens ligger på styrelse- och ledningsnivå.

Bolagsstyrning utgör en viktig komponent i beredskapsarbetet, där tydliga roller och ansvar samt samordning är avgörande för organisatorisk resiliens. Utmaningen ligger i att uppnå ett integrerat arbetssätt och undvika silostrukturer.

Befintlig ISO-standard om organisatorisk resiliens sammanfattar ovan väl:

> *Det finns inte ett enskilt tillvägagångssätt för att stärka en organisations resiliens. Det finns etablerade ledningsdiscipliner som gemensamt bidrar till resiliens, men var och en för sig räcker de inte för att garantera en organisations resiliens. Organisatorisk resiliens är resultatet av ett samspel mellan egenskaper och aktiviteter, och av bidrag från annan teknisk och vetenskaplig expertis.*[35]

För vidare läsning, se FSPOS Promemoria *Organisatorisk resiliens - En överblick.*[36]

---

[32] *SS-ISO 22316:2020 - Säkerhet och resiliens - Organisatorisk resiliens – Principer.*

[33] *FSPOS - Organisatorisk resiliens - En överblick.*

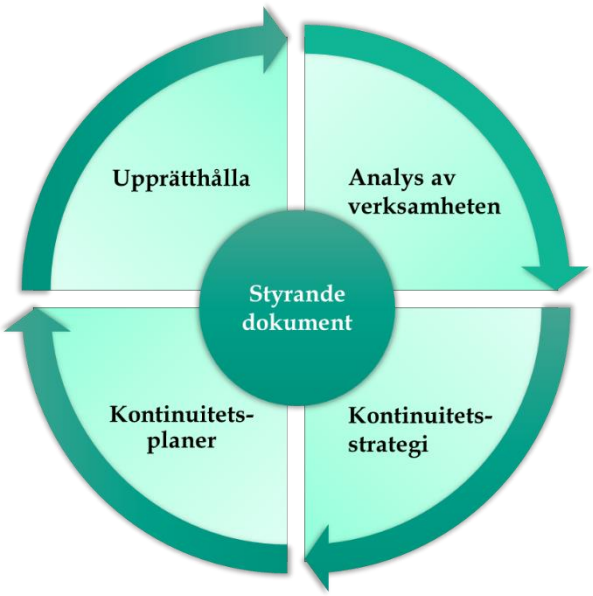
[34] *MSB - Resiliens: begreppets olika betydelser och användningsområden - Publikationsnummer MSB569.*

[35] *SS-ISO 22316:2020 - Säkerhet och resiliens - Organisatorisk resiliens – Principer.*

[36] *FSPOS - Organisatorisk resiliens - En överblick.*

3 Process för kontinuitetshantering

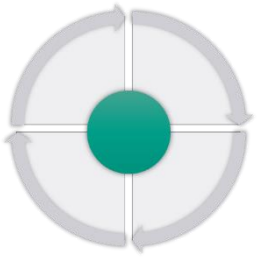
Kontinuitetshanteringsarbetet behöver löpande utvecklas. För att säkerställa detta bör arbetet bedrivas som ett program för kontinuitetshantering. Med program för kontinuitetshantering menas den löpande process med ledning och styrning som stöds av den högsta ledningen och tilldelas tillräckliga resurser för att implementera kontinuitetshantering och upprätthålla kontinuitet i verksamheten.



Processen för kontinuitetshantering.

Programmet för kontinuitetshantering bör drivas som en förbättringscykel, där respektive steg förbättras kontinuerligt. Förbättringsarbetet bör även löpande utvärdera risker mot programmet som sådant och utvärdera hur målen för programmet uppfylls. Hur lång cykel som en organisation väljer kan dels bero på ambition eller krav på verksamheten, men vanligast är att cykeln löper över ett år. Värt att notera är samtidigt att externa krav, exempelvis lagkrav eller avtal, ofta kräver att uppdatering av planer utvärderas och revideras årligen. Processen för kontinuitetshantering kan beskrivas enligt illustrationen ovan. Nedan presenteras också, kortfattat, vad respektive steg innebär. I Appendix A-E beskrivs varje steg mer djupgående.

3.1 *Styrande dokument*



En nyckel till ett framgångsrikt arbete med kontinuitetshantering är att säkerställa en tydlig inriktning och avgränsning för det samlade kontinuitetsarbetet. I de styrande dokumenten definieras inriktningen utifrån syfte och mål med kontinuitetsarbetet, medan avgränsningen görs genom att ange de kritiska processer som innefattas i kontinuitetsarbetet. Organisation, roller och ansvar samt metod för kontinuitetsarbetet beskrivs också i de styrande dokumenten.

I FSPOS vägledning benämns det huvudsakliga styrande dokumentet Policy. Organisationens policy för kontinuitetshantering är det övergripande styrdokumentet som på en strategisk nivå definierar inriktning, ansvar och roller samt avgränsningar för kontinuitetsarbetet. Valet av styrande dokument och nivå bör grundas på organisationens befintliga styrmodell för att säkerställa enhetlighet och effektivitet. Inom vissa områden, exempelvis hur kontinuitetsarbetet bedrivs, kan det ibland vara motiverat att ge en mer detaljerad beskrivning i ett separat styrande dokument såsom en riktlinje. Det är dock viktigt att förhållandet mellan detta dokument tydligt framgår i policyn samt att en tydlig referens till avgränsningen ges i policydokumentet.

En viktig utgångspunkt för kontinuitetsarbetet är att det finns en gemensam syn på verksamhetens riskbenägenhet, det vill säga var gränsen för acceptabla/oacceptabla konsekvenser går. En metod för att definiera oacceptabla konsekvenser för den egna organisationen är framtagande av en kriteriemodell. I en kriteriemodell beskrivs konsekvenserna av en störning utifrån olika konsekvenskategorier (exempelvis ekonomi och förtroende/varumärke) och konsekvensnivåer (obetydlig, märkbar, allvarlig). Därefter bestäms vilka konsekvenser som är acceptabla/oacceptabla. Riskacceptansen bör dokumenteras i de styrande dokumenten och användas som utgångspunkt i det vidare kontinuitetsarbetet. Om en riskmatris finns inom organisationen används den som utgångspunkt.

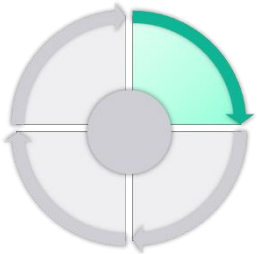
I exemplet nedan är gränsen mellan oacceptabla och acceptabla konsekvenser angiven med den röda linjen mellan nivåerna betydande och kritisk. Med detta menas att konsekvenser inom ekonomi och förtroende/varumärke accepteras upp till det som beskrivs inom nivån betydande. Konsekvenserna inom nivån kritisk accepteras inte.

	Märkbar	**Betydande**	**Kritisk**
Ekonomisk påverkan	Förlust: 1 kr – 1 mkr Kassalikviditet påverkas <15%	Förlust: 1 mkr – 20 mkr Kassalikviditet påverkas 15-40%	Förlust: > 20 mkr Kassalikviditet påverkas >40%
Påverkan på förtroende/varumärke	Ryktet relativt opåverkat Enskild negativ publicering, lokal spridning, aktualitet en dag	Ryktet kortsiktigt påverkat Ett fåtal negativa publiceringar, nationell spridning, aktualitet en dag till ett fåtal dagar	Ryktet långsiktigt påverkat Flera publiceringar med hård kritik, nationell spridning, aktualitet dagar till veckor

Kriteriemodellen är ett viktigt verktyg i att göra en så kallad strategisk konsekvensanalys, d.v.s. att prioritera organisationens produkter och tjänster och dess stödjande processer.

Prioriteringen av produkter och tjänster utgår ifrån vilka produkter och tjänster som är nödvändiga för att organisationen ska kunna uppnå sina verksamhetsmål och eventuella externa krav. Prioriteringen kan därefter göras utifrån tidskritikalitet, d.v.s. hur länge produkten eller tjänsten kan vara otillgänglig innan oacceptabla konsekvenser uppstår. Den tiden kallas maximalt tolerabel avbrottstid[37]. För de prioriterade produkterna och tjänsterna identifieras därefter stödjande processer. Även för dessa fastställs maximalt tolerabel avbrottstid som stöd för prioritering. De prioriterade produkterna och tjänsterna tillsammans med de stödjande kritiska processerna omfattas av kontinuitetsarbetet. På så sätt avgränsas kontinuitetsarbetets omfattning.

3.2 *Analys av verksamheten*

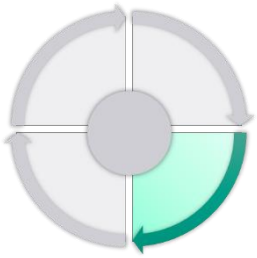


I analys av verksamheten görs en djupare analys av organisationens prioriterade processer. Som underlag för detta arbete är det bra att inventera arbete som tidigare gjorts inom organisationen, såsom processkartläggningar, informationskartläggningar eller detaljerade verksamhetsbeskrivningar.

De kritiska processerna analyseras därefter utifrån vilka effekter som störningar och avbrott har på leveransen av produkter och tjänster. Detta görs genom att analysera varje kritisk process och identifiera kritiska aktiviteter för denna. För att kunna utföra de identifierade kritiska aktiviteterna krävs i sin tur både interna och externa resurser såsom personal, it-system (informationsbärare), lokaler och leverantörer. För varje aktivitet identifieras därmed de interna och externa resurser som behövs.

Ur ett informationssäkerhetsperspektiv är det viktigt att identifiera vilka informationstillgångar som är nödvändiga för att utföra respektive kritisk aktivitet, samt vilka informationsbärande resurser som hanterar och lagrar respektive informationstillgång. Detta syftar till att få ett grepp om vilken information som processen och dess aktiviteter skapar och utnyttjar, vilket i sin tur underlättar vid utformningen av lämpliga kontinuitetsstrategier i nästa steg.

3.3 *Kontinuitetsstrategi*



Kontinuitetsstrategier utgör gemensamma principer som möjliggör för organisationen att välja lämpliga sätt att förebygga och hantera hot mot de prioriterade processerna, aktiviteterna, resurserna och informationstillgångarna. Valda kontinuitetsstrategier ska säkerställa att prioriterade aktiviteter och resurser fungerar inom de uppsatta tidskraven, samt att informationssäkerheten upprätthålls på lämplig nivå vid störning. Kontinuitetsstrategier sätts på en övergripande nivå och utgör en inriktning för vilka kontinuitetslösningar som ska implementeras.

---

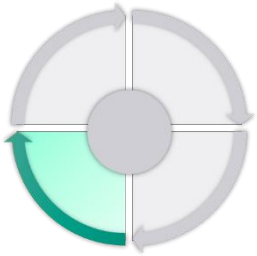
[37] *SS-EN ISO 22313 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Vägledning för implementering av ISO 22301. MTPD – Maximum Tolerable Period of disruption. MAO – Maximum Acceptable Outage (ISO 22313).*

Strategierna bör formuleras på strategisk nivå och av de som har mandat att fatta beslut kring hur personella och finansiella resurser ska fördelas. Strategierna kan ta sikte på att hantera störningar före, under och/eller efter att de inträffar. Strategier före en störning syftar till att förebygga och/eller minska sannolikheten för önskade händelser, strategier under en störning syftar till att skapa så små avbrott som möjligt i verksamheten under en störning, och strategier efter en störning syftar till att minska konsekvenserna av en störning efter att den inträffat.

Exempel på strategier kan vara diversifiering av affärskritiska delar av verksamheten, att nyttja olika typer av resurser eller att upprätta avtal med flera olika leverantörer. Olika strategier kan vara mer eller mindre lämpade beroende på omständigheter och vilken typ av process, aktivitet eller resurs de söker upprätthålla. Viktigt är att strategierna utformas så att informationssäkerheten kan upprätthållas både före, under och efter en störning.

Beslut om implementering av kontinuitetsstrategier kan medföra ökade kostnader för organisationen. Dessa kostnader måste vägas mot den nytta de förväntas innebära.

3.4 Kontinuitetsplaner



Utifrån kontinuitetsstrategin och de tidigare stegen i kontinuitetsprocessen identifieras konkreta kontinuitetslösningar som sedan beskrivs i kontinuitetsplaner. Viktigt är att de lösningar som beskrivs i dokumentet beskriver hur kontinuiteten i kritiska aktiviteter och resurser ska upprätthållas, hur resursen återställs vid störningar samt hur återgång till normalläge ska ske då resurserna är återställda.

I kontinuitetsplanen beskrivs detaljerade kontinuitetslösningar, för var och en av de kritiska resurserna, i form av checklistor för de tre delarna:

- Reservrutiner - *Hur arbetar vi på alternativa sätt under ett avbrott?*
- Återställningsrutiner - *Hur återställer vi den kritiska resursen efter ett avbrott?*
- Återgångsrutiner - *Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen?*

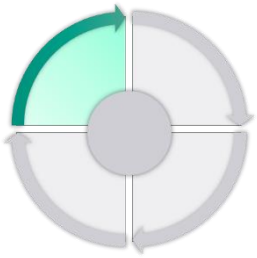
Det är viktigt att kontinuitetslösningarna är specifika och detaljerade i beskrivningarna för att planen ska kunna användas operativt under en störning. Viss flexibilitet behövs dock för att kunna svara mot oväntade hot samt förändrade interna och externa förhållanden.

I de beskrivna kontinuitetslösningarna bör även särskilda åtgärder beaktas för att bevara informationens skyddsvärden under hela avbrottet.

Det innebär att checklistorna bör utformas så att informationens konfidentialitet, riktighet och tillgänglighet upprätthålls på lämplig nivå för samtliga reservrutiner, återställningsrutiner och återgångsrutiner.

Kontinuitetsplanerna aktiveras vid behov för att kunna upprätthålla kritiska processer och möjliggöra för en snabb återgång till normal verksamhet.

3.5 *Upprätthålla*

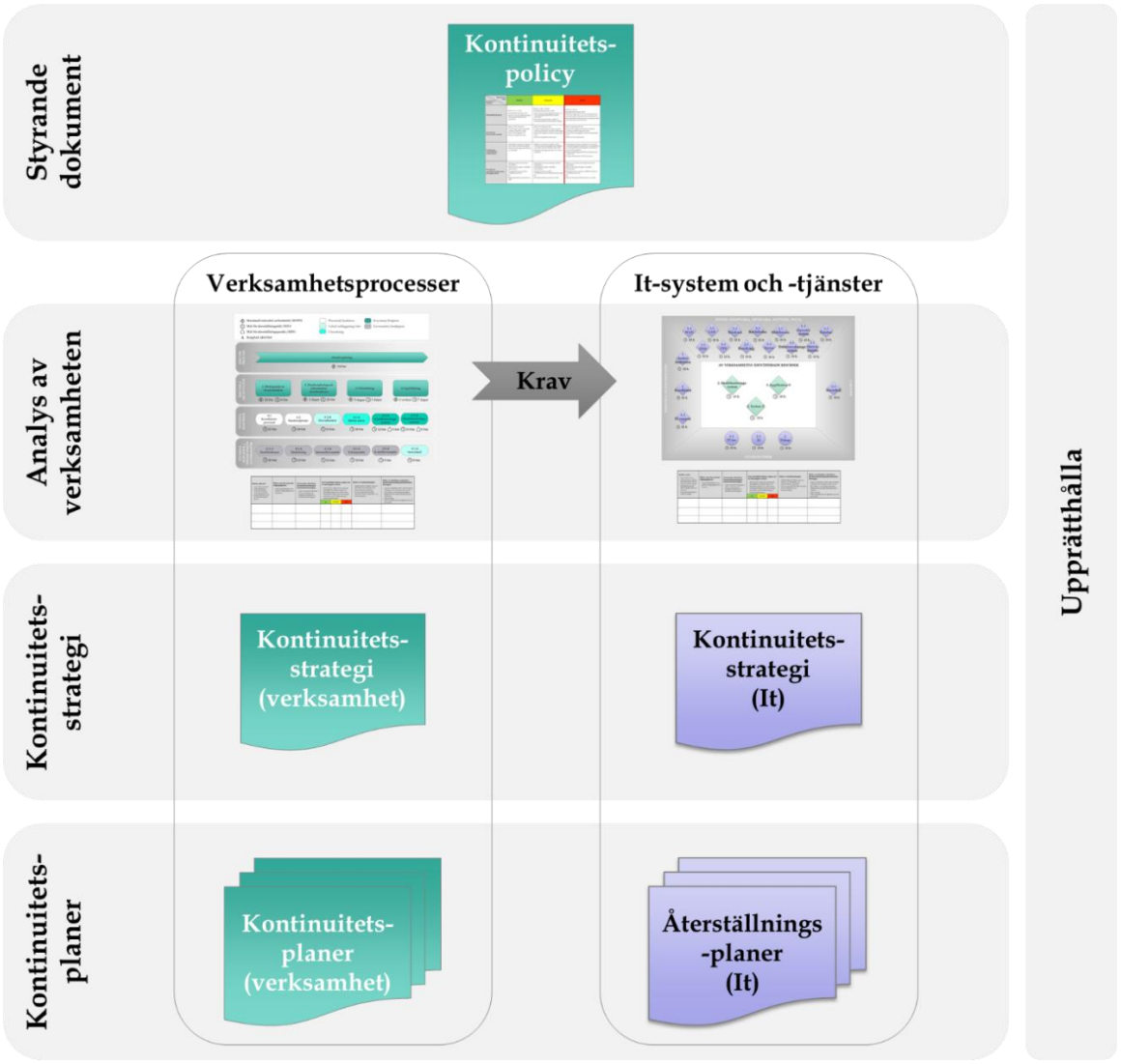


Likt med andra verksamhetsprocesser så måste arbetet med kontinuitetshantering kontinuerligt upprätthållas och förbättras. Detta kan exempelvis ske genom granskning och revidering av styrande dokument, genomförda analyser och utvecklade kontinuitetsplaner utifrån förändrade förutsättningar. Ett annat sätt att upprätthålla och förbättra kontinuitetsarbetet är genom utbildning, övning och test, detta för att öka förståelsen och förmågan i organisationen.

Omvärlden och organisationer är i ständig förändring, det är därför av vikt att regelbundet granska och revidera kontinuitetsarbetet för att säkerställa att kontinuitetsstrategier, -lösningar och -planer är tillämpliga. Revision och granskning kan genomföras både av interna och externa parter. Det är utöver granskning och revidering viktigt att regelbundet öva och testa de implementerade kontinuitetsplanerna för att säkerställa att befintliga kontinuitetslösningar är tillräckliga för att möta de tidskrav som satts upp, samt att informationssäkerheten upprätthålls på en lämplig nivå. Omfattning och frekvens av övning och test bör kopplas till hur kritisk en process eller resurs är för verksamheten. Även utbildningar är en viktig del av implementeringen av kontinuitetshantering inom organisationen. Utbildningar bör genomföras för olika nivåer inom organisationen samt med olika syften baserat på målgruppens behov och roll i arbetet.

Utbildning, övning och test är av stor betydelse för att skapa en organisationskultur som främjar kontinuitetshantering där arbetssättet är känt i organisationen, ansvaret är tydligt fördelat, ledningen har belyst vikten av därmed tilldelat tillräckliga resurser till arbetet, och där kontinuitetshantering är integrerat i alla delar av verksamheten.

I figuren nedan visas hur slutprodukterna av respektive steg hänger ihop samt kopplingen mellan verksamhetens och it-organisationens kontinuitetsarbete.



APPENDIX A - H

Vägledningens appendix innehåller fördjupande beskrivningar. Nedan beskrivs kortfattat innehåll och målgrupp för respektive appendix.

Appendix A innehåller en mer djupgående beskrivning av det första steget i kontinuitetshanteringsprocessen; **Styrande dokument**. Målgrupp för detta avsnitt är framför allt organisationens övergripande ansvariga för kontinuitetshantering. Det är dessa personer som ska besluta kring ramverk, målsättning och resursfördelning för arbetet med kontinuitetshanterings. I Appendix A finns också mallar och exempel att använda som stöd vid utveckling av styrande dokument.

Appendix B innehåller en mer djupgående beskrivning av det andra steget i kontinuitetshanteringsprocessen; **Analys av verksamheten**. Målgrupp för detta avsnitt är kontinuitetshanteringsansvariga i verksamheten, det vill säga de personer som ansvarar för att kontinuitetshanteringsarbetet genomförs i verksamheten och som har kunskap om den del av verksamheten som ska analyseras. I Appendix B finns också mallar och exempel att använda som stöd vid genomförande av analys av verksamheten.

Appendix C innehåller en mer djupgående beskrivning av det tredje steget i kontinuitetshanteringsprocessen; **Kontinuitetsstrategier**. Målgrupp för detta avsnitt är de personer i organisationen som har mandat att fatta beslut kring inriktning och strategier för det övergripande kontinuitetshanteringsarbetet. I Appendix C finns också mallar och exempel att använda som stöd vid framtagandet av kontinuitetsstrategier.

Appendix D innehåller en mer djupgående beskrivning av det fjärde steget i kontinuitetshanteringsprocessen; **Kontinuitetsplaner**. Målgrupp för detta avsnitt är kontinuitetshanteringsansvariga i verksamheten. De personer som i normalläge är ansvariga för en viss verksamhet bör också vara de som är ansvariga för att upprätta kontinuitetsplaner för dessa. I Appendix D finns också mallar och exempel att använda som stöd vid utvecklig av kontinuitetsplaner.

Appendix E innehåller en mer djupgående beskrivning av det femte steget i kontinuitetshanteringsprocessen; **Upprätthålla**. Målgrupp för avsnittet är samtliga som ska arbeta med kontinuitetshantering i verksamheten, men särskilt beslutsfattare som ansvarar för utveckling och upprätthållande av kontinuitetsarbetet.

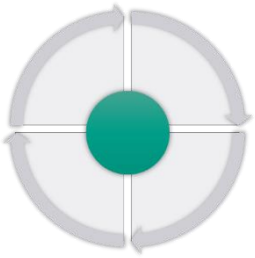
Appendix F innehåller en övergripande beskrivning av **kontinuitetshanteringsprocessen för it-verksamheten**. Målgrupp är kontinuitetshanteringsansvariga i it-verksamheten. I Appendix F finns också mallar och exempel att använda som stöd vid genomförande.

Appendix G innehåller en övergripande beskrivning av hur aktörerna kan arbeta med **kontinuitetshantering vid outsourcing**.

Appendix H ger ett stöd i hur **tester av verksamhetens kontinuitetsplaner** kan planeras, genomföras och utvärderas. Målgrupp för avsnittet är samtliga som ska arbeta med kontinuitetshantering i verksamheten, men särskilt de personer som är ansvariga för utveckling och upprätthållande av kontinuitetsarbetet, exempelvis BCM-ansvariga, processägare eller planägare.

Appendix A - Styrande dokument

För att säkerställa inriktning och avgränsningar i arbetet med kontinuitetshantering, upprättas med fördel styrande dokument. I FSPOS vägledning benämns det huvudsakliga styrande dokumentet *Policy*.



Organisationens policy för kontinuitetshantering är det övergripande styrdokumentet som på en strategisk nivå definierar inriktning, ansvar och roller samt avgränsningar för kontinuitetshanteringsarbetet. Viktigt är att organisationens syfte och mål med kontinuitetshanteringen klargörs. För att hela organisationen ska ha samma utgångspunkt är det också av vikt att tydliggöra vilka principer som gäller för kontinuitetsarbetet och att definiera centrala begrepp. Avgränsningar i arbetet med kontinuitetshantering kan definieras med hjälp av en strategisk konsekvensanalys, vilket beskrivs vidare i detta appendix.

Policyn kan också stödjas av andra styrande dokument, exempelvis instruktion, riktlinje, rutinbeskrivning. I dessa beskrivs processer, rutiner och metoder för hur kontinuitetsarbetet bedrivs inom organisationen. Valet av styrande dokument och nivå bör grundas på organisationens befintliga styrmodell för att säkerställa enhetlighet och effektivitet. Det är viktigt att välja dokument som är förenliga med befintliga styrdokument för att undvika förvirring och dubbelarbete. Det är också viktigt att förhållanden mellan dokumenten tydligt framgår samt att en tydlig referens till avgränsningen ges i policydokumentet.

De styrande dokumenten anger tydliga ingångsvärden för arbetet med kontinuitetshanteringen och dokumenten behöver ständigt hållas uppdaterade. En rutin för regelbunden uppdatering av dokumenten bör finnas fastställd. I rutinen bör ansvarig och frekvens för uppdatering anges, samt vid vilka förändringar i omgivningen som föranleder uppdatering, exempelvis vid nya/förändrade föreskrifter eller andra regelverk. Genomförda förändringar bör dokumenteras i dokumenthistoriken.

A.1. Organisationens kontext

I de styrande dokumenten beskrivs den kontext som organisationen verkar inom. Med detta menas att organisationen har en uppfattning om vilka interna och externa faktorer som påverkar dess mål och i vissa fall ställer krav på kontinuitetshantering.

Interna faktorer kan utgöras bland annat av vilka värdeskapande produkter och tjänster som organisationen levererar, hur kontinuitetshanteringsarbetet organiseras samt vilka mål, policys och rutiner verksamheten har i övrigt. Externa faktorer kan utgöras av drivkrafter och förväntningar från intressenter såsom kunder, partners, leverantörer och tredjepart. Även organisationens makro-miljö bör tillgodoses, såsom sociala, ekonomiska, tekniska, eller politiska omständigheter. Bland annat bör organisationen ha en tydlig bild över vilka externa krav som finns från regelverk eller intressenter såsom kunder eller leverantörer.[38] För att skapa en tydligare bild över dessa faktorer kan en kartläggning över organisationens intressenter och dess förväntningar göras. Intressenternas förväntningar kan se olika ut i normalläge och vid ett avbrott. Det kan därför finnas anledning att belysa förväntningarna i båda dessa lägen.

---

[38] *SS-EN ISO 22313 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Vägledning för implementering av ISO 22301.*

Vid kartläggningen kan en prioritering göras för att tydliggöra vilka intressenter som är särskilt styrande för organisationen.

A.2. Kriteriemodell

En viktig utgångspunkt för kontinuitetsarbetet är en gemensam syn på organisationens riskacceptans, det vill säga var gränsen går för vilka konsekvenser som är oacceptabla. Riskacceptansen fastställs vanligen med stöd av en så kallad kriteriemodell, vilken ger inriktning vid arbete för att fastställa kontinuitetsarbetets omfattning och för att förtydliga dess avgränsningar. Finns en riskmatris[39] används denna med fördel som utgångspunkt.

Format	• Utveckling av kriteriemodellen utförs med fördel genom en workshop. • Viktigt att kriteriemodellen beslutas av ledningen och förankras inom hela organisationen.
Deltagare	• Representanter från ledningen med kunskap om organisationen och mandat att fatta beslut.
Tidsåtgång	• En eller två halvdagar för workshop. • Tillräckligt med tid för förankring och beslut.
Slutprodukt	• En kriteriemodell som är gemensam för hela organisationen och som definierar vilka konsekvenser som är acceptabla och oacceptabla.

I kriteriemodellen definieras vilka konsekvenser som organisationen anser vara acceptabla/oacceptabla genom konsekvensbeskrivningar inom olika konsekvenskategorier (exempelvis ekonomisk påverkan och påverkan på förtroende/varumärke) och konsekvensklasser (märkbar, betydande, kritisk). Därefter beskrivs var gränsen mellan acceptabel/oacceptabelt går. I exemplet nedan är gränsen angiven med en röd linje mellan nivåerna betydande och kritisk. Med detta menas att konsekvenser inom ekonomisk påverkan och påverkan på förtroende/varumärke är acceptabla upp till och med det som beskrivs inom nivån betydande. Konsekvenserna inom nivån kritisk bedöms inte som acceptabla. Detta är ett sätt för organisationen att bedöma maximalt tolerabel avbrottstid (MTPD) för verksamheten, som då inte får överstiga den röda linjen.

	Märkbar	Betydande	Kritisk
Ekonomisk påverkan	Förlust: 1 kr – 1 mkr Kassalikviditet påverkas <15%	Förlust: 1 mkr – 20 mkr Kassalikviditet påverkas 15-40%	Förlust: > 20 mkr Kassalikviditet påverkas >40%
Påverkan på förtroende/varumärke	Ryktet relativt opåverkat Enskild negativ publicering, lokal spridning, aktualitet en dag	Ryktet kortsiktigt påverkat Ett fåtal negativa publiceringar, nationell spridning, aktualitet en dag till ett fåtal dagar	Ryktet långsiktigt påverkat Flera publiceringar med hård kritik, nationell spridning, aktualitet dagar till veckor

Den röda linjen i bilden illustrerar gränsen mellan acceptabla/oacceptabla konsekvenser.

[39] *Matris för analys av risker med "Sannolikhet" och "Konsekvens" på Y- respektive X-axlarna.*

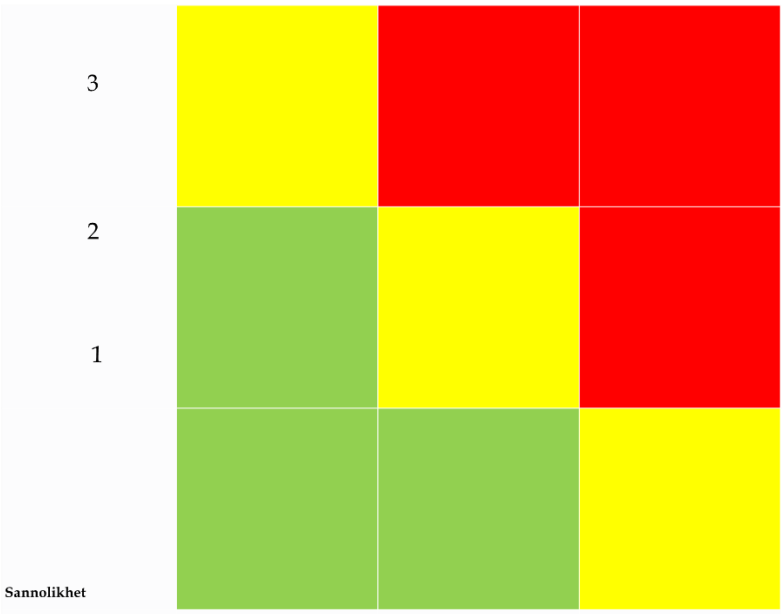
I exemplet används tre konsekvensnivåer. Kriteriemodellen skulle även kunna ange ett större annat antal nivåer om det skulle anses lämpligt att segmentera analysen ytterligare, exempelvis genom att använda nivåerna *obetydlig*, *märkbar*, *allvarlig, kritisk* och *katastrofal*. Om en riskmatris redan finns i organisationen för att analysera sannolikhet och konsekvens för identifierade risker, bör denna användas som utgångspunkt. Antalet konsekvensnivåer i kriteriemodellen bör därmed överensstämma med angivna nivåer i riskmatrisen. Det är även viktigt att definitionerna av respektive konsekvensnivå är mätbara, detta för att minimera möjligheten att göra egna tolkningar.

På ett liknande sätt kan fler konsekvenskategorier än påverkan på ekonomi och rykte/varumärke läggas till i kriteriemodellen baserat på vilka områden organisationen anser lämpliga, exempelvis *påverkan på verksamhetens funktionalitet*, *påverkan på samhällets skyddsvärden* eller *påverkan på regelefterlevnad.* Vidare kan olika konsekvenskategorier vara relevanta endast för specifika delar av verksamheten. Därför kan olika kategorier läggas till/tas bort för specifika verksamhetsdelar. Det är viktigt att de olika konsekvensnivåerna samt beslut om vilka konsekvenser som är oacceptabla beslutas på en strategisk nivå och utifrån verksamhetens målsättning/krav samt intressenter/legala krav.

Kriteriemodellen signalerar till verksamheten vilka typer av konsekvenser som är oönskade och vilka som inte accepteras av organisationen på en övergripande nivå. Modellen utgör en gemensam måttstock och söker därigenom säkerställa att analyser och bedömningar görs utifrån samma övergripande bild om vad organisationen eftersträvar motverka med kontinuitetshantering. Med ett enhetligt angreppssätt kan organisationen undvika att olika verksamheter gör subjektiva bedömningar och analyser baserat på olika kriterier. Kriteriemodellen är ett nödvändigt stöd för analys av verksamheten, där den används för att bestämma hur långa verksamhetsavbrott som är acceptabla.

Tips för genomförande:
- Vid val av konsekvenskategorier, utgå ifrån vad som är viktigt för den aktuella organisationen
- Vid beskrivning av konsekvenserna för respektive nivå, börja med beskrivning av konsekvenserna på den mest kritiska nivån
- Tänk på att samtliga beskrivningar ska vara mätbara
- Efter att kriteriemodellen är ifylld, "kalibrera" respektive kolumn

Som nämndes ovan bör en eventuell riskmatris användas som utgångspunkt för kriteriemodellen. Kriteriemodellen utgör då ett komplement och en konkretisering av riskmatrisen genom att definiera vad konsekvenser på de olika nivåerna enligt riskmatrisen innebär. Se exempel på nästkommande sida.



Riskmatris
Används för att analysera risker utifrån sannolikhet och konsekvens

Konsekvensnivå / Konsekvens-kategori	Märkbar	Betydande	Kritisk
Ekonomisk påverkan	• *Förlust: 1 kr – 1 mkr* • *Kassalikviditet påverkas <15%* • *Smärre justering i gällande budget, alla planerade aktiviteter kan genomföras*	• *Förlust: 1 mkr – 20 mkr* • *Kassalikviditet påverkas 15-40%* • *Större omprioritering i gällande budget, ett större antal planerade aktiviteter kan ej genomföras* • *Årsredovisningen påverkas, utfallet av årsvinsten kommer att bli mindre än väntat*	• *Förlust: > 20 mkr* • *Kassalikviditet påverkas >40%* • *Gällande budget räcker inte till, stöd utifrån krävs för att genomföra planerade prioriterade aktiviteter* • *Det finansiella resultatet kommer att påverkas starkt, årsvinsten kommer att försvinna*
Påverkan på förtroende/varumärke	• *Ryktet relativt opåverkat* • *Enskild negativ publicering, lokal spridning, aktualitet en dag* • *Större antal klagomål (>5)* • *Förlust av låg andel kunder*	• *Ryktet kortsiktigt påverkat* • *Ett fåtal negativa publiceringar, nationell spridning, aktualitet en dag till ett fåtal dagar* • *Fåtal krav på åtgärder och/eller kompensation (<5)* • *Förlust av betydande andel kunder*	• *Ryktet långsiktigt påverkat* • *Flera publiceringar med hård kritik, nationell spridning, aktualitet dagar till veckor* • *Stort antal krav på åtgärder och/eller kompensation (>5)* • *Förlust av stor andel kunder*
Påverkan på verksamhetens funktionalitet	• *Obetydlig minskning i förmågan att lösa kritiska verksamhetsuppgifter* • *Produktionsförmågan påverkad med kan bibehållas*	• *Märkbar minskning i förmågan att lösa kritiska verksamhetsuppgifter (kan fullföljas, men effektiviteten är påvisbart reducerad)* • *Produktionsförmågan påverkas och minskas temporärt*	• *Allvarlig begränsning i förmågan att lösa kritiska verksamhetsuppgifter (omfattning och varaktighet så att verksamheten inte kan fullgöra en eller flera av sina primära uppgifter)* • *Produktionsförmågan påverkas och minskas under en längre tid* • *Indraget tillstånd från Finansinspektionen*
Påverkan på samhällets skyddsvärden	• *Måttliga direkta eller indirekta hälsoeffekter* • *Begränsade störningar i samhällets funktionalitet* • *Övergående misstro mot flera samhällsinstitutioner* *eller* • *Begränsade skador på egendom och miljö*	• *Betydande direkta eller måttliga indirekta hälsoeffekter,* • *Allvarliga störningar i samhällets funktionalitet,* • *Bestående misstro mot flera samhällsinstitutioner eller förändrat beteende,* *eller* • *allvarliga skador på egendom och miljö*	• *Mycket stora direkta eller betydande indirekta hälsoeffekter* • *Mycket allvarliga störningar i samhällets funktionalitet* • *Bestående misstro mot flera samhällsinstitutioner och förändrat beteende* *eller* • *Mycket allvarliga skador på egendom och miljö*

Kriteriemodell
Används för att definiera konsekvenser på olika nivåer

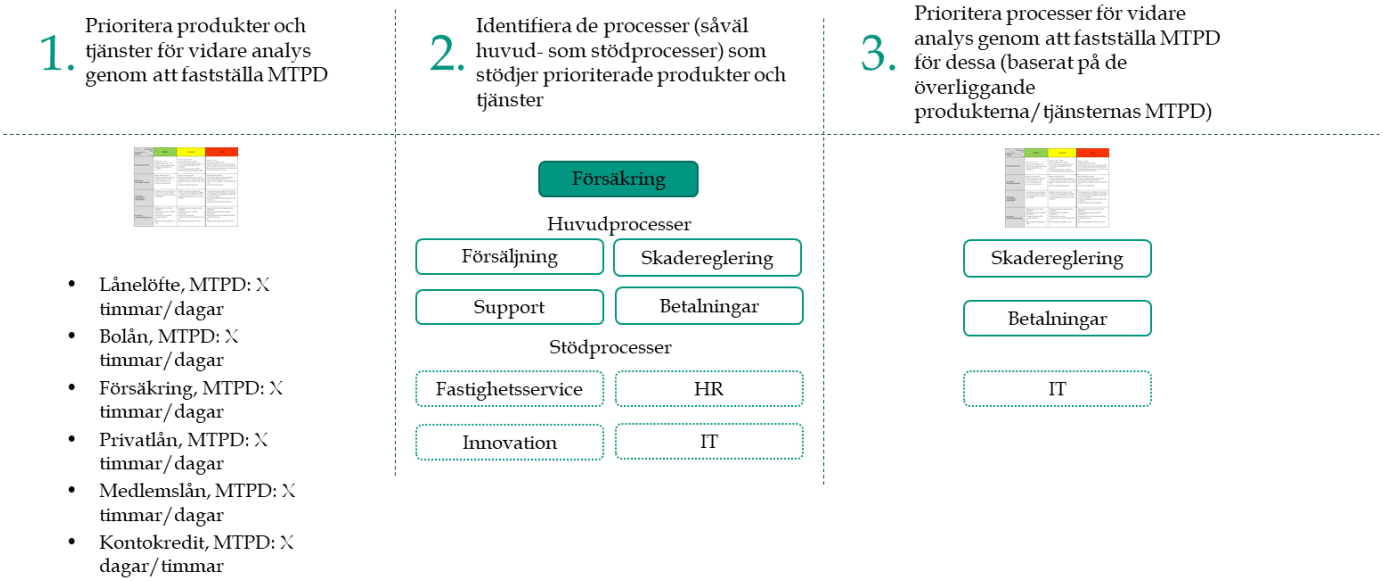
A.3. Strategisk konsekvensanalys

I policyn bör det tydligt klargöras vilka delar av verksamheten som ska omfattas i kontinuitetsarbetet. Avgränsningen kan göras utifrån prioriterade produkter och tjänster, och i förlängningen utifrån processer som stödjer leverans av prioriterade produkter och tjänster. För att fastställa vilka produkter och tjänster, samt vilka av de stödjande processerna som ska inkluderas i kontinuitetsarbetet görs med fördel en så kallad *strategisk konsekvensanalys*.

I ett första steg inventeras och prioriteras organisationens produkter och tjänster. Prioriteringen av produkter och tjänster utgår i första hand ifrån vilka produkter och tjänster som är nödvändiga för att organisationen ska kunna uppnå sina verksamhetsmål och eventuella externa krav.

För samtliga produkter och tjänster fastställs därefter maximalt tolerabel avbrottstid (MTPD)[40] genom att, med utgångspunkt i kriteriemodellen, bedöma hur länge produkten eller tjänsten kan vara otillgänglig innan oacceptabla konsekvenser uppstår. Om det finns en "kalenderrelation" där konsekvenserna är mer påtagliga vid olika tidpunkter (månadsslut, årsslut, kontraktsperioder) ska analysen utgå ifrån att en eventuell störning eller ett avbrott faktiskt sker under dessa perioder. För ytterligare stöd för att definiera maximalt tolerabel avbrottstid för produkter och tjänster, se vidare i detta avsnitt som berör definiering av maximalt tolerabel avbrottstid på processnivå. Samma metod kan användas för produkter och tjänster.

För de produkter och tjänster som är mest tidskritiska identifieras därefter samtliga processer som stödjer leveransen av respektive produkt och tjänst. Dessa processer kan utgöras av såväl huvud- som stödprocesser. Huvudprocesser utgör vanligen sådana processer som är nödvändiga för leveransen av flera produkter och tjänster, medan stödprocesser stödjer huvudprocesser eller produkter och tjänster mer indirekt såsom HR eller it.



Strategisk konsekvensanalys.

[40] *(MTPD) Den maximala tiden som processen kan vara otillgängligt innan oacceptabla konsekvenser uppstår. På engelska Maximum tolerable period of disruption (MTPD).*

När samtliga processer är identifierade analyseras vilken påverkan ett avbrott får om verksamhetens processer är otillgängliga. Detta görs med utgångspunkt från definierade konsekvensnivåer och konsekvenskategorier i kriteriemodellen.

Exemplet nedan utgår från tre konsekvensnivåer; *märkbar påverkan*, *betydande påverkan* och *kritisk påverkan*. Konsekvenskategorierna som används i exemplet är; *ekonomisk påverkan*, *påverkan på förtroende/varumärke* och *påverkan på verksamhetens funktionalitet*. Analysen över påverkansgrad inom respektive konsekvenskategori utgör ett viktigt underlag för att definiera och motivera maximalt tolerabel avbrottstid för processen.

För att definiera maximalt tolerabel avbrottstid för processen kan följande fråga ställas; Hur länge kan processen ligga nere innan någon av konsekvenskategorierna når kriteriemodellens röda linje (avbrottet får inte riskera att nå en kritisk påverkan enligt kriteriemodellen). Den längsta tid som ett avbrott kan fortgå, utan att konsekvenserna blir så pass allvarliga att de enligt kriteriemodellen definieras som oacceptabla, definieras som maximalt tolerabel avbrottstid för processen. För att definiera maximalt tolerabel avbrottstid kan olika tidsintervall användas som utgångspunkt. Exempel på tidsintervall; 4 timmar, 8 timmar, 12 timmar, 24 timmar, 2 dagar, 3 dagar, 7 dagar, 14 dagar, >14 dagar. Vid fastställande av tidskrav tas även hänsyn till prioriterade produkter eller tjänsters beroende till processen.

En konsekvensbeskrivning tas fram för att beskriva vilken påverkan som uppstår om processen inte är tillgänglig. Konsekvensbeskrivningen utgör motivering till satt maximalt tolerabel avbrottstid och görs med fördel utifrån framtagen kriteriemodell. Det är viktigt att motiveringen till satta maximalt tolerabel avbrottstid dokumenteras, detta för att underlätta såväl den vidare analysen som uppföljningar och revideringar.

Kritisk process	**Beskrivning**	Ekonomisk påverkan	Påverkan på förtroende/ varumärke	Påverkan på verksamhetens funktionalitet	**Maximalt tolerabel avbrottstid (MTPD) för processen**	**Motivering till satt maximalt tolerabel avbrottstid (MTPD) för processen**	**Kommentar**
		Nivå (märkbar, betydande, kritisk)	Nivå (märkbar, betydande, kritisk)	Nivå (märkbar, betydande, kritisk)	X timmar/dagar	Konsekvensbeskrivning utifrån bedömning av påverkan (kriteriemodellen)	
Skadereglering	Innefattar samtliga produkter och tjänster för reglering av skador.	**2. Betydande påverkan**	**1. Märkbar påverkan**	**2. Betydande påverkan**	24 timmar	Om processen inte är tillgänglig under 24 timmar kommer detta innebära Förlust: > 20 mkr till följd av avgifter för återförsäkring avtal 2345:7-45 Produktionsförmågan påverkas och minskas under en längre tid då backlogg skapas då kundärenden inte kan mottas. Begränsningar i kapacitet.	Se över avtal för återförsäkring

Definiera konsekvensnivåer utifrån konsekvenskategorier
Vilken påverkan får ett längre avbrott i processen? Utgå från kriteriemodellens konsekvenskategorier och konsekvensnivåer

1

När inträffar en allvarlig påverkan på verksamheten?
Utgå från några olika tidsintervall för att hitta maximalt tolerabel avbrottstid för processen (MTPD), detta i förhållande till bedömda konsekvensnivåer i tidigare steg (1).
Exempel på tidsintervall (4 timmar, 8 timmar, 12 timmar, 24 timmar, 2 dagar, 3 dagar, 7 dagar, 14 dagar , >14 dagar)

2

Definiera MTPD. Ifyllt exempel för processen skadereglering.

Processerna prioriteras i ett sista steg utifrån tidskritikalitet. Processer med korta tidskrav (MTPD) prioriteras för vidare analys, medan processer med längre tidskrav inte prioriteras för vidare åtgärder i ett första steg. För processer med medellånga tidskrav kan en förenklad konsekvensanalys göras. Oavsett tidskritikalitet är det viktigt att tillse att kritiska processer har en utsedd processägare för att besluta om ambition och tidplan. Att ledningen tillser att det finns tillräckligt med tid och resurser för vidare analys är också en viktig förutsättning för att analysen ska bli väl underbyggd och bidra med värde.

Det är viktigt att urvalet av kritiska processer har stöd från verksamhetsledningen, annars riskerar arbetet att stagnera exempelvis på grund av bristande engagemang eller otillräckliga mandat. Det är även viktigt att säkerställa att de kritiska processerna utgör faktiska processer med tydligt definierat start och slut.

I ISO 22301 definieras en process som *"en grupp av aktiviteter som samverkar eller påverkar varandra, och som använder underlag för att åstadkomma ett avsett resultat."*[41] En tumregel som kan användas är att en process bör bestå av en kedja av värdeskapande aktiviteter. Exempel på kritiska processer för finansiella aktörer kan exempelvis vara kreditprocessen för en bank eller skadereglering för ett försäkringsbolag.

Avsnittet i policyn om omfattning och avgränsning bör motivera varför vissa delar av verksamheten eventuellt har uteslutits. En anledning kan vara att en produkt eller tjänst inom snar framtid inte längre kommer att erbjudas av organisationen. En annan kan vara att produkten eller tjänsten bidrar med en väldigt låg andel av organisationens intäkt eller lönsamhet. Vid denna bedömning bör hänsyn tas till eventuell påverkan på viktiga intressenter om produkterna eller tjänsterna skulle vara utsatta för avbrott. Hänsyn bör även tas till regel- och lagkrav, samt påverkan på organisationens rykte. Den avgränsning som beslutats bör ses över och revideras löpande, exempelvis en gång om året. Samtidigt kan omständigheter motivera att detta sker tidigare än den årliga genomgången, exempelvis om organisationens inställning till risk eller marknadsvillkoren ändras. Andra sådana faktorer kan vara att produkter eller tjänster tillkommer eller avslutas, eller att nya lagkrav uppkommer.

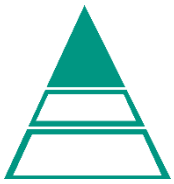
För organisationer som inte tidigare arbetat med kontinuitetshantering kan arbetet till en början upplevas som överväldigande. En rekommendation är därför att de organisationer som ännu inte etablerat att arbetssätt för kontinuitetshantering inledningsvis sätter rimliga mål och förväntningar. Exempelvis genom att till en början endast omfatta ett fåtal verksamheter samt att driva arbetet i projektform.

[41] *SS-EN ISO 22301 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Krav (ISO 22301).*

A.4. Roller och ansvar

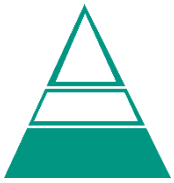
En huvudsaklig framgångsfaktor för kontinuitetshantering är tillsättande av personal med rätt kompetens. I policyn fördelas roller och ansvarsområden, bland annat genom att klargöra frågor som vem som äger processen för kontinuitetshantering samt vilka resurser som finns att tillgå för att implementera kontinuitetshantering.

Organisationens ledning ansvarar för att tillräckligt ansvar och tillräckliga befogenheter tilldelas och delegeras för att säkerställa att kontinuitetsarbetet ska kunna upprätthållas. Ansvar och arbetsuppgifter bör göras formellt tydliga genom att de skrivs in i respektive ansvarig persons arbetsbeskrivning. Ledningen bör också säkerställa att de får regelbunden rapportering avseende kontinuitetshanteringen. Roller och ansvar delas ofta in i strategisk, taktisk, och operativ nivå.



Med den strategiska nivån menas typiskt sett den högsta ledningen. Ansvar på denna nivå inkluderar ofta beslut av policyn och finansiering av kontinuitetsarbetet. Någon från ledningen bör ges ett övergripande ansvar för kontinuitetshanteringen och för arbetets effektivitet. Beroende på storlek och ambition kan även en styrgrupp tillsättas för den strategiska ledningen av kontinuitetshanteringen.

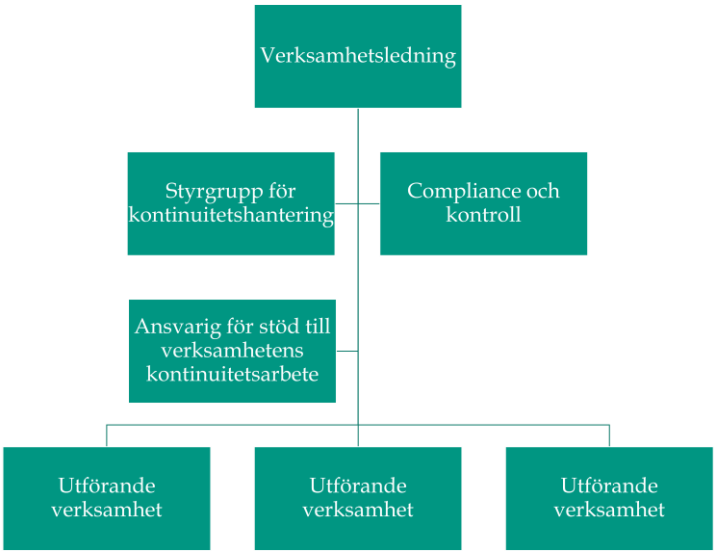
Den taktiska nivån utgör kompetenscentra avseende kontinuitetshanteringen. Den taktiska nivån består av en eller flera personer med det övergripande ansvaret för att stödja det arbete med kontinuitetshantering som bedrivs i organisationen. Ansvar delegeras bland annat avseende utveckling av övningsprogram samt program för utbildning och medvetenhet. Den taktiska nivån leder verksamhetens arbete med de olika stegen, utvecklar och underhåller relevanta mallar och verktyg samt hanterar dokumentation.



Den operativa nivån är de individer som ansvarar för och arbetar i de verksamheter som kontinuitetshanteringen söker upprätthålla. Dessa personer genomför analys av verksamheten, utvecklar kontinuitetslösningar och -planer för sina områden, samt genomför tester och övningar. Dessa personer bör ha en hög kompetens avseende kontinuitetshantering inom sitt område.

Gemensamt för samtliga nivåer är att individer som tilldelas ansvar och roller bör ha tillräcklig kompetens och ha genomgått relevant utbildning. Vidare är det viktigt att kontinuitetspolicyn är förankrad på samtliga nivåer för att säkerställa gemensamma förväntningar och målsättningar med kontinuitetsarbetet.

Ett exempel på hur roller och ansvar kan organiseras återges i diagrammet på nästkommande sida. Beroende på organisationens storlek och behov inom kontinuitetshantering kan dessa nivåer självfallet se olika ut. Som noterats ovan är oftast nyttan av en styrgrupp tydligare hos större organisationer, där kontinuitetshanteringen också är mer omfattande.



Roller och ansvar inom kontinuitetshantering.

Verksamhetsledningen står typiskt sett för den strategiska inriktningen, vilket även kompletteras av en eventuell styrgrupp. Compliance och kontroll är den funktion som utvärderar kontinuitetshanteringen kopplat till mål samt regelefterlevnad.

A.5. Metod och rutiner

Policyn bör beskriva vilka metoder och rutiner som är relevanta i arbetet med kontinuitetshantering. När organisationen tar fram en policy kan det vara nyttigt att lyfta fram standarder eller vägledningar som följs, såsom ISO 22301. Hänsyn bör tas till hur policyn förhåller sig till angränsande områden som kvalitets- och säkerhetsarbetet, samt till organisationens arbete med incident-, risk- och krishantering. Har organisationen en policy för kontinuitetshantering på plats kan en gap-analys belysa hur policyn förhåller sig till vägledningar och standarder. Gapet däremellan avgör i vilken utsträckning och på vilket sätt dokumentationen behöver kompletteras, uppdateras eller flyttas till andra typer av styrande dokument. Referenser kan noteras till såväl egna som externt tillhandahållna vägledningar, metodstöd eller standarder.

Medan policyn ger en inriktning kring *vad* kontinuitetsarbetet innefattar, beskriver en riktlinje/instruktion/rutinbeskrivning *hur* kontinuitetsarbetet genomförs genom tydligt beskrivna processer, rutiner och metoder.

Policy

Exempelstruktur

1. Introduktion
   - Syfte och mål
   - Inriktning och principer
2. Organisationens kontext
   - Interna faktorer
   - Externa faktorer
3. Avgränsning och omfattning
4. Roller och ansvar
5. Metoder och rutiner
6. Kriteriemodell

Checklista innehåll

- Introduktion
  - Vad betyder kontinuitetshantering för organisationen?
  - Vad är målsättningen med kontinuitetshantering i organisationen?
  - Vilken är målgruppen för policyn?
  - Vilka standarder och andra vägledande dokument utgår kontinuitetsarbetet ifrån?
  - Vilka principer styr kontinuitetsarbetet?
- Kriteriemodell
  - Vilka kriterier utgår organisationen för?
  - Vilken är organisationens riskacceptans?
- Organisationens kontext
  - Vilka interna drivkrafter styr arbetet, exempelvis kunders och partners förväntningar?
  - Vilka externa drivkrafter styr arbetet, exempelvis lagar/regleringar
- Avgränsning och omfattning
  - Vilka produkter och tjänster omfattas/omfattas inte?
  - Vilka kritiska processer omfattas/omfattas inte?
  - Geografisk och/eller organisatorisk avgränsning?
- Roller och ansvar
  - Vem är ytterst ansvarig?
  - Vem är ansvarig för implementeringen/ansvarig för att driva kontinuitetshanteringsprogrammet?
  - Vilka resurser finns att tillgå i organisationen för att implementera kontinuitetshantering?
- Metoder och rutiner
  - Metodval och hänvisning till exempelvis riktlinje/instruktion/rutinbeskrivning med utförligare metodbeskrivningar
  - Gap-analys mot standarder

Kartläggning av intressenters förväntningar/krav

Produkt/tjänst A

Intressenter	Förväntningar/krav vid normalläge	Förväntningar/krav vid avbrott	Prioritet
Kunder			
Investerare			
Anställda			
Leverantörer/tredjepart			
Tillsynsmyndigheter			
Partners			
Media			
…			

Produkt/tjänst B

Intressenter	Förväntningar/krav vid normalläge	Förväntningar/krav vid avbrott	Prioritet
Kunder			
Investerare			
Anställda			
Leverantörer/tredjepart			
Tillsynsmyndigheter			
Partners			
Media			
…			

Kriteriemodell

Struktur

Konsekvens -nivå / Konsekvens-Kategori	Märkbar	Betydande	Kritisk

Exempel på innehåll

Konsekvens -nivå / Konsekvens-Kategori	1.Märkbar	2. Betydande	3. Kritisk
Ekonomisk påverkan	• *Förlust: 1 kr – 1 mkr* • *Kassalikviditet påverkas <15%* • *Smärre justering i gällande budget, alla planerade aktiviteter kan genomföras*	• *Förlust: 1 mkr – 20 mkr* • *Kassalikviditet påverkas 15-40%* • *Större omprioritering i gällande budget, ett större antal planerade aktiviteter kan ej genomföras* • *Årsredovisningen påverkas, utfallet av årsvinsten kommer att bli mindre än väntat*	• *Förlust: > 20 mkr* • *Kassalikviditet påverkas >40%* • *Gällande budget räcker inte till, stöd utifrån krävs för att genomföra planerade prioriterade aktiviteter* • *Det finansiella resultatet kommer att påverkas starkt, årsvinsten kommer att försvinna*
Påverkan på förtroende/varumärke	• *Ryktet relativt opåverkat* • *Enskild negativ publicering, lokal spridning, aktualitet en dag* • *Större antal klagomål (>5)* • *Förlust av låg andel kunder*	• *Ryktet kortsiktigt påverkat* • *Ett fåtal negativa publiceringar, nationell spridning, aktualitet en dag till ett fåtal dagar* • *Fåtal krav på åtgärder och/eller kompensation (<5)* • *Förlust av betydande andel kunder*	• *Ryktet långsiktigt påverkat* • *Flera publiceringar med hård kritik, nationell spridning, aktualitet dagar till veckor* • *Stort antal krav på åtgärder och/eller kompensation (>5)* • *Förlust av stor andel kunder*
Påverkan på verksamhetens funktionalitet	• *Obetydlig minskning i förmågan att lösa kritiska verksamhetsuppgifter* • *Produktionsförmågan påverkad med kan bibehållas*	• *Märkbar minskning i förmågan att lösa kritiska verksamhetsuppgifter (kan fullföljas, men effektiviteten är påvisbart reducerad)* • *Produktionsförmågan påverkas och minskas temporärt*	• *Allvarlig begränsning i förmågan att lösa kritiska verksamhetsuppgifter (omfattning och varaktighet så att verksamheten inte kan fullgöra en eller flera av sina primära uppgifter)* • *Produktionsförmågan påverkas och minskas under en längre tid* • *Indraget tillstånd från Finansinspektionen*
Påverkan på samhällets skyddsvärden	• *Måttliga direkta eller indirekta hälsoeffekter* • *Begränsade störningar i samhällets funktionalitet* • *Övergående misstro mot flera samhällsinstitutioner* *eller* • *Begränsade skador på egendom och miljö*	• *Betydande direkta eller måttliga indirekta hälsoeffekter,* • *Allvarliga störningar i samhällets funktionalitet,* • *Bestående misstro mot flera samhällsinstitutioner eller förändrat beteende,* *eller* • *allvarliga skador på egendom och miljö*	• *Mycket stora direkta eller betydande indirekta hälsoeffekter* • *Mycket allvarliga störningar i samhällets funktionalitet* • *Bestående misstro mot flera samhällsinstitutioner och förändrat beteende* *eller* • *Mycket allvarliga skador på egendom och miljö*

Fastställande av maximalt tolerabel avbrottstid för produkt/tjänst

Produkt/tjänst	**Beskrivning**	Ekonomisk påverkan	Påverkan på förtroende/ varumärke	Påverkan på verksamhetens funktionalitet	**Maximalt tolerabel avbrottstid (MTPD) för produkten/tjänsten**	**Motivering till satt maximalt tolerabel avbrottstid (MTPD) för produkten/tjänsten**	**Kommentar**
		Nivå	Nivå	Nivå	X timmar/dagar	Konsekvensbeskrivning utifrån bedömning av påverkan (kriteriemodellen)	

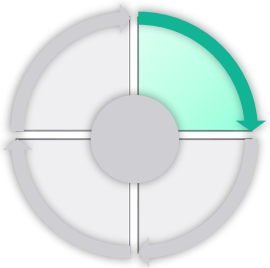
Fastställande av maximalt tolerabel avbrottstid för stödjande processer

Kritisk process	**Beskrivning**	Ekonomisk påverkan	Påverkan på förtroende/ varumärke	Påverkan på verksamhetens funktionalitet	**Maximalt tolerabel avbrottstid (MTPD) för processen**	**Motivering till satt maximalt tolerabel avbrottstid (MTPD) för processen**	**Kommentar**
		Nivå	Nivå	Nivå	X timmar/dagar	Konsekvensbeskrivning utifrån bedömning av påverkan (kriteriemodellen)	

Beroendekartläggning mellan produkter/tjänster och huvudsakliga-/stödjande processer

Stödjande processer / **Produkter och tjänster**		Process 1	Process 2	Process 3	…
		X timmar/dagar (MTPD)	X timmar/dagar (MTPD)	X timmar/dagar (MTPD)	
Produkt/tjänst 1	X timmar/dagar (MTPD)				
Produkt/tjänst 2	X timmar/dagar (MTPD)				
Produkt/tjänst 3	X timmar/dagar (MTPD)				
…	X timmar/dagar (MTPD)				
…	X timmar/dagar (MTPD)				

Appendix B - Analys av verksamheten



Analys av verksamheten syftar till att skapa en kartläggning av organisationens kritiska processer, vilka identifierats genom den strategiska konsekvensanalysen beskriven i Appendix A. För de identifierade och prioriterade kritiska processerna genomförs en konsekvensanalys[42] för att skapa en förståelse för hur avbrott och störningar påverkar verksamhetens operativa förmåga och möjlighet att uppnå fastställda verksamhetsmål. Konsekvensen klargör även hur beroendekedjorna ser ut, samt vilka krav på tillgänglighet som bör ställas på processerna för att upprätthålla kontinuitet.

Efter konsekvensanalysen görs en riskbedömning för att avgöra om de befintliga kontinuitetslösningarna är tillräckliga för att möta uppsatta krav för upprätthållande. Riskbedömningen skapar en förståelse för verksamhetens befintliga förmåga att möta avbrott och störningar, samt fastställer en utgångspunkt för det fortsatta arbetet med utveckling av kontinuitetsstrategier samt kontinuitetslösningar och -planer. Genom konsekvensanalysen och riskbedömningen kan verksamheten identifiera åtgärder för att minimera konsekvenserna av ett avbrott, minska avbrottstiden samt minska sannolikheten att ett avbrott inträffar.

Analys av verksamheten är det steg som är mest tidskrävande för involverade personer i den operativa verksamheten. För att få bra kvalitet i analysresultatet är det viktigt att säkerställa att tillräckligt med tid kan frigöras för de personer som bör inkluderas i analysen. Att det inom organisationen finns ett gemensamt arbetssätt, en fastställd kriteriemodell samt mallar för genomförande och dokumentation av analysresultatet är andra nyckelparametrar. I takt med att kontinuitetshantering implementeras i verksamheten är det viktigt att samla lärdomar från genomförd analys och använda dessa erfarenheter som ingångsvärden vid vidare arbete, samt vid revision av styrande dokument. Analys av verksamheten kan sammanfattningsvis delas in i två delar:

B.1. Konsekvensanalys

Konsekvensanalysen görs för respektive kritisk process som prioriterats för vidare analys i tidigare aktivitetssteg. Om de kritiska processerna har definierats och beskrivits i tidigare arbete, exempelvis i genomförda processkartläggningar, informationskartläggningar eller verksamhetsbeskrivningar, bör underlaget tas med i det vidare kontinuitetsarbetet.

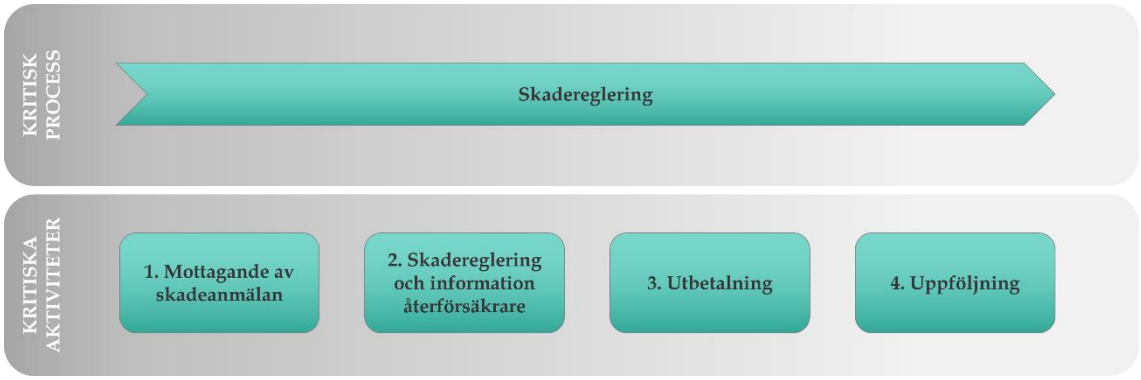
[42] BIA - *Business Impact Analysis (ISO 22301).*

Genom konsekvensanalysen analyseras den effekt som en störning eller avbrott har på verksamheten. Att ha kunskap om hur störningar och avbrott kan påverka verksamhetens förmåga att utföra processen är central för att säkerställa kontinuitet i verksamheten. Genom konsekvensanalysen genereras även kravställning gentemot såväl interna som externa resurserna i form av tidskrav.

Format	• Konsekvensanalysen utförs med fördel genom en workshop för respektive identifierad kritisk process. • Som komplement kan intervjuer göras. Dessa riskerar dock ofta att bli tidskrävande. Även enkäter kan användas men då kan kontrollen över kvaliteten i insamlat underlag riskera att förloras.
Deltagare	• 5-10 deltagare, viktigt att säkerställa att gruppen inkluderar: – Personer som har en övergripande roll och har mandat att fatta beslut. – Personer med operativ kunskap om aktiviteter och resurser samt vilka konsekvenser det får om resurser är otillgängliga.
Tidsåtgång	• En till två halvdagar för att rita upp kartan och en till två halvdagar för att sätta tidskraven (beroende på omfattning och komplexitet).
Slutprodukt	• En karta som visualiserar den kritiska processens aktiviteter samt beroende till interna och externa resurser. • Definierade maximalt tolerabel avbrottstid för aktiviteter. • Definierade mål för återställningstid för aktiviteter och resurser. • Definierade mål för återställningspunkt för it-resurser.

Identifiering av kritiska aktiviteter

Första steget i konsekvensanalysen är att identifiera vilka kritiska aktiviteter som måste kunna utföras för att säkerställa att den kritiska processen fungerar. I figuren nedan visas hur de identifierade aktiviteterna kan presenteras i form av ett förenklat exempel för processen ”skadereglering” för ett försäkringsbolag.



Exempel på kritiska aktiviteter.

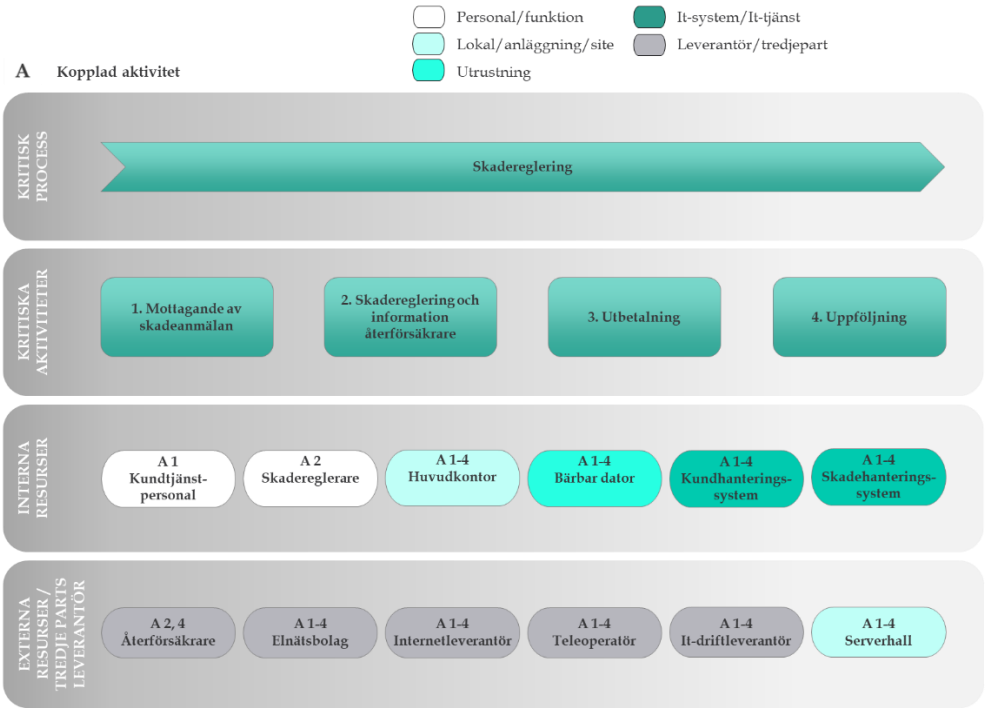
Om en aktivitet innefattar moment som har olika lösningar vid avbrott och/eller är olika tidskritiska, så bör den delas upp i olika aktiviteter. Eftersom aktivitetsidentifieringen är grunden för stora delar av analysen är det viktigt att säkerställa att alla kritiska aktiviteter är med, men även att aktiviteter som inte är kritiska sorteras bort. Samtliga aktiviteter numreras avslutningsvis för att underlätta visualiseringen av beroendet till underliggande resurser.

Tips för genomförande:
- Börja hellre med få ”breda” aktiviteter än att dela upp dem för detaljerat
- Tänk på att beskriva aktiviteterna i form av ”vad som görs”, beskriv gärna som hela meningar inledningsvis för att komma igång
- Är det ett tydligt flöde, beskriv även aktiviteterna i denna form, om inte, gruppera istället efter leveransområde eller typ av tjänst
- Notera vid behov kommentarer (t.ex. vad som ingår i aktiviteten)

Identifiering av kritiska resurser

För att kunna utföra de identifierade kritiska aktiviteterna krävs i sin tur både interna och externa resurser. Ett nästa steg är därför att identifiera de resurser som behövs för att utföra respektive aktivitet. Identifiering sker med fördel genom att ta en aktivitet i taget och identifiera de interna och externa resurser som behövs för att genomföra aktiviteten. Nedan ges några exempel på övergripande resurstyper samt interna och externa resurser.

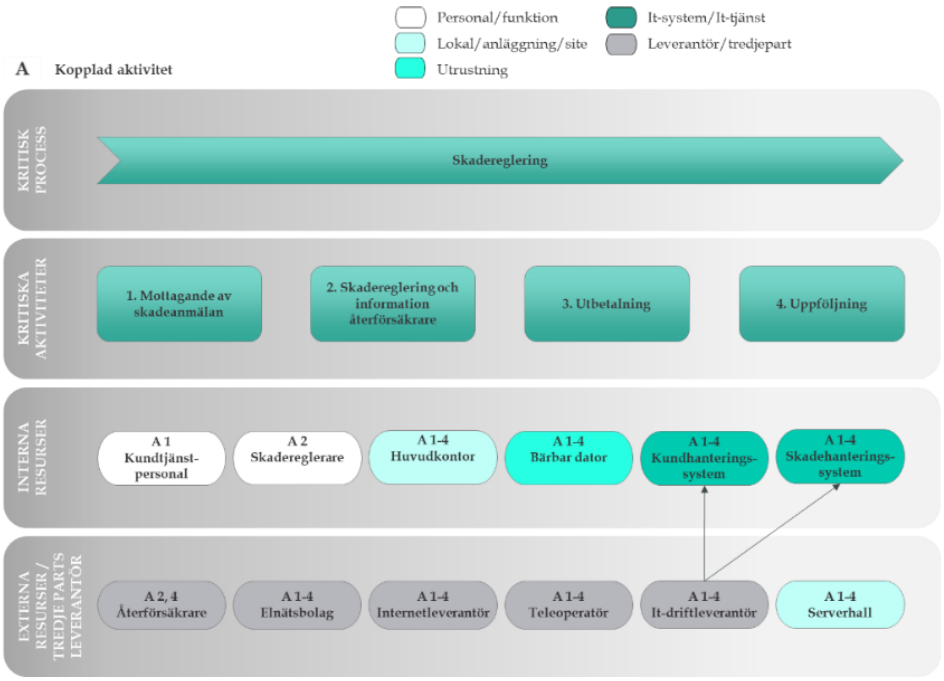
Interna resurser:	Externa resurser:
• Personal/funktion • Lokal/anläggning/site • Utrustning • It-system/It-tjänst (informationsbärande resurser)	• Leverantör/tredjepart – Tjänsteleverantör, systemleverantör, outsourcingpartner etc. • Personal/funktion • Lokal/anläggning/site • Utrustning • It-system/It-tjänst (informationsbärande resurser)



Exempel på kritiska resurser.

Visualisering av beroendekedjor

Resultatet av identifiering av aktiviteter samt interna och externa resurser presenteras med fördel i en karta som även visualiserar processens underliggande beroendekedjor. Beroendet mellan resurser och aktiviteter visualiseras genom att ange motsvarande aktivitetsnummer på den eller de aktiviteter (A) som resursen stödjer. Genom att använda pilar kan specifika beroenden mellan resurser visualiseras. Det är viktigt att konsekvensanalysen beskriver hur processens beroendekedjor ser ut i ett normalläge, vilket innebär att den inte ska inkludera reservlösningar som exempelvis reservkraft. I figuren nedan visas hur de identifierade aktiviteterna och resurserna kan beskrivas för det förenklade exemplet ”Skadereglering”.



Visualisering av beroendekedjor.

Bedömning av maximalt tolerabel avbrottstid

När kritiska aktiviteter samt interna och externa resurser identifierats är nästa steg att definiera hur långa avbrott som kan tolereras för respektive aktivitet. I tidigare avsnitt definierades maximalt tolerabel avbrottstid (MTPD) för processen ”Skadereglering” till 24 timmar (se appendix A för vidare läsning om strategisk konsekvensanalys).

I tidigare avsnitt definierades maximalt tolerabel avbrottstid (MTPD) för processen till 24 timmar.

För att kunna definiera maximalt tolerabel avbrottstid för aktiviteterna är det viktigt att utgå från maximalt tolerabel avbrottstid för den överliggande processen, samt framtagen kriteriemodell som definierar organisationens riskacceptans.

Tips för genomförande:

- För varje aktivitet ställs frågan; Hur länge kan aktiviteten ligga nere innan något av kriterierna når kriteriemodellens röda linje? Svaret på frågan är maximalt tolerabel avbrottstid för aktiviteten
- Motivera satta tidskrav
- Tänk på att mäta mot samtliga konsekvenskategorier och konsekvensnivåer i kriteriemodellen och fastställa tidskravet baserat på den kategori som ger kortast tid
- Om konsekvenserna av ett avbrott varierar beroende på när det inträffar ska tidskraven utgå ifrån ett avbrott under den mest kritiska perioden
- Gå tillbaka till avsnittet A3 Strategisk konsekvensanalys i vägledning för att få ytterligare stöd i att definiera maximalt tolerabel avbrottstid (MTPD)

Den längsta tid som ett avbrott kan fortgå, utan att konsekvenserna blir så allvarliga att de enligt kriteriemodellen definieras som oacceptabla, är maximalt tolerabel avbrottstid för aktiviteten. När maximalt tolerabel avbrottstid definieras för respektive aktivitet så bör antagandet göras att övriga aktiviteter inom processen fungerar normalt. Maximalt tolerabel avbrottstid kan variera från minuter till månader beroende på vilken typ av aktivitet det handlar om, men kan som lägst överensstämma med maximalt tolerabel avbrottstid för processen. Med detta menas att om avbrottstid för hela processen är 24 timmar, så kan inte avbrottstiden för en aktivitet understiga 24 timmar. Om en aktivitet bedöms ha kortare maximalt tolerabel avbrottstid än så, behöver maximalt tolerabel avbrottstid för processen justeras.

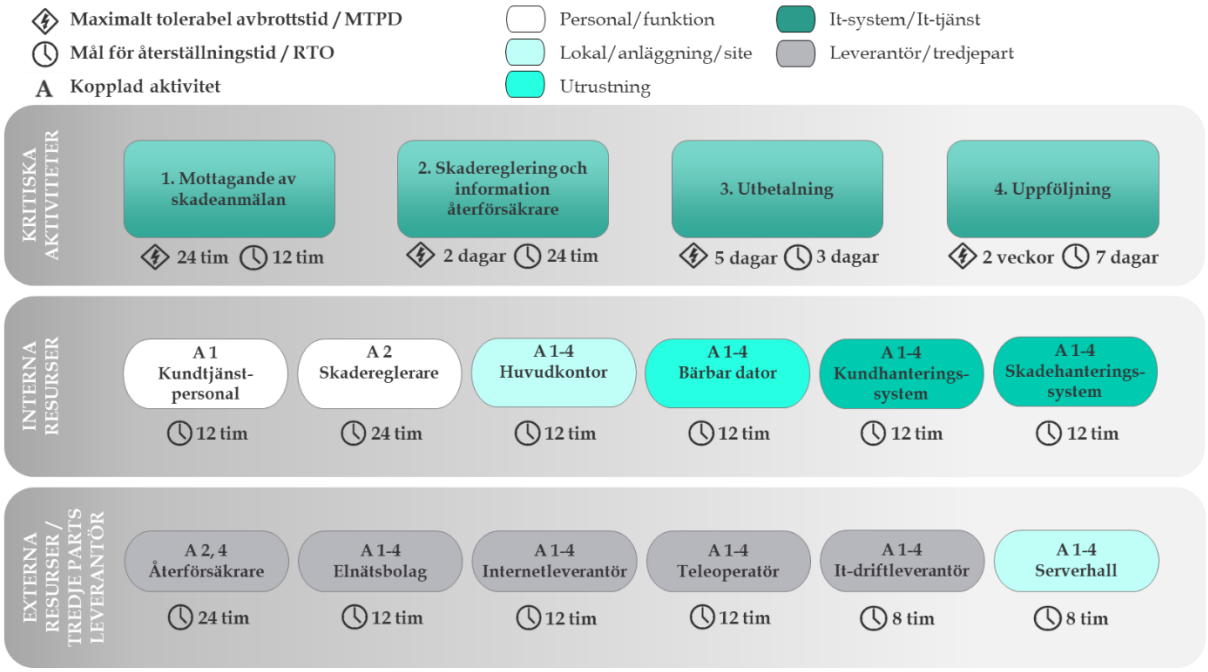
Bedömning av mål för återställningstid (RTO)

Som ett nästa steg definieras aktiviteternas och resursernas mål för återställningstid (RTO). Återställningstid är den tid efter en incident inom vilken det är nödvändigt att en aktivitet eller resurs återställs.

Med detta menas den tid inom vilken aktiviteten eller resursen måste kunna återgå till normal funktion efter ett avbrott för att maximalt tolerabel avbrottstid ej ska överskridas. Definierade mål för återställningstider kan inte överskrida maximalt tolerabel avbrottstid.[43]

Definierad maximalt tolerabel avbrottstid samt mål för återställningstid på aktivitetsnivå utgör ingångsvärden till mål på återställningstid på de underliggande resurserna. Mål för återställningstid på resursnivå anger inom vilken tid den enskilda resursen måste återställas vid ett avbrott, för att den/de aktiviteter resursen stödjer inte ska överskrida definierad maximalt tolerabel avbrottstid. En resurs stödjer vanligtvis flera aktiviteter. Mål för återställningstid för resursen bör då vara i nivå med den kortaste återställningstiden för den aktivitet som resursen stödjer. Detta exemplifieras i figuren nedan där återställningstiden för resursen *skadehanteringssystem* definieras till 12 timmar, då den kortaste återställningstiden för de aktiviteter som resursen stödjer är 12 timmar (*1. Mottagande av skadeanmälan*). För resurser med underliggande resursberoenden är det också viktigt att ta hänsyn till hela beroendekedjan inför fastställande av mål för återställningstid för respektive resurs.

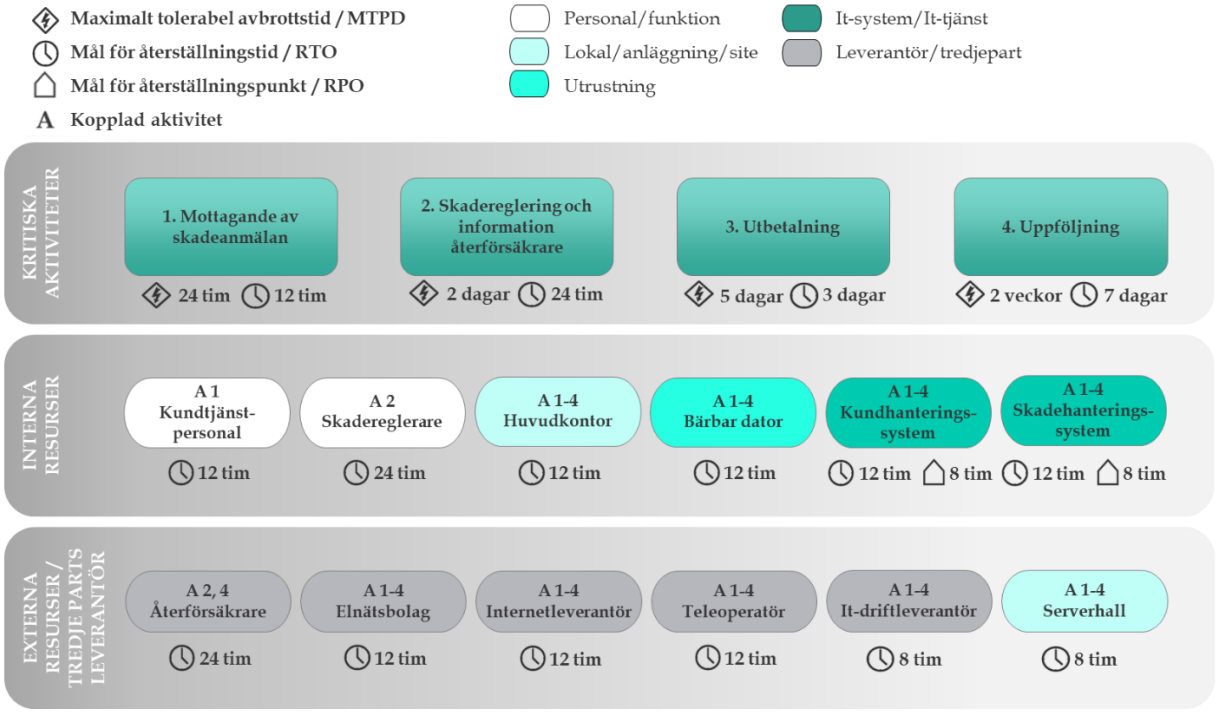
Mål för återställningstid bör alltid sättas med en säkerhetsmarginal i förhållande till maximalt tolerabel avbrottstid.



[43] *SS-EN ISO 22301 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Krav. Recovery Time Objective (RTO). Återställningstid definieras även på aktivitetsnivå utifrån uppdateringar i ISO 22301.*

Bedömning av återställningspunkt (RPO)

För informationsbärande resurser, exempelvis it-system, bör mål för återställningspunkt (RPO)[44] definieras. Detta mått innebär den punkt till vilken det är nödvändigt att återställa den information/data som används av en it-resurs, för att möjliggöra för resursen att återgå till normal leveranskapacitet. Mål för återställningspunkt anger hur mycket information/data som kan gå förlorad innan förlusten får negativa konsekvenser. Begreppet kan även kallas ”Maximum data loss”. Definierat mål för återställningspunkt blir ett krav mot it-verksamheten gällande hur ofta informationen behöver säkerhetskopieras.



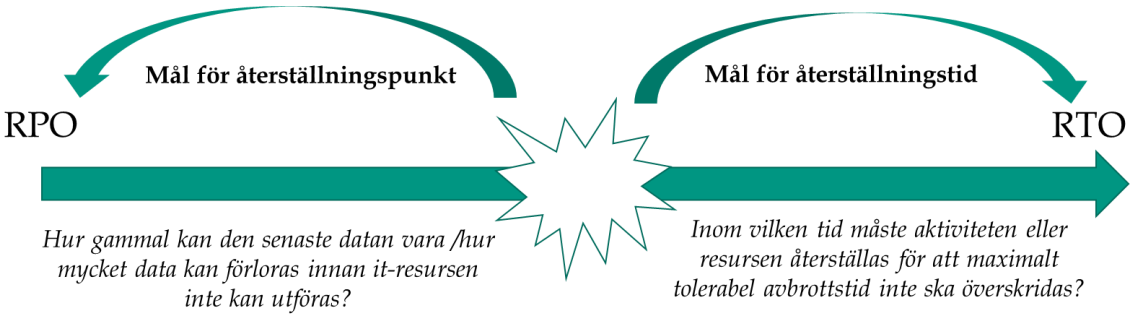
Exempel på definierade mål för återställningspunkt (RPO) för informationsbärande resurser.

Förtydliganden av begreppen mål för återställningstid samt mål för återställningspunkt

Mål för återställningstid och mål för återställningspunkt är två viktiga mått inom ramen för kontinuitetshantering och är även centrala begrepp inom it och disaster recovery.

De mål för återställningstider/-punkter som definieras för kritiska resurser anger bland annat hur kontinuitetslösningar behöver dimensioneras och utgör också en grund för prioritering mellan kritiska resurser. Se illustrationen nedan för ytterligare beskrivning av de två begreppen.

[44] *Recovery Point Objective (RPO) (ISO 22301).*



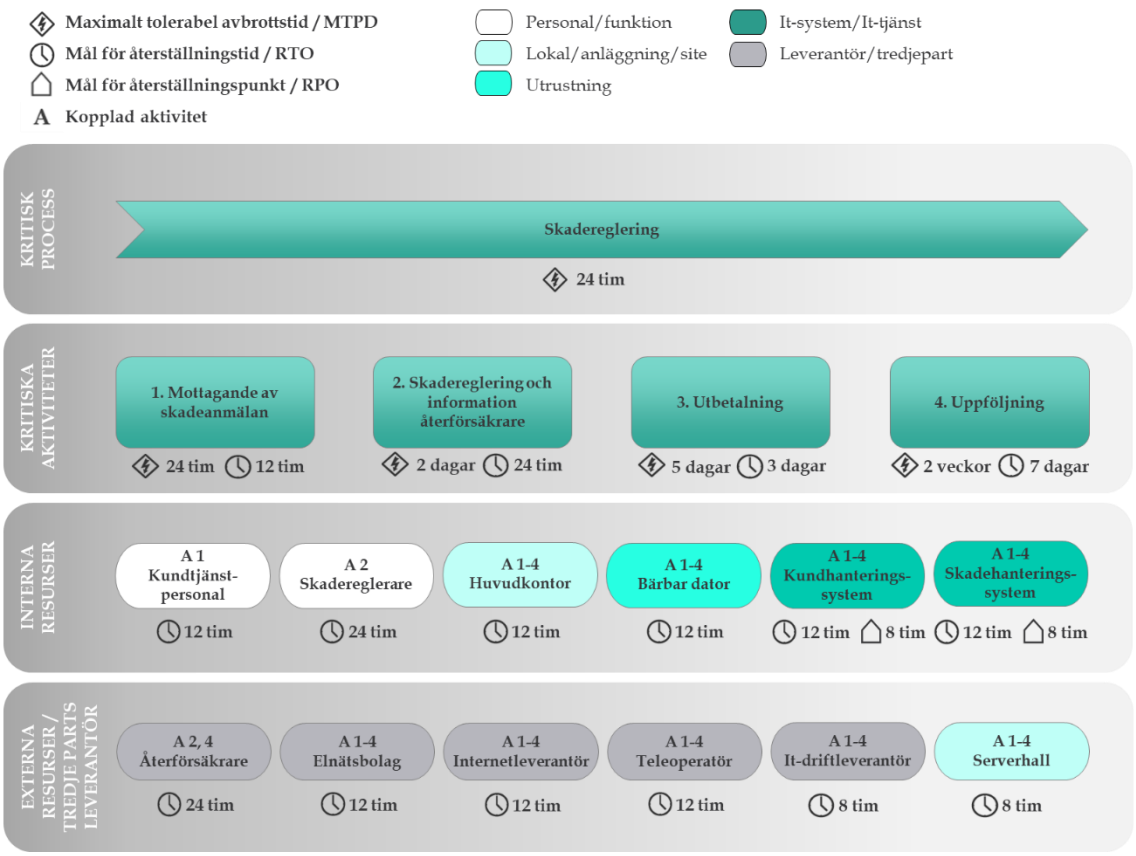
De definierade tidskraven används samlat som stöd för prioritering av åtgärder vid händelse av avbrott eller störning. Tidskraven utgör även en intern såväl som extern kravställning på resurser som processen är beroende av för att kunna upprätthållas. Tidskrav på interna it-system och it-tjänster fungerar exempelvis som ingångsvärden för it-verksamhetens fortsatta kontinuitetsarbete. För it-tjänster blir analysen ofta omfattande och en beskrivning av hur denna analys kan genomföras finns i Appendix F – *Kontinuitetshantering för it-verksamheten*.

På samma sätt används tidskraven gällande externa beroenden i dialog och kravställning gentemot leverantörerna enligt Appendix G – *Kontinuitetshantering för outsourcad verksamhet*.

Dokumentation av konsekvensanalys

Det finns olika sätt att dokumentera resultatet av konsekvensanalysen. Ett sätt är att visualisera beroendekedjor är i en karta. Resultatet av analysen kan även dokumenteras i ett Excelark där kritiska aktiviteter, interna och externa resurser samt tidskrav specificeras. Det viktiga är att se till att dokumentationen av konsekvensanalysen visar processens underliggande beroendekedjor i form av vilka aktiviteter som måste kunna utföras för att den kritiska processen ska upprätthållas, vilka interna och externa resurser som stödjer respektive aktivitet, samt vilka tidskrav som definierats för aktiviteter och resurser.

I figurerna nedan visas förslag på hur konsekvensanalysen kan dokumenteras.



Exempel på hur resultatet av konsekvensanalysen kan visualiseras.

På aktivitetsnivå - dokumentation av kritiska aktiviteter

Kritisk aktivitet	Beskrivning	Ekonomisk påverkan	Påverkan på förtroende/ varumärke	Påverkan på verksamhetens funktionalitet	Maximalt tolerabel avbrottstid (MTPD) för aktiviteten	Motivering till satt maximalt tolerabel avbrottstid (MTPD) för aktiviteten	Mål för återställningstid (RTO) för aktiviteten	Motivering till satt mål för återställningstid (RTO) för aktiviteten	Kommentar
		Nivå	Nivå	Nivå	X timmar/dagar	Konsekvens-beskrivning utifrån bedömning av påverkan (kriteriemodellen)	X timmar/dagar	Krav på återställning utifrån satta tidskrav på aktiviteten	
Mottagande av skadeanmälan	Då ärende mottas via telefon eller hemsida.	1. Märkbar påverkan	1. Märkbar påverkan	2. Betydande påverkan	24 timmar	Om aktiviteten inte är tillgänglig under 24 timmar kommer det innebära en allvarlig påverkan på produktionsförmågan (minskas) under en längre tid, eftersom backlogg skapas då kundärenden inte kan mottas.	12 timmar	För att inte riskera att överskrida satt MTPD behöver aktiviteten mottagande av skadeanmälan vara återställd inom 12 timmar.	Se över kapacitets-begränsningar
...									

Exempel på hur kritiska aktiviteter från konsekvensanalysen kan dokumenteras.

På resursnivå - dokumentation av kritiska resurser

Kritisk resurs	Beskrivning	Typ av resurs	Resurskategori	Kopplad aktivitet/ aktiviteter	Mål för återställningstid (RTO) för resursen	Motivering till satt mål för återställnings-tid (RTO) för resursen	Mål för återställnings-punkt (RPO) för resursen (endast för it-system/it-tjänster)	Motivering till satt mål för återställnings-punkt (RPO) för resursen	Kommentar
		Intern/extern	Personal/funktion Lokal/anläggning/ site Utrustning It-system/It-tjänst Leverantör/tredjepart	Ange den/de aktiviteter som resursen stödjer	X timmar/dagar	Återställnings-beskrivning utifrån satta tidskrav	X timmar/dagar	Beskriv behovet av återställning för den information/data som används av it-resursen utifrån satta tidskrav	
Skadehanterings-system	System för hantering av skadeanmälningar	Intern	It-system/It-tjänst	A 1-4 1. Mottagande av skadeanmälan 2. Skadereglering och information återförsäkrare 3. Utbetalning 4. Uppföljning	12 timmar	RTO sätts i förhållande till de aktiviteter som resursen stödjer. För att inte riska att överskrida beslutad MTPD behöver systemet återtällas inom 12 timmar.	8 timmar	För att inte efterregisterings-arbetet ska bli för omfattande kan inte datan i systemet vara äldre än 8 timmar.	
...									

Exempel på hur kritiska resurser från konsekvensanalysen kan dokumenteras.

B.2. Konsekvensanalys – Informationsbärande resurser

En grundläggande förutsättning för att knyta samman informationssäkerhet och kontinuitetshantering är en genomförd informationsklassning där organisationens information värderas utifrån vilka konsekvenser otillräckligt skydd för informationens konfidentialitet, riktighet och tillgänglighet skulle kunna få. Detta utgör grunden för att kunna upprätthålla informationssäkerhet i kontinuitetsarbetet och behöver således vara genomfört innan arbetet med konsekvensanalys påbörjas.

Om informationsklassning inte är genomförd inom organisationen sedan tidigare är det normalt sett informationssäkerhetsansvarig (eller annan ansvarig funktion) som ska initiera detta arbete. MSB har tagit fram ett metodstöd för systematiskt informationssäkerhetsarbete[45] som innehåller vägledningar, verktyg, tips, mallar och annat stöd och råd för informationsklassning och andra stödjande aktiviteter.

För att kunna uppfylla krav på planering och upprätthållande av informationssäkerhet under en störning i enlighet med ISO 27000-serien är det nödvändigt att konsekvensanalysen även innefattar informationstillgångar och dess beroenden gentemot informationsbärande resurser. Detta syftar till att skapa en tydlig bild över vilka informationstillgångar som är nödvändiga för att utföra respektive kritisk aktivitet, samt vilka informationsbärande resurser som hanterar och lagrar respektive informationstillgång.

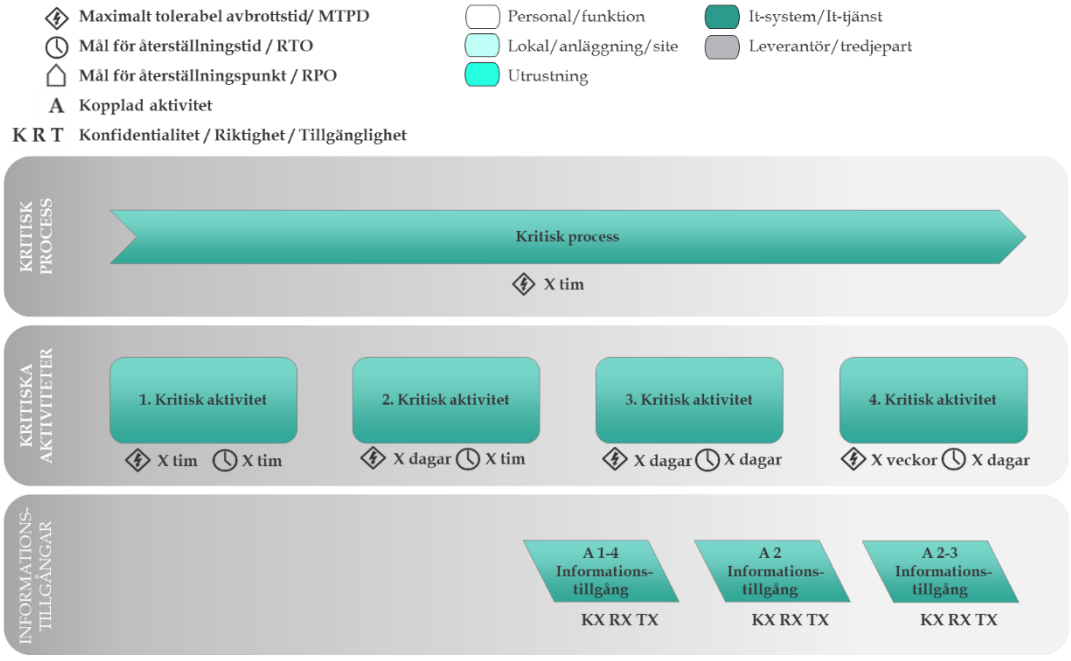
[45] *MSB - Stöd för systematiskt arbete med informationssäkerhet i organisationer.* https://www.informationssakerhet.se/

Detta avsnitt i vägledningen för kontinuitetshantering tar sin utgångspunkt från MSB:s vägledning för processorienterad informationskartläggning[46] som är tänkt att vara ett stöd för att kartlägga och analysera den information en organisation är beroende av.

Om organisationen har genomfört processorienterad informationskartläggning i enlighet med MSB:s vägledning kan kartläggningen överföras direkt till konsekvensanalysen. Om en sådan kartläggning inte finns tillgänglig bör en grundläggande informationskartläggning göras direkt i samband med konsekvensanalysen.

När de kritiska aktiviteterna har identifierats och dokumenterats i konsekvensanalysen är det dags att identifiera samtliga informationsgångar som är nödvändiga för att utföra respektive kritisk aktivitet. Ta gärna stöd av processägare och informationsägare under denna analysfas. För att analysen inte ska bli för komplex bör informationstillgångar beskrivas på en lämplig nivå. Om konsekvensanalysen har föregåtts av en informationsklassning eller processorienterad informationskartläggning bör samtliga informationstillgångar redan vara identifierade, beskrivna och klassade. Identifierade informationstillgångar kan även grupperas eller slås ihop för att förenkla konsekvensanalysen något.

I figuren nedan visas principen för hur resultatet av de identifierade informationstillgångarna kan presenteras i förhållande till processen och dess kritiska aktiviteter. Beroendet mellan informationstillgångar och aktiviteter visualiseras genom att ange motsvarande aktivitetsnummer på den eller de aktiviteter (A) som informationstillgången stödjer. Nytt i figuren är även informationstillgångarnas klassning utifrån krav på konfidentialitet, riktighet och tillgänglighet.



Exempel på hur identifierade informationstillgångarna kan visualiseras i förhållande till processen och dess kritiska aktiviteter.

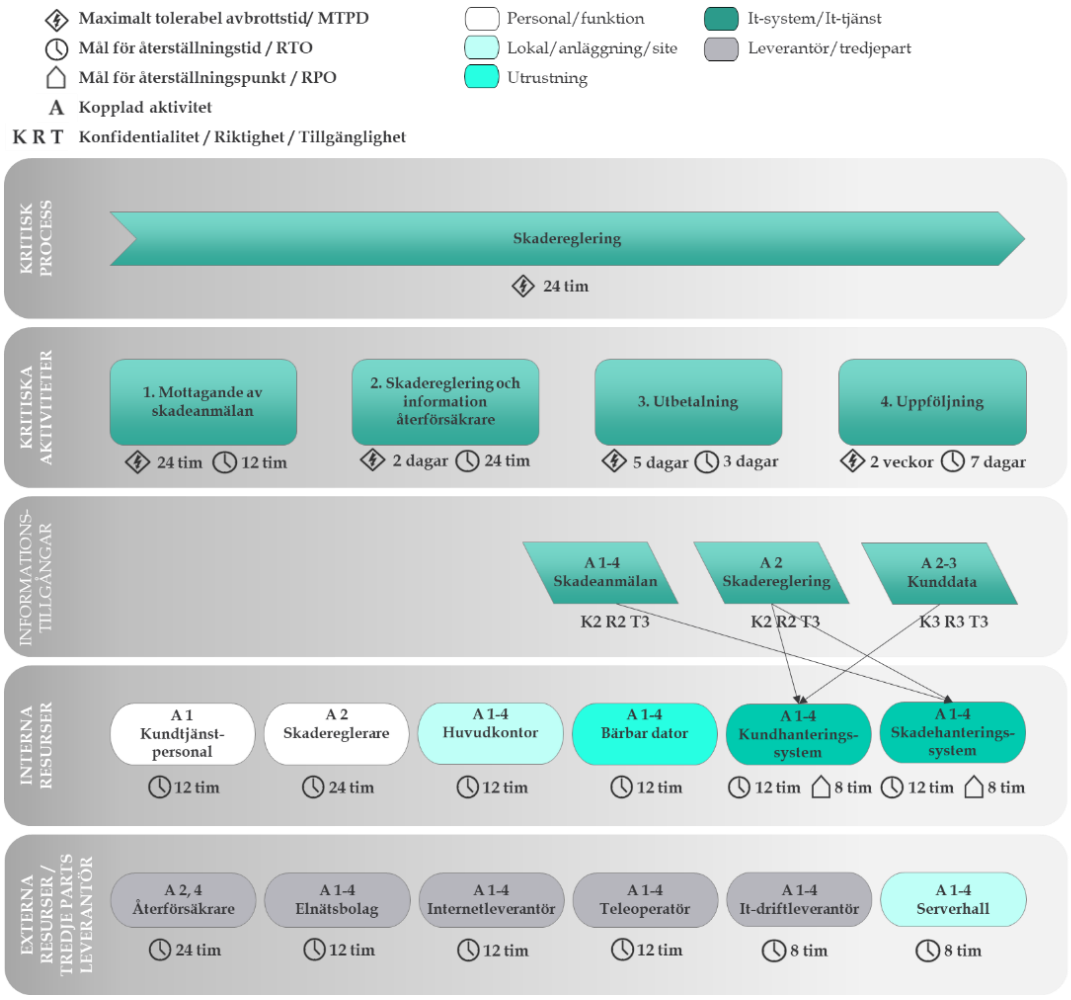
[46] *MSB - Vägledning för processorienterad informationskartläggning.*

I nästa steg anges de beroenden som finns mellan de identifierade informationstillgångarna och de informationsbärande resurserna genom att använda pilar. Ta gärna stöd av informationsägare och systemägare under analysen för att säkerställa att samtliga beroenden identifieras och dokumenteras.

Viktigt att beakta är om flera informationstillgångar behandlas eller lagras i samma informationsbärande resurs, eller om en enskild informationstillgång behandlas eller lagras i flera informationsbärande resurser. Det sistnämnda kan exempelvis vara information som både sparas i ett it-system och samtidigt publiceras på webben.

När samtliga beroendekedjor har identifierats och dokumenterats återstår att ange informationstillgångarnas klassning som erhålls från den redan gjorda informationsklassningen.

I figuren nedan visas identifierade informationstillgångar och dess beroenden för det förenklade exemplet ”Skadereglering”. Genom att studera konsekvensanalysen i dess helhet inklusive dess informationstillgångar kan viktiga slutsatser dras som har avgörande betydelse för att kunna upprätthålla informationssäkerheten genom hela processen vid en störning.



Visualisering av beroendekedjor.

Här följer några exempel på slutsatser som kan dras när konsekvensanalysen är färdigställd:

- Vilka aktiviteter som blir påverkade och därmed konsekvenserna om en enskild informationstillgång blir otillgänglig.
- Vilka informationstillgångar som blir påverkade och därmed konsekvenserna om ett enskilt it-system eller annan informationsbärare blir otillgänglig.
- Diskrepanser mellan informationstillgångars klassning och mål för återställningstid (RTO) och mål för återställningspunkt (RPO) för de informationsbärande resurserna.
- Konsekvenser i verksamheten vid bortfall av informationsbärande resurser och därigenom informationstillgångar.
- Behov av särskilda åtgärder för att bevara informationens skyddsvärden (konfidentialitet, riktighet, tillgänglighet) vid händelse av ett avbrott i en informationsbärande resurs (se riskbedömning).

På resursnivå – dokumentation av informationsbärande resurser och informationstillgångar

Kritisk resurs	**Beskrivning**	**Typ av resurs**	**Resurskategori**	**Kopplad aktivitet/ aktiviteter**	**Informations-tillgångar**	**Mål för åter-ställningstid (RTO) för resursen**	**Motivering till satt mål för återställnings-tid (RTO) för resursen**	**Mål för återställnings-punkt (RPO) för resursen (endast för it-system/it-tjänster)**	**Motivering till satt mål för återställnings-punkt (RPO) för resursen**	**Kommentar**
		Intern/extern	Personal/funktion Lokal/anläggning/ site Utrustning It-system/It-tjänst Leverantör/tredjepart	Ange den/de aktiviteter som resursen stödjer	Ange informations-tillgångar som den informations-bärande resursen hanterar och klassning	X timmar/dagar	Återställnings-beskrivning utifrån satta tidskrav	X timmar/dagar	Beskriv behovet av återställning för den information/data som används av it-resursen utifrån satta tidskrav	
Skadehanterings-system	System för hantering av skadeanmälningar	Intern	It-system/It-tjänst	A 1-4 1. Mottagande av skadeanmälan 2. Skadereglering och information återförsäkrare 3. Utbetalning 4. Uppföljning	Skadeanmälan (K2 R2 T3) Skadereglering (K2 R2 T3) Kunddata (K3 R3 T3)	12 timmar	RTO sätts i förhållande till de aktiviteter som resursen stödjer. För att inte riska att överskrida beslutad MTPD behöver systemet återtällas inom 12 timmar.	8 timmar	För att inte efterregisteringsarbe tet ska bli för omfattande kan inte datan I systemet vara äldre än 8 timmar.	
...										

Exempel på hur informationsbärande resurser och informationstillgångar från konsekvensanalysen kan dokumenteras.

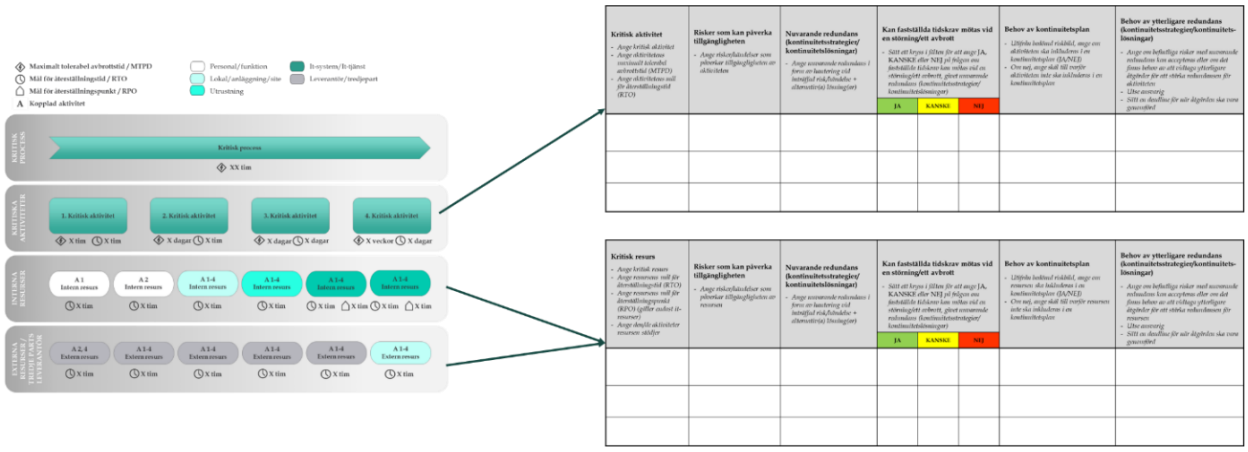
B.3. Riskbedömning

Som sista steg i *Analys av verksamheten* görs en riskbedömning för att få en djupare förståelse för risker kopplade till de aktiviteter och resurser som stödjer den kritiska processen. Genom riskbedömningen avgörs om befintliga strategier och lösningar är tillräckliga för att säkerställa att de identifierade tidskraven inte överskrids. Även eventuella single-point-of-failures identifieras genom en väl genomförd riskbedömning.

I riskbedömningen bedöms organisationens förmåga att möta risker som kan påverka tillgängligheten hos kritiska aktiviteter och resurser, med hänsyn tagen till befintliga

kontinuitetslösningar. Till skillnad mot traditionell riskhantering, exempelvis i enlighet med ISO 31000, utgår riskbedömningen från motståndskraften hos processens stödjande aktiviteter och resurser. Traditionell riskhantering tar istället avstamp i identifierade risker och söker identifiera behandlingar för dessa.

Se avsnitt 2.4, *Koppling till incident-, risk-, och krishantering,* för förtydligande av skillnader mellan kontinuitetshantering och riskhantering. Riskbedömningen kan genomföras på såväl aktivitets- som resursnivå, enligt figuren nedan.



Riskbedömning kan genomföras både på aktivitetsnivå och resursnivå.

På aktivitetsnivån bedöms motståndskraften hos respektive aktivitet på en övergripande nivå, d.v.s. utan att analysera enskilda resursers eventuella bortfall (detta hanteras i riskbedömningen på resursnivå). Befintliga redundans (kontinuitetsstrategier/-lösningar) på aktivitetsnivå identifieras. Utifrån bedömd riskbild anges också om aktiviteten ska inkluderas i en kontinuitetsplan. Där ett behov av ytterligare strategier/lösningar finns, dokumenteras också detta.

På resursnivå identifieras risker för varje kritisk resurs och därefter bedöms huruvida befintlig redundans (kontinuitetsstrategier/-lösningar) är tillräckliga för att möta målet för återställningstid. Utifrån bedömd riskbild anges också om resursen ska inkluderas i en kontinuitetsplan. I de fall befintliga lösningar inte anses tillräckliga, föreslås åtgärder.

Såväl riskbedömning på aktivitetsnivå som på resursnivå följer nedanstående steg:

1. **Identifiera risker som kan påverka tillgängligheten hos aktiviteten eller resursen.**

   Detta steg handlar inte om att skapa en lång lista över samtliga, enskilda risker som kan inträffa och därmed påverka aktiviteten/resursen. Istället bör endast typfall av risker, vilka leder till olika typer av konsekvenser och därmed olika typer av kontinuitetslösningar, identifieras.

2. **Identifiera nuvarande redundans (kontinuitetsstrategier/-lösningar).**

   I detta steg beskrivs befintlig redundans (kontinuitetsstrategier/-lösningar) för att hantera de identifierade riskerna. Lösningarna kan inkludera såväl hantering av den inträffade risken (exempelvis larmning, informationsdelning, återställande av resursen [om intern], felsökning etc.) som alternativa lösningar för att hantera störningen/avbrottet i aktiviteten eller resursen (exempelvis manuella rutiner, reservlokaler, omfördelning av arbetsuppgifter etc.). Endast lösningar som finns på plats i dagsläget ska inkluderas.

   Denna del av riskbedömningen utgör underlag för författandet av kontinuitetsplaner, i vilka de befintliga kontinuitetslösningarna beskrivs vidare i detalj.

   Ytterligare ett resultat av denna del av riskbedömningen är att överdimensionerade kontinuitetslösningar kan identifieras, d.v.s. aktiviteter/resurser som har för hög motståndskraft i relation till uppsatta tidskrav.

3. **Bedöm huruvida aktiviteten och resursen klarar att möte fastställda tidskrav givet att risken inträffar, samt befintlig redundans (kontinuitetsstrategier/-lösningar).**

   Utifrån en skala (exempelvis ”ja”, ”kanske”, ”nej”) bedöms huruvida aktiviteten eller resursen klarar att möta fastställt tidskrav, givet befintlig redundans (kontinuitetsstrategier/-lösningar). Om bedömningen leder till ”kanske” eller ”nej”, föreligger ett behov av att identifiera förslag på ytterligare lösningar som bidrar till att aktiviteten/resursen kan möta fastställt tidskrav.

   Alternativt behöver ett aktivt beslut fattas om att ytterligare kontinuitetslösningar inte ska implementeras, exempelvis p.g.a. orimligt höga kostnader i relation till nyttan.

4. **Behov av kontinuitetsplan**

   Utifrån bedömd riskbild, ange om aktiviteten ska inkluderas i en kontinuitetsplan (exempelvis ”ja” och ”nej”). Om nej, ange skäl till varför aktiviteten/resursen inte ska inkluderas i en kontinuitetsplan.

5. **Beskriv behov av ytterligare redundans (kontinuitetsstrategier/-lösningar)**

   För de aktiviteter och/eller resurser där behov av ytterligare redundans (kontinuitetsstrategier/-lösningar) identifieras, beskriv dessa, uppskatta kostnad samt utse ansvarig och deadline för det fortsatta arbetet.

Figuren nedan visar ett förslag på hur riskbedömning för kritiska resurser kan dokumenteras.

Kritisk resurs - *Ange kritisk resurs* - *Ange resursens mål för återställningstid (RTO)* - *Ange resursens mål för återställningspunkt (RPO) (gäller endast it-resurser)* - *Ange den/de aktiviteter resursen stödjer*	**Risker som kan påverka tillgängligheten** - *Ange risker/händelser som påverkar tillgängligheten av resursen*	**Nuvarande redundans (kontinuitetsstrategier/-lösningar)** - *Ange nuvarande redundans i form av hantering vid inträffad risk/händelse + alternativ(a) lösning(ar)*	**Kan fastställda tidskrav mötas vid en störning/ett avbrott** - *Sätt ett kryss i fälten för att ange* JA, KANSKE *eller* NEJ *på frågan om fastställda tidskrav kan mötas vid en störning/ett avbrott, givet nuvarande redundans (kontinuitetsstrategier/-lösningar)*			**Behov av kontinuitetsplan** - *Utifrån bedömd riskbild, ange om resursen ska inkluderas i en kontinuitetsplan (JA/NEJ)* - *Om nej, ange skäl till varför resursen inte ska inkluderas i en kontinuitetsplan*	**Behov av ytterligare redundans (kontinuitetsstrategier/-lösningar)** - *Ange om befintliga risker med nuvarande redundans kan accepteras eller om det finns behov av att vidtaga ytterligare åtgärder för att stärka redundansen för resursen* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*
			JA	KANSKE	NEJ		
Huvudkontor - *RTO: 12 tim* - *Mottagande av skadeanmälan, Skadereglering och information återförsäkrare, Utbetalning, Uppföljning*	Brand	Prioriterade arbetsuppgifter kan utföras på alternativ plats. Samtlig personal kan delvis arbeta hemifrån med VPN-lösning.		X		JA	VPN-lösning kräver att anställda har med sin arbetsdator hem, vilket inte alla har. Säkerställ att rutin om att alltid ta med arbetsdator hem förtydligas och kommuniceras *Ansvar: It-chef* *Deadline: ÅÅ-MM-DD*
	Elavbrott	Finns reservkraft samt diesel för 3 dagars drift. Prioriterade arbetsuppgifter kan utföras på alternativ plats.	X			JA	Viktigt med löpande test av reservkraft *Ansvar: Kontorschef* *Deadline: årligen MM-DD*

Exempel på hur en riskbedömning kan dokumenteras för kritiska resurser.

Format	• Riskbedömningen utförs med fördel genom en workshop • Som komplement kan intervjuer göras. Dessa riskerar dock ofta att bli tidskrävande. Även enkäter kan användas men då riskerar kontrollen över kvaliteten i insamlat underlag att förloras.
Deltagare	• Samma deltagare som i konsekvensanalysen
Tidsåtgång	• En till två halvdagar (beroende på antal identifierade resurser och deras komplexitet)
Slutprodukt	• En bedömning av om befintlig redundans för respektive resurs är tillräcklig för att uppnå uppsatta mål för återställningstid

B.4. Riskbedömning – Informationsbärande resurser

Riskbedömning av informationsbärande resurser är avgörande för att identifiera svagheter och gap i nuvarande redundans och kontinuitetslösningar i förhållande till informationstillgångarnas klassning. Dessa gap och svagheter måste vara synliggjorda och hanterade vid revidering av befintliga eller utformning av nya kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner.

Genom att samtliga beroendekedjor mellan aktiviteter, informationstillgångar och informationsbärande resurser har identifierats i konsekvensanalysen, kan dessa användas för att identifiera särskilda åtgärder för att bevara informationstillgångarnas skyddsvärden under hela störningen, från att störningen inträffar till att normal verksamhet åter uppnås. Vid riskbedömningen måste således konsekvenserna av att informationen förlorar konfidentialitet och riktighet beaktas och prioriteras utöver behovet att upprätthålla tillgången till informationen. Ibland kan det dock vara nödvändigt att anpassa informationssäkerhetskraven beroende på vilken typ av störning det rör sig om.

Riskbedömning av informationsbärande resurser med hänsyn till informationstillgångarnas klassning har i praktiken samma upplägg och slutprodukt som vid ordinarie riskbedömning på resursnivå, med tillägg av särskilda åtgärder för att bevara informationens skyddsvärden.

För att underlätta riskbedömningen av informationsbärande resurser anges resursens mål för återställningstid (RTO) och mål för återställningspunkt (RPO), samt informationstillgångar som resursen hanterar och deras klassning. Därefter genomförs riskbedömningen enligt steg 1 till 5 som beskrivs i föregående avsnitt.

I steg 6, som är unik vid riskbedömning av informationsbärande resurser, identifieras särskilda åtgärder för att bevara informationens skyddsvärden. Detta steg syftar till att beakta konsekvenserna av att informationen förlorar konfidentialitet och riktighet i samband med risker som påverkar tillgängligheten av den informationsbärande resursen. Även behovet att upprätthålla tillgången till informationen i samband med avbrottet behöver beaktas.

Konsekvens på:	Exempel på åtgärder att beakta:
Konfidentialitet	• Upprätthåll konfidentialiteten vid manuell behandling och lagring av information (ex. inlåsning i säkerhetsskåp och lämna aldrig utan uppsikt). • Extra behörighetskontroller för icke ordinarie personal (intern eller inhyrd).
Riktighet	• Verifiera informationens riktighet vid manuell behandling och lagring under avbrottet, samt vid återföring av data efter avbrottet (ex. rutiner för att säkra att informationen är tillförlitlig, korrekt och komplett).
Tillgänglighet	• Tillgång till informationen på alternativa sätt under avbrottet (ex. utskrift på papper eller genom lagring på alternativa lagringsplatser). • Tillgång till informationen efter avbrottet (ex. genom backup och säker nedstängning av it-system).

Ta gärna stöd av processägare, informationsägare och systemägare under analysen för att säkerställa att nödvändiga åtgärder identifieras och dokumenterats utifrån konsekvensen om informationens skyddsvärden inte kan upprätthållas i samband med avbrottet. Räkna med längre tidsåtgång beroende på antal identifierade informationstillgångar och deras komplexitet.

I figuren nedan visas ett förslag på hur riskbedömning av en informationsbärande resurs kan dokumenteras.

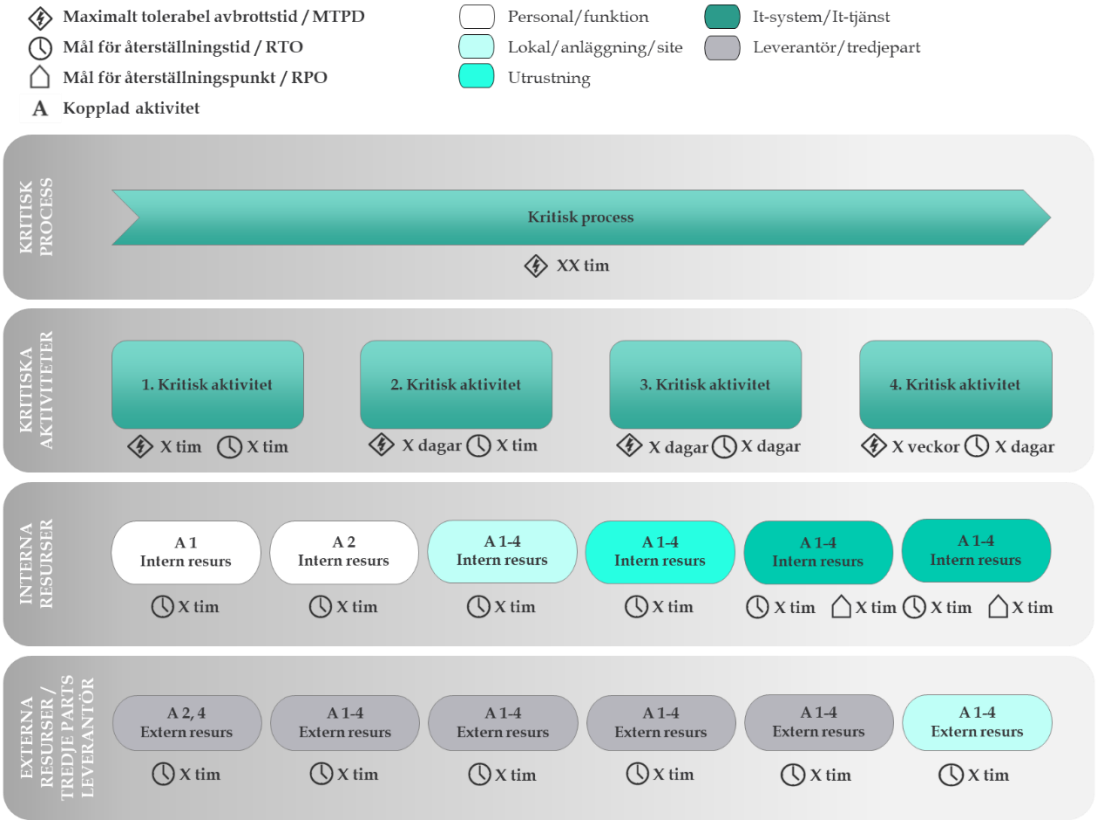
Kritisk resurs (endast informationsbärande resurser) - *Ange kritisk it-resurs* - *Ange it-resursens mål för återställningstid (RTO)* - *Ange it-resursens mål för återställningspunkt (RPO)* - *Ange den/de aktiviteter it-resursen stödjer* - *Ange de informationstillgångar som it-resursen hanterar och klassning*	**Risker som kan påverka tillgängligheten** - *Ange risker/händelser som påverkar tillgängligheten av it-resursen*	**Nuvarande redundans (kontinuitetsstrategier/-lösningar)** - *Ange nuvarande redundans i form av hantering vid inträffad risk/händelse + alternativ(a) lösning(ar)*	**Kan fastställda tidskrav mötas vid en störning/ett avbrott** - *Sätt ett kryss i fälten för att ange* JA, KANSKE *eller* NEJ *på frågan om fastställda tidskrav kan mötas vid en störning/ett avbrott, givet nuvarande redundans (kontinuitetsstrategier/-lösningar)*			**Behov av kontinuitetsplan** - *Utifrån bedömd riskbild, ange om it-resursen ska inkluderas i en kontinuitetsplan (JA/NEJ)* - *Om nej, ange skäl till varför it-resursen inte ska inkluderas i en kontinuitetsplan*	**Behov av ytterligare redundans (kontinuitetsstrategier/-lösningar)** - *Ange om befintliga risker med nuvarande redundans kan accepteras eller om det finns behov av att vidtaga ytterligare åtgärder för att stärka redundansen för it-resursen* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*	**Särskilda åtgärder för att bevara informationens skyddsvärden** - *Ange om det finns behov att vidtaga ytterligare åtgärder för att bevara informationstillgångarnas skyddsvärden utifrån (K)onfidentialitet, (R)iktighet, (T)illgänglighet* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*
			JA	**KANSKE**	**NEJ**			
Skadehanteringssystem - *12 timmar (RTO)* - *8 timmar (RPO)* - *Mottagande av skadeanmälan, Skadereglering och information återförsäkrare, Utbetalning, Uppföljning* - *Skadeanmälan (K2 R2 T3), Skadereglering (K2 R2 T3)*	Elavbrott	Finns reservkraft samt diesel för 3 dagars drift.	X			*JA*	Löpande test av reservkraft - *Ansvar: kontorschef* - *Deadline: ÅÅÅÅ-MM-DD*	Säkerställ att informationen är opåverkad om reservkraften inte längre fungerar - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD* Säkerställ rutiner för informationssäkerhet vid manuell skadereglering - *Ansvar: chef för skadereglering* - *Deadline: ÅÅÅÅ-MM-DD*
	Internet ligger nere	Kontakta IT-leverantör. Ingen alternativ internetförbindelse finns.			X	*JA*	Utred möjliga redundanslösningar - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD*	Säkerställ att informationen är opåverkad under hela avbrottet - *Ansvar: IT-chef* - *Deadline: innan årsskiftet* Säkerställ rutiner för informationssäkerhet vid arbete hemifrån - *Ansvar: chef för skadereglering* - *Deadline: ÅÅÅÅ-MM-DD*
	Skadlig kod	Anti-virusprogram finns, oklart om tillräckligt		X		*JA*	Se över befintlig redundanslösning - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD*	Säkerställ att isolerade backuper finns för att skydda mot förstörelse av ursprungliga data, samt att informationens skyddsvärden bevaras under hela återställnings-förfarandet från backup - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD*

Exempel på hur en riskbedömning kan dokumenteras för informationsbärande resurser.

Mallar för genomförande

Konsekvensanalys

Beroendekartläggning - visualisering av kritiska processer, aktiviteter och resurser



Dokumentation av kritiska aktiviteter

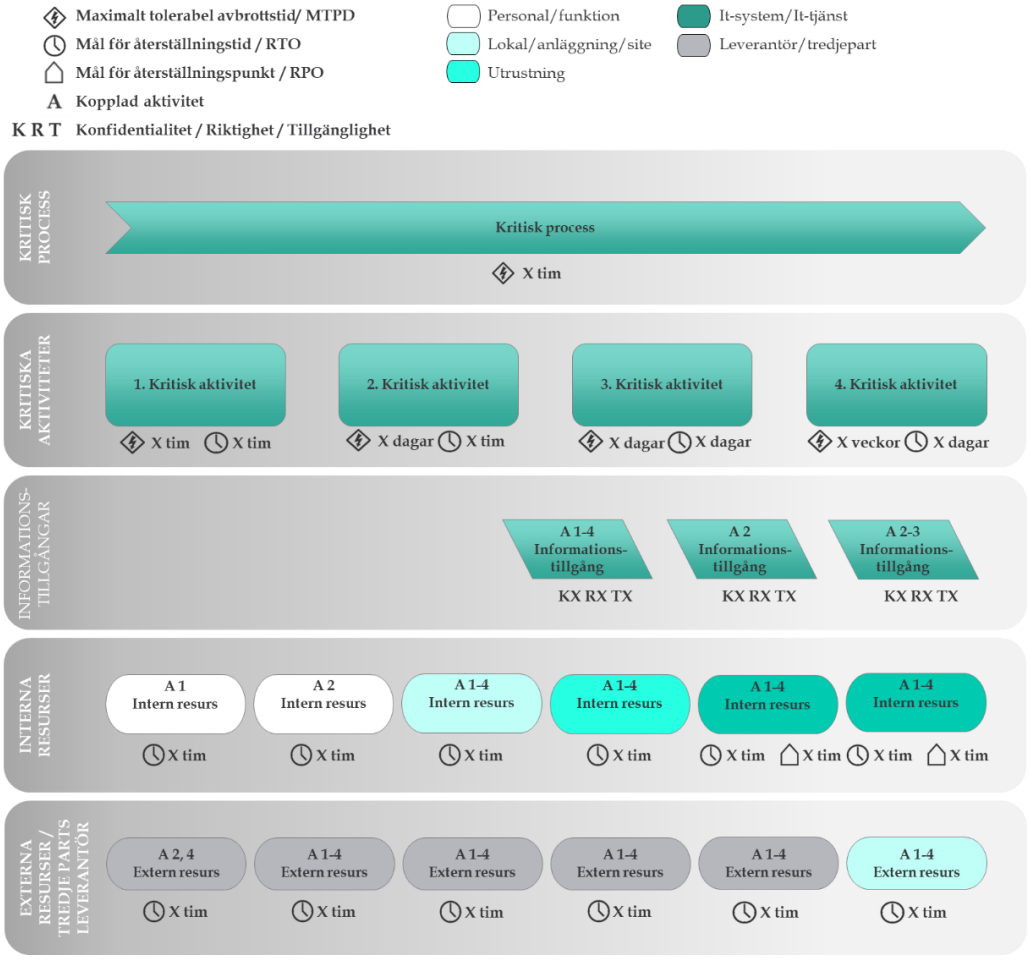
Kritisk aktivitet	Beskrivning	Ekonomisk påverkan	Påverkan på förtroende/ varumärke	Påverkan på verksamhetens funktionalitet	Maximalt tolerabel avbrottstid (MTPD) för aktiviteten	Motivering till satt maximalt tolerabel avbrottstid (MTPD) för aktiviteten	Mål för återställningstid (RTO) för aktiviteten	Motivering till satt mål för återställningstid (RTO) för aktiviteten	Kommentar
		Nivå	Nivå	Nivå	X timmar/dagar	Konsekvens-beskrivning utifrån bedömning av påverkan (kriteriemodellen)	X timmar/dagar	Krav på återställning utifrån satta tidskrav på aktiviteten	

Dokumentation av kritiska resurser

Kritisk resurs	Beskrivning	Typ av resurs	Resurskategori	Kopplad aktivitet/ aktiviteter	Mål för återställningstid (RTO) för resursen	Motivering till satt mål för återställnings-tid (RTO) för resursen	Mål för återställnings-punkt (RPO) för resursen (endast för it-system/it-tjänster)	Motivering till satt mål för återställnings-punkt (RPO) för resursen	Kommentar
		Intern/extern	Personal/funktion Lokal/anläggning/ site Utrustning It-system/It-tjänst Leverantör/tredjepart	Ange den/de aktiviteter som resursen stödjer	X timmar/dagar	Återställnings-beskrivning utifrån satta tidskrav	X timmar/dagar	Beskrivning av behov för återställning av information/data som används av en it-resurs utifrån satta tidskrav	

Konsekvensanalys – Informationsbärande resurser

Beroendekartläggning - visualisering av informationsbärande resurser och informationstillgångar



Dokumentation av informationsbärande resurser och informationstillgångar

Kritisk resurs	Beskrivning	Typ av resurs	Resurskategori	Kopplad aktivitet/ aktiviteter	Informations-tillgångar	Mål för återställningstid (RTO) för resursen	Motivering till satt mål för återställnings-tid (RTO) för resursen	Mål för återställnings-punkt (RPO) för resursen (endast för it-system/it-tjänster)	Motivering till satt mål för återställnings-punkt (RPO) för resursen	Kommentar
		Intern/extern	Personal/funktion Lokal/anläggning/ site Utrustning It-system/It-tjänst Leverantör/tredjepart	Ange den/de aktiviteter som resursen stödjer	Ange informations-tillgångar som den informations-bärande resursen hanterar och klassning	X timmar/dagar	Återställnings-beskrivning utifrån satta tidskrav	X timmar/dagar	Beskriv behovet av återställning för den information/data som används av it-resursen utifrån satta tidskrav	

Riskbedömning

Dokumentation av riskbedömning på aktivitetsnivå

Kritisk aktivitet - *Ange kritisk aktivitet* - *Ange aktivitetens maximalt tolerabel avbrottstid (MTPD)* - *Ange aktivitetens mål för återställningstid (RTO)*	**Risker som kan påverka tillgängligheten** - *Ange risker/händelser som påverkar tillgängligheten av aktiviteten*	**Nuvarande redundans (kontinuitetsstrategier/-lösningar)** - *Ange nuvarande redundans i form av hantering vid inträffad risk/händelse + alternativ(a) lösning(ar)*	**Kan fastställda tidskrav mötas vid en störning/ett avbrott** - *Sätt ett kryss i fälten för att ange* JA, KANSKE *eller* NEJ *på frågan om fastställda tidskrav kan mötas vid en störning/ett avbrott, givet nuvarande redundans (kontinuitetsstrategier/-lösningar)*			**Behov av kontinuitetsplan** - *Utifrån bedömd riskbild, ange om aktiviteten ska inkluderas i en kontinuitetsplan (JA/NEJ)* - *Om nej, ange skäl till varför aktiviteten inte ska inkluderas i en kontinuitetsplan*	**Behov av ytterligare redundans (kontinuitetsstrategier/-lösningar)** - *Ange om befintliga risker med nuvarande redundans kan accepteras eller om det finns behov av att vidtaga ytterligare åtgärder för att stärka redundansen för aktiviteten* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*
			JA	KANSKE	NEJ		

Dokumentation av riskbedömning på resursnivå

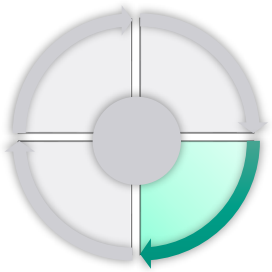
Kritisk resurs - *Ange kritisk resurs* - *Ange resursens mål för återställningstid (RTO)* - *Ange resursens mål för återställningspunkt (RPO) (gäller endast it-resurser)* - *Ange den/de aktiviteter resursen stödjer*	**Risker som kan påverka tillgängligheten** - *Ange risker/händelser som påverkar tillgängligheten av resursen*	**Nuvarande redundans (kontinuitetsstrategier/-lösningar)** - *Ange nuvarande redundans i form av hantering vid inträffad risk/händelse + alternativ(a) lösning(ar)*	**Kan fastställda tidskrav mötas vid en störning/ett avbrott** - *Sätt ett kryss i fälten för att ange* JA, KANSKE *eller* NEJ *på frågan om fastställda tidskrav kan mötas vid en störning/ett avbrott, givet nuvarande redundans (kontinuitetsstrategier/-lösningar)*			**Behov av kontinuitetsplan** - *Utifrån bedömd riskbild, ange om resursen ska inkluderas i en kontinuitetsplan (JA/NEJ)* - *Om nej, ange skäl till varför resursen inte ska inkluderas i en kontinuitetsplan*	**Behov av ytterligare redundans (kontinuitetsstrategier/-lösningar)** - *Ange om befintliga risker med nuvarande redundans kan accepteras eller om det finns behov av att vidtaga ytterligare åtgärder för att stärka redundansen för resursen* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*
			JA	KANSKE	NEJ		

Riskbedömning - Informationsbärande resurser

Dokumentation av riskbedömning för informationsbärande resurser och informationstillgångar

Kritisk resurs (endast informationsbärande resurser) - *Ange kritisk it-resurs* - *Ange it-resursens mål för återställningstid (RTO)* - *Ange it-resursens mål för återställningspunkt (RPO)* - *Ange den/de aktiviteter it-resursen stödjer* - *Ange de informationstillgångar som it-resursen hanterar och klassning*	**Risker som kan påverka tillgängligheten** - *Ange risker/luåndelser som påverkar tillgängligheten av it-resursen*	**Nuvarande redundans (kontinuitetsstrategier/-lösningar)** - *Ange nuvarande redundans i form av hantering vid inträffad risk/luåndelse + alternativ(a) lösning(ar)*	**Kan fastställda tidskrav mötas vid en störning/ett avbrott** - *Sätt ett kryss i fälten för att ange* JA, KANSKE *eller* NEJ *på frågan om fastställda tidskrav kan mötas vid en störning/ett avbrott, givet nuvarande redundans (kontinuitetsstrategier/-lösningar)*			**Behov av kontinuitetsplan** - *Utifrån bedömd riskbild, ange om it-resursen ska inkluderas i en kontinuitetsplan (JA/NEJ)* - *Om nej, ange skäl till varför it-resursen inte ska inkluderas i en kontinuitetsplan*	**Behov av ytterligare redundans (kontinuitetsstrategier/-lösningar)** - *Ange om befintliga risker med nuvarande redundans kan accepteras eller om det finns behov av att vidtaga ytterligare åtgärder för att stärka redundansen för it-resursen* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*	**Särskilda åtgärder för att bevara informationens skyddsvärden** - *Ange om det finns behov att vidtaga ytterligare åtgärder för att bevara informationstillgångarnas skyddsvärden utifrån (K)onfidentialitet, (R)iktighet, (T)illgänglighet* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*
			JA	KANSKE	NEJ			

Appendix C - Kontinuitetsstrategi



Kontinuitetsstrategier utgör gemensamma principer som möjliggör för organisationen att välja lämpliga sätt att förebygga och hantera hot mot prioriterade aktiviteter och resurser. Valda kontinuitetsstrategier ska säkerställa att prioriterade aktiviteter och resurser kan upprätthållas inom de uppsatta tidskraven.

Kontinuitetsstrategier sätts på en övergripande nivå och utgör en inriktning för vilka lösningar och åtgärder som ska implementeras. Strategierna bör formuleras på strategisk nivå och av de som har mandat att fatta beslut kring hur personella och finansiella resurser ska fördelas. De initiala strategierna kan komma att behöva revideras efter att mer detaljerade analyser av processer, aktiviteter och resurser har genomförts. Utformningen av strategierna kan även påverkas av de särskilda åtgärder som har beslutats i riskbedömningen för att bevara informationstillgångarnas skyddsvärden. Strategierna kan ta sikte på att hantera störningar före, under och/eller efter att de inträffar.

I slutet av detta appendix återfinns ett förslag på struktur för kontinuitetsstrategier.

C.1. Före en störning

Denna typ av strategier syftar till att förebygga och/eller minska sannolikheten för oönskade händelser. Strategierna kan inkludera att överföra risken till tredje part, till exempel genom outsourcing. I de flesta fall kvarstår dock ansvaret, och därmed vissa risker, för tjänsten hos den egna organisationen.

Förebyggande strategier kan också innebära diversifiering av verksamhetens kritiska processer genom att ha dem uppdelade på flera platser. På så sätt blir varje enskild plats inte lika kritisk och ett avbrott får därmed inte lika stora konsekvenser.

Strategierna kan också innebära beslut att avsluta eller ändra ursprungsgenomförandet av de kritiska aktiviteterna. Detta kan medföra ett beslut att inte erbjuda en viss tjänst eftersom den innebär alltför stora risker, alternativt förändra utförandet av tjänsten för att minska sannolikheten för att oönskade risker inträffar. Denna typ av strategi kan dock medföra nya risker, exempelvis i form av minskat förtroende, ökad arbetsbelastning för personal eller ökade kostnader för implementering av ny lösning.

C.2. Under en störning

Denna typ av strategier syftar till att skapa så små avbrott som möjligt i verksamheten under en störning. Det kan exempelvis handla om att tillfälligt flytta kritiska aktiviteter eller resurser till annan intern eller extern plats. Alternativa lokaler bör ligga geografiskt åtskilda från ordinarie lokaler.

Det måste också säkerställas att den utrustning som finns på alternativ plats snabbt kan sättas upp, att den fungerar och att personalen har kompetens att använda den. Ett annat exempel kan vara att skapa möjligheter för egen personal att arbeta hemifrån. I sådana fall bör det säkerställas att tillgång till kritiska it-system/kritisk information kan nås hemifrån.

Andra strategier kan vara att identifiera reservkapacitet, exempelvis i form av reservkraft, möjligheter att skala upp/ner vissa tjänster vid störningar i andra tjänster eller att göra omprioriteringar i verksamheten genom att skifta personal/resurser från mindre kritisk verksamhet till mer kritisk. Det kan också vara att säkerställa tillgång till kritiska personella och materiella resurser, genom att sprida kompetens på flera individer, skaffa en outsourcing-partner eller att lagerhålla kritiska resurser. Vid större och dyrare resurser är det inte alltid lönsamt att hålla lager. I sådana fall kan kontrakt med tredjepart eller att dela lager med andra vara alternativ.

Slutligen kan också strategier av denna typ innebära att arbeta enligt alternativa metoder under en begränsad tid. Vissa kritiska aktiviteter kan organisationen klara sig utan ett tag genom att arbeta på alternativa sätt som ger ungefär likvärdiga resultat. Detta fungerar oftast endast under begränsade perioder eftersom det sannolikt är mer tids- och personalkrävande. Ett exempel på detta är manuella rutiner vid störningar i it-system.

C.3. Efter en störning

Denna typ av strategier syftar till att minska konsekvenserna av en störning efter att den inträffat. Strategierna kan exempelvis innebära tecknande av försäkringar. Detta kan främst ge finansiell kompensation i samband med ökade kostnader/förluster vid en oönskad händelse. Försäkringar kan sällan täcka hela den ekonomiska förlusten och kan inte heller kompensera för andra typer av konsekvenser såsom minskat marknadsvärde eller tappat förtroende.

Strategierna kan också innebära upprättandet av en effektiv kommunikationsorganisation med målsättningen att kunna bemöta allmänhet och media och därmed minska negativ spridning av information om organisationen vid en störning.

C.4. Struktur för kontinuitetsstrategier

Ett sätt att besluta om vilka strategier som ska implementeras och hur dessa ska riktas kan vara att gruppera resurserna enligt deras mål för återställningstid, där de med kortast tidskrav är de mest kritiska. Strategierna ger på så vis en inriktning för processansvariga i arbetet med att utveckla konkreta kontinuitetslösningar i händelse av avbrott. Det ger också en tydligare bild över hur prioriteringen i framtagandet av kontinuitetsstrategier kan göras utifrån ställda kontinuitetskrav.

I exemplet nedan finns strategier riktade mot revidering av underlag samt krav på eskalering och rapportering. Utifrån denna strategi kan exempelvis beslut rörande investeringar och verksamhetsinriktning fattas.

Prioritering / Krav	4 Liten betydelse	3 Medelhög betydelse	2 Stor betydelse	1 Avgörande betydelse
Tidskrav för återställning samt definition	*> 5 dagar* *Återhämta när lämpligt*	*2-5 dagar* *Återhämta*	*2 -24 timmar* *Återhämta snarast*	*0 – 2 timmar* *Upprätthåll*
Krav på revision och test av kontinuitetsplan	• *Kontinuitetsplanen revideras och kritiska lösningar testas årligen*	• *Kontinuitetsplanen revideras och kritiska lösningar testas årligen*	• *Kontinuitetsplanen revideras och samtliga lösningar testas årligen*	• *Kontinuitetsplanen revideras och samtliga lösningar testas 2 ggr per år*
Krav på eskalering och rapportering vid avbrott	• *Eskalering till områdeschef* • *Utredning och rapportering av inträffat avbrott vid behov*	• *Eskalering till områdeschef* • *Utredning och rapportering av inträffat avbrott*	• *Eskalering till ledningsgrupp* • *Fullständig utredning och rapportering av inträffat avbrott*	• *Omedelbar eskalering till ledningsgrupp* • *Fullständig utredning och rapportering av inträffat avbrott*

Stöd för prioritering av kontinuitetsstrategier utifrån kontinuitetskrav.

C.5. Kostnad-nyttoanalys

Beslut om implementering av kontinuitetsstrategier kan medföra ökade kostnader för organisationen, till exempel vid av anskaffandet av redundant utrustning eller vid upprättandet av avtal med ytterligare leverantörer. Kostnaderna för att implementera strategier ökar i regel ju kortare mål för återställningstid resurserna har.

Kostnaderna måste vägas mot nyttan de förväntas innebära. Nyttan består till exempel i att ett systematiskt arbete med kontinuitetshantering gör det möjligt för organisationen att optimera sina investeringar i robusthet för den kritiska verksamheten. Vidare bidrar analysen av verksamheten till att redundans- och säkerhetsbrister kan identifieras för de kritiska processerna, aktiviteterna och resurserna. Analysen kan även identifiera resurser där redundansen är oproportionerligt hög jämfört med hur kritiska de är för verksamheten. Kontinuitetshantering möjliggör att insatser för ökad robusthet optimeras mot bakgrund av vad som är affärskritiskt för verksamheten.

För strategier som syftar till att minska sannolikheten för oönskade händelser kan nyttan beräknas genom att estimera minskningen i sannolikhet multiplicerat med konsekvenserna störningen förväntas ha i termer av kostnader. För strategier som syftar till att minska konsekvenserna kan nyttan beräknas på liknande sätt, genom att multiplicera minskningen av konsekvenser i termer av kostnader med sannolikheten för den oönskade händelsen. På dessa sätt kan ett ROI-värde (return on investment) beräknas, vilket ger ett bra beslutsunderlag för att prioritera identifierade kontinuitetsstrategier och -lösningar. När det gäller händelser som har en mycket låg sannolikhet bör ROI-värdet ses som ett sätt att jämföra alternativa lösningar med varandra, och inte tolkas bokstavligen. I kostnad-nyttoanalysen behöver också tidsaspekten beaktas, nämligen inom hur lång tid den implementerade strategin beräknas ha effekt jämfört med hur stor sannolikheten för en oönskad händelse är.

Exempel på struktur för kontinuitetsstrategi

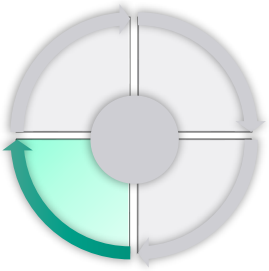
1. Introduktion
2. Strategier för personal/funktion
    a. Före
    b. Under
    c. Efter
3. Strategier för lokal/anläggning/site
    a. Före
    b. Under
    c. Efter
4. Strategier för utrustning
    a. Före
    b. Under
    c. Efter
5. Strategier för it-system/it-tjänst
    a. Före
    b. Under
    c. Efter
6. Strategier för leverantör/tredjepart
    a. Före
    b. Under
    c. Efter
7. Strategier för övriga resurser
    a. Före
    b. Under
    c. Efter

Prioritering av kontinuitetsstrategier utifrån kontinuitetskrav

Prioritering / Krav	4 Liten betydelse	3 Medelhög betydelse	2 Stor betydelse	1 Avgörande betydelse
Tidskrav för återställning samt definition				
Krav på revision och test av kontinuitetsplan				
Krav på eskalering och rapportering vid avbrott				
Krav på …				

Appendix D - Kontinuitetsplaner

Utifrån kontinuitetsstrategin och de tidigare stegen i kontinuitetsarbetet identifieras konkreta kontinuitetslösningar för respektive process. Lösningarna beskrivs sedan i en kontinuitetsplan. Kontinuitetslösningar kan tas fram för såväl processens kritiska aktiviteter som resurser. Viktigt är att de lösningar som beskrivs i dokumentet beskriver hur kritiska aktiviteter/resurser ska upprätthållas, hur resurser återställs vid störningar samt hur återgång till normalläge ska ske då aktiviteter/resurser åter fungerar normalt.



I kontinuitetsplanen beskrivs kontinuitetslösningar som ett antal checklistor med tydliga beskrivningar av roller, ansvar och befogenheter, samt nödvändiga kontaktuppgifter. Kontinuitetsplaner aktiveras vid behov för att kunna upprätthålla kritiska processer och möjliggöra för en snabb återgång till normal verksamhet. I slutet av detta appendix återfinns ett exempel på struktur för kontinuitetsplaner.

Format	• Kontinuitetsplaner utarbetas lämpligast i workshop-format • Utifrån resultatet från workshopen kan kompletterande information behöva inhämtas, exempelvis från andra befintliga planer eller specialistkompetens.
Deltagare	• Samma deltagare som vid workshop för konsekvensanalys och riskbedömning
Tidsåtgång	• En till två halvdagar per plan (beroende på antalet resurser samt deras komplexitet)
Slutprodukt	• En kontinuitetsplan med dokumenterade kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner

Hur mycket och vilken information som paketeras i en och samma plan baseras på vilka de tänkta användarna är. Det viktiga är att de tänkta användarna kan finna relevant information i planen. I de fall en kontinuitetsplan stöds av andra kontinuitetsplaner, inkludera hänvisningar. Vanligt är exempelvis att återställning av it-resurser beskrivs i separata återställningsplaner eller disaster recovery-planer.

Tips för genomförande:
- Tänk på att beskriva kontinuitetslösningarna så konkret som möjligt och med sådan detaljnivå att de lätt kan förstås av samtliga berörda
- Utse en person som är ansvarig för kontinuitetsplanen och därmed ansvarar för att uppdateringar görs, benämn gärna med funktion istället för namn

Nedan listas ett antal rubriker som kan ingå i en kontinuitetsplan:

- **Dokumentägare och rutin för uppdatering**
    - Varje kontinuitetsplan ska ha en dokumentägare som ansvarar för regelbunden uppdatering av planen enligt fastslagen rutin. Dokumentägaren säkerställer också spridning av planen till de som behöver ha tillgång till den, lagring av planen på lämplig plats och att den finns sparad både digitalt och analogt.
- **Kriterier och rutiner för aktivering**
    - I inledningen av planen ska det finnas beskrivet under vilka omständigheter planen ska aktiveras och hur detta ska ske.
- **Beskrivning av den process som omfattas av planen**
    - Den process som omfattas av planen bör beskrivas inledningsvis. Vilka prioriterade produkter och tjänster stöds av processen och vad avgränsar processen, d.v.s. var börjar och slutar processen? Vilka produkter och tjänster omfattar planen?
- **Beskrivning av kontinuitetslösningar för aktiviteter**
    - Kontinuitetslösningar kan utvecklas för processens aktiviteter baserat på de kontinuitetsstrategier som fastställts. Exempel på kontinuitetslösning på aktivitetsnivå är utbetalning på föregående månads underlag.
- **Beskrivning av kontinuitetslösningar för resurser**
    - För var och en av de kritiska resurserna beskrivs detaljerade kontinuitetslösningar. Kontinuitetslösningarna kan beskrivas i form av reservrutiner (*hur arbetar vi på alternativa sätt under ett avbrott?*), återställningsrutiner (*hur återställer vi den kritiska resursen efter ett avbrott?*) samt återgångsrutiner (*hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen?*).
    - Det är viktigt att kontinuitetslösningarna är specifika och detaljerade i beskrivningarna för att planen ska kunna användas operativt under en störning. Viss flexibilitet behövs dock för att kunna svara mot oväntade hot samt förändrade interna och externa förhållanden.
    - Det är viktigt att kontinuitetslösningarna även innefattar åtgärder för att upprätthålla informationstillgångarnas skyddsvärden utifrån krav på konfidentialitet, riktighet och tillgänglighet. Dessa åtgärder bör ha identifierats under riskbedömningen av informationsbärande resurser.
    - Kontinuitetslösningarna beskrivs lämpligtvis checklisteformat, i termer av *vad* som ska göras, *vem* som ska utföra detta, *hur* det ska genomföras och *när*. Lösningarna kan antingen grupperas enligt vilken typ av resurs de tillhör (som personella resurser, lokaler och utrustning, tekniska system och externa beroenden) eller enligt vilken process de tillhör (exempelvis spara, låna och betala eller skadereglering och återförsäkring).
- **Roller/uppgifter, ansvar och befogenheter.**
    - För var och en av kontinuitetslösningarna ska roll- och ansvarsfördelning beskrivas. Vem har mandat att åberopa åtgärder? Vem fattar beslut om att åtgärder ska genomföras? Vem utför åtgärderna?

- **Nödvändig kontaktinformation**
    - För respektive åtgärd behöver också nödvändig kontaktinformation anges.

Nedan redogörs ett exempel på kontinuitetslösning för den kritiska resursen huvudkontor. Exemplet innefattar kontinuitetslösningen att flytta delar av verksamheten till en reservplats. I kontinuitetsplanen beskrivs kontinuitetslösningen i form av en instruktion av hur flytten ska ske och om det är några specifika rutiner som gäller i nya lokalen (reservrutin), hur arbetet med att återställa den ordinarie lokalen hanteras (återställningsrutin) samt instruktion för återflytt till ordinarie lokaler (återgångsrutin). Enligt motsvarande struktur beskrivs även ett exempel på kontinuitetslösning för den kritiska resursen bärbar dator.

Kritisk resurs (Mål för återställningstid)	Kontinuitetslösningar
Huvudkontor (12 timmar)	Reservrutin: Flytt till reservlokal - VD beslutar om flytt - Respektive chef informerar sina medarbetare - VD kontaktar ansvarig för reservlokal och informerar om flytten - Rutinbeskrivning av hur flytten ska gå till och vilka särskilda rutiner som gäller för vistelsen på den nya platsen finns i bilaga 1 Återställningsrutin: - Kontakta hyresvärd och informera om problemet - Håll löpande kontakt med hyresvärd som informerar om status på återställningen av lokalerna - Informera anställda om när lokalerna beräknas vara tillgängliga Återgångsrutin: - VD beslutar om att flytta tillbaka till ordinarie lokal - Respektive chef informerar sina medarbetare - Rutinbeskrivning av hur flytten ska gå till och vilka särskilda aktiviteter som ska genomföras finns i bilaga 2 Nödvändiga kontaktuppgifter: - Ansvarig för reservlokal (se bilaga 3) - Hyresvärd (se bilaga 3)
Bärbar dator (12 timmar)	Reservrutin: Använd manuella rutiner - Prioritera arbetsuppgifterna. - Vid behov, stäm av prioritering med närmsta chef - Dokumentera genomförda transaktioner enligt manuella rutiner (se bilaga 2) - Ta nödvändiga kontakter via telefon istället för via mail (se bilaga 3) Återställningsrutin: - Kontakta hårdvaruleverantör som enligt avtal reparerar/levererar ny utrustning inom mål för återställningstid Återgångsrutin: - För in manuell dokumentation digitalt Nödvändiga kontaktuppgifter: - Viktiga intressenter (se bilaga 3) - Hårdvaruleverantör (se bilaga 3)

Exempel på kontinuitetslösningar.

Kontinuitetsplan för verksamheten

Denna kontinuitetsplan beskriver de reserv-, återställnings- och återgångsrutiner som används för att för att säkerställa kontinuiteten i Processen X, oavsett vad som inträffat. Kontinuitetsplanen tar sin utgångspunkt i regelbundet uppdaterade konsekvensanalyser och riskbedömningar.

Ansvarig för kontinuitetsplanen förvarar den elektroniskt samt papperskopia på lämplig plats för att säkerställa att den alltid finns tillgänglig.

Innehållsförteckning:

1. Dokumentinformation

Process:

Kritisk(a) period(er) för processen:

Ansvarig för kontinuitetsplanen:

Datum för senaste revidering:

Datum för senaste test/övning:

2. Användning och eskalering av kontinuitetsplanen

Kriterier för aktivering av plan:

Händelser då planen aktiveras omedelbart:

Kontaktpersoner vid aktivering:

3. Beskrivning av den process som planen innefattar

Process X: *Stödjer Produkt/tjänst Y*
Process X definieras enligt följande…/inkluderar följande aktiviteter…
/startar…/avslutas…

4. *Beskrivning av kontinuitetslösningar på aktivitetsnivå*

Aktivitet (maximalt tolerabel avbrottstid/mål för återställningstid)	**Kontinuitetslösningar**
Aktivitet X (MTPD/RTO)	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska aktiviteten är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

5. *Beskrivning av kontinuitetslösningar på resursnivå*

Resurskategori: Personal/funktion

Kritisk resurs (mål för återställningstid/ mål för återställningspunkt)	**Kontinuitetslösningar**
Resurs X (RTO)	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

Resurskategori: Lokal/anläggning/site

Kritisk resurs (mål för återställningstid)	Kontinuitetslösningar
Resurs X (RTO)	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

Resurskategori: It-system/it-tjänster

Kritisk resurs (mål för återställningstid)	Kontinuitetslösningar
Resurs X (RTO/RPO)	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

Resurskategori: Utrustning

Kritisk resurs (mål för återställningstid)	Kontinuitetslösningar
Resurs X (RTO)	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

Resurskategori: Leverantör/tredjepart

Kritisk resurs (mål för återställningstid)	Kontinuitetslösningar
Resurs X (RTO)	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

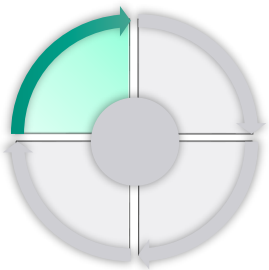
Resurskategori: Övriga resurser

Kritisk resurs (mål för återställningstid)	Kontinuitetslösningar
Resurs X (RTO)	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

6. Bilagor

- Kontaktlistor interna/externa kontakter
- Checklistor/beskrivningar för specifika åtgärder vid särskilda händelser
- Kopior på verksamhetskritiska avtal
- Logglista för att dokumentera händelseförlopp, fattade beslut och dess utfall.

Appendix E - Upprätthålla



Liksom med andra verksamhetsprocesser måste arbetet med kontinuitetshantering upprätthållas och förbättras. Detta kan exempelvis ske genom regelbunden granskning och revidering av styrande dokument, genomförda analyser och framtagna kontinuitetsplaner eller vid förändrade förutsättningar. Ett annat sätt att upprätthålla och förbättra kontinuitetsarbetet är genom utbildningar, övningar och tester för att öka förståelsen och förmågan i organisationen.

E.1. Granskning och revidering

Omvärlden och organisationer är i ständig förändring, det är därför av vikt att regelbundet granska och revidera kontinuitetsarbetet för att säkerställa att kontinuitetsstrategier, -lösningar och -planer är tillämpliga. Även vid större förändringar i verksamheten, såsom organisationsförändringar, införande av nya it-system eller byte av leverantörer, bör en revidering göras. En revidering av informationsklassning föranleder ofta till reviderad konsekvensanalys och riskbedömning. Utvärdering av inträffade incidenter kan också användas som underlag inför revidering. Tänk på att revideringar av exempelvis avgränsning eller inriktning för kontinuitetsarbetet innebär följdändringar.

Revision och granskning kan genomföras både av interna och externa parter. I policyn bör frekvens och ansvar för granskning och revidering fastställas. Det bör också vara tydligt definierat hur resultat från granskningar ska tillvaratas.

E.2. Övning och test

Utöver granskning och revidering är det viktigt att regelbundet öva och testa implementerade kontinuitetsplaner för att säkerställa att kontinuitetslösningarna är tillräckliga för att möta de tidskrav som satts upp.

Övning är en aktivitet för att träna, bedöma, tillämpa och utveckla organisationers förmåga och färdigheter. Övningar utgår från ett lärande och utbildande perspektiv, med fokus på att bygga upp en förmåga hos individer eller grupper snarare än att verifiera enskilda processer. Däremot kan en övning ha testande inslag. Test är en aktivitet för att bestämma helhet, kvalitet eller riktighet i det testade objektet. Den tydligaste skillnaden mellan övningar och tester är att tester innefattar moment av prövning och mätning, utifrån en förväntan om att det/de testade objekten antingen ska godkännas eller underkännas inom ramen för uppsatta mål och mätpunkter. Tester används för att verifiera en eller flera utpekade förmågor eller planer, exempelvis för att bedöma om befintlig förmåga är tillräcklig eller om framtagna kontinuitetsplaner fungerar som avsett.

Övningar kan bland annat syfta till att:

- **Öka medvetenhet och kompetens bland personalen**
  - *Är det rätt personal som är involverad – kompetens, förmåga, beslutsrätt?*
  - *Utveckla individers och gruppers förmåga.*
  - *Testa förmågor under press.*

Tester kan bland annat syfta till att:

- **Testa uppsatta tidskrav**
  - *Går tidskraven att möta?*
  - *Är befintliga logistik-/leverantörslösningar tillräckliga?*
  - *Är informationssäkerheten tillräcklig?*

Övning och test av kontinuitetslösningar kan exempelvis göras för manuella rutiner eller för flytt till reservlokal. Tester av kontinuitetslösningar gällande it-system kan göras på olika sätt, exempelvis kan ”fail over” (vilket innebär automatisk övergång till ett redundant it-system då ordinarie it-system är ur funktion) testas genom att stänga ner ordinarie it-system för att se om reservrutinen fungerar. Storleken på övningar eller tester kan variera, från enskilda mindre övningar eller tester till mer omfattande där delar av, eller hela organisationen deltar.

Beroende på organisationens vana av att arbeta med kontinuitetshantering samt tidigare erfarenheter av övning och test kan, och bör, komplexiteten i valet av övnings- eller testtyper anpassas. Skrivbordsövningar lämpar sig väl för organisationer med låg mognadsnivå, samt som ett bra komplement för mer mogna organisationer. Skrivbordsövningar kan även genomföras för nya eller uppdaterade planer eller rutiner. Under skrivbordsövningar diskuterar deltagarna planernas ändamålsenlighet utifrån ett eller flera scenarier som påverkar en eller flera planer samtidigt. Skrivbordsövningar har framförallt ett lärande syfte, där deltagarna i lugn och ro ges möjligheten att reflektera och diskutera utifrån olika scenarier. För mer erfarna deltagare kan simuleringar vara lämpliga. Dessa har ofta ett mer testande fokus där deltagarna agerar enligt de rutiner och instruktioner som finns. För mer information om genomförande av test av kontinuitetsplaner, se Appendix H - *Test av kontinuitetsplaner*.

Övning eller test kan genomföras för enskilda kontinuitetslösningar eller för flera kontinuitetslösningar parallellt. Dokumentationen kan vara i form av övningsrapporter eller testprotokoll. Resultaten från övningar och tester kan leda till revidering av kontinuitetsarbetet.

För att säkerställa relevanta övningar och tester bör en övnings- och teststrategi upprättas som tydligt visar hur organisationen över tid säkerställer förmåga att upprätthålla sina kritiska processer. Övnings- och teststrategi bör svara på vad organisationen vill uppnå och varför, hur organisationen ska nå dit, samt hur utvecklingen ska mätas. Övnings– och teststrategin bör inkluderas i den övergripande kontinuitetsstrategin.

Som komplement till den strategiska och långsiktiga övnings- och teststrategin bör en specifik övnings- och testplan tas fram. En övnings- och testplan bör visa hur respektive identifierad kritisk process löpande ska övas eller testas. I övnings- och testplanen dokumenteras förslagsvis övnings och testformat, förmågeområden, prioritering och målgrupp. Omfattning och frekvens av övningar och tester bör kopplas till hur kritisk en process eller resurs är för verksamheten. Genom att kontinuitetslösningar för de mest kritiska resurserna testas och övas mer frekvent och omfattande än de mindre kritiska, kan resurserna optimeras.

Finansinspektionen reglerar test av kontinuitetsplaner genom Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4) samt Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1). Enligt föreskrifterna ska berörda aktörer, minst årligen, uppdatera och testa sina kontinuitetsplaner så att de är anpassade för verksamheten och dess förutsättningar.

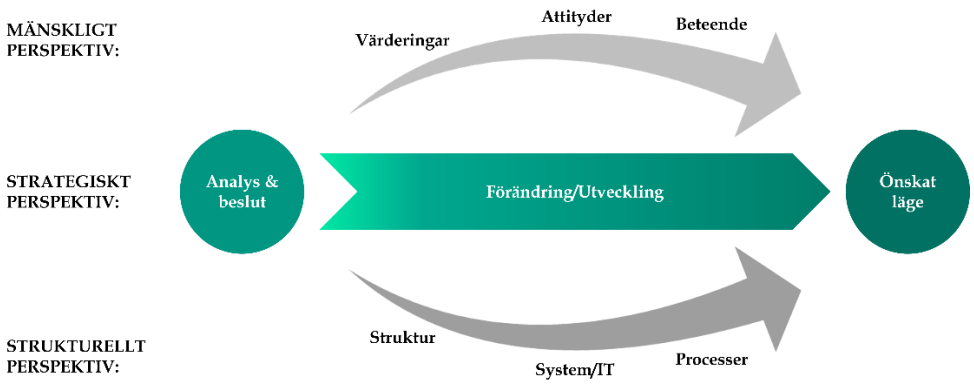
E.3. Utbildning

Utbildningar är en viktig del av implementeringen av kontinuitetshantering inom organisationen. Utbildningar bör genomföras för olika nivåer av organisationen och med olika syften. För vissa delar av organisationen räcker det med kortare utbildning i syfte att informera om att ett kontinuitetsarbete har inletts och hur det kommer att påverka utbildningsdeltagarna i deras dagliga arbete. För andra, exempelvis för de som ska arbeta aktivt i och ha ett ansvar för kontinuitetshanteringsprocessen, behövs djupgående utbildningar som syftar till att förklara metoder och tillvägagångssätt.

E.4. Kultur för kontinuitetshantering

Utbildning, övning och test är av stor betydelse för att skapa en organisationskultur som främjar kontinuitetshantering. I en sådan kultur är medvetenhet om kontinuitetshanteringen och dess arbetssätt känt i organisationen, ansvaret är tydligt fördelat och ledningen har belyst vikten av kontinuitetsarbetet och tilldelat tillräckliga resurser. Vidare är kontinuitetshanteringen integrerad i alla delar av verksamheten och utförs inte som en separat process vid sidan av övriga.

För att uppnå en kontinuitetshanteringskultur krävs, som vid förändringar av alla slag i en organisation, att olika perspektiv beaktas.



Det strategiska perspektivet inkluderar att ledningen fattar beslut om önskat läge och tar fram tidplaner samt utser ansvariga för att nå dit. Det strukturella perspektivet innebär att ta fram system, processer och annat stöd, exempelvis mallar och checklistor, som underlättar arbetet med att nå önskat läge. Det mänskliga perspektivet är också viktigt i förändringsprocesser, men glöms ofta bort. Förståelse bland medarbetare och andra intressenter kring varför och hur förändringen ska genomföras och hur den kan vara värdeskapande är därmed viktig.

Förändring bygger på en insiktsfull integration av de tre perspektiven, där alla är viktiga för en effektiv implementering i organisationen. I ett kontinuitetsperspektiv kan det strategiska perspektivet beaktas i exempelvis policyn, där arbetets omfattning och resurstilldelning anges. Det strukturella perspektivet kan beaktas genom framtagande av checklistor och mallar för de olika stegen i kontinuitetsarbetet eller inköp av it-system som ska stödja arbetet. Det mänskliga perspektivet tillgodoses genom att medvetandegöra anställda och andra intressenter om arbetet och de fördelar det för med sig genom exempelvis utbildningar och övningar.

Appendix F - Kontinuitetshantering för it-verksamheten

För aktörer i den finansiella sektorn får avbrott i it-tjänster stora konsekvenser för verksamheten, vilket i förlängningen leder till konsekvenser för kunderna. It-verksamheten är därför en viktig stödfunktion, oavsett om den är intern eller outsourcad till tredje part, och det är viktigt att säkerställa robusthet i denna. Detta kan med fördel göras genom ett strukturerat arbete med kontinuitetshantering.

Kontinuitetshantering handlar om att skapa redundans vilket it-verksamheten vanligtvis både identifierat och arbetar intensivt med. Detta genom exempelvis back-up, spegling av viktig information och systematiserad incidentrapportering och -hantering. Även om it-verksamheten vanligtvis arbetar med att skapa redundans för kritiska system/data etc. kan ett mer systematiskt kontinuitetshanteringsarbete ge stora fördelar, exempelvis i form av effektivitetsvinster eller identifiering av brister i befintliga redundanslösningar.

Genom den övergripande verksamhetens kontinuitetshanteringsarbete har organisationens mest kritiska verksamhetsprocesser, aktiviteter och resurser kartlagts samt att tidskrav i form av maximalt tolerabel avbrottstid och mål för återställningstid[47] har definierats. Mål för återställningstiderna för resurser med koppling till it-verksamheten utgör ett viktigt ingångsvärde för it-verksamhetens arbete med kontinuitetshantering. På så sätt utgör kontinuitetsarbetet inom it-verksamheten en förlängning av kontinuitetsarbetet för verksamheten.

Den process för kontinuitetshantering som presenteras i detta appendix följer processen som presenteras i standarderna ISO 22301[48] om ledningssystem för kontinuitetshantering och ISO 27031[49] om kontinuitetshantering för it-verksamhet. Processtegen är således de samma som de processteg som presenteras i vägledningens huvuddokument, med skillnaden att detta appendix ger fördjupad vägledning specifikt för it-verksamheten genom samtliga processteg. Även det processorienterade ramverket IT Infrastructure Library (ITIL) som ger vägledning för styrning och leverans av it-tjänster ger ingångsvärden för hur företag och organisationer kan arbeta med kontinuitet beträffande leverans av it-tjänster.

För att säkerställa att innehållet ligger i linje med de önskemål och behov som finns i den finansiella sektorn har ett antal intervjuer med kontinuitetsansvariga hos olika typer av finansiella aktörer genomförts inför författandet av detta appendix.

---

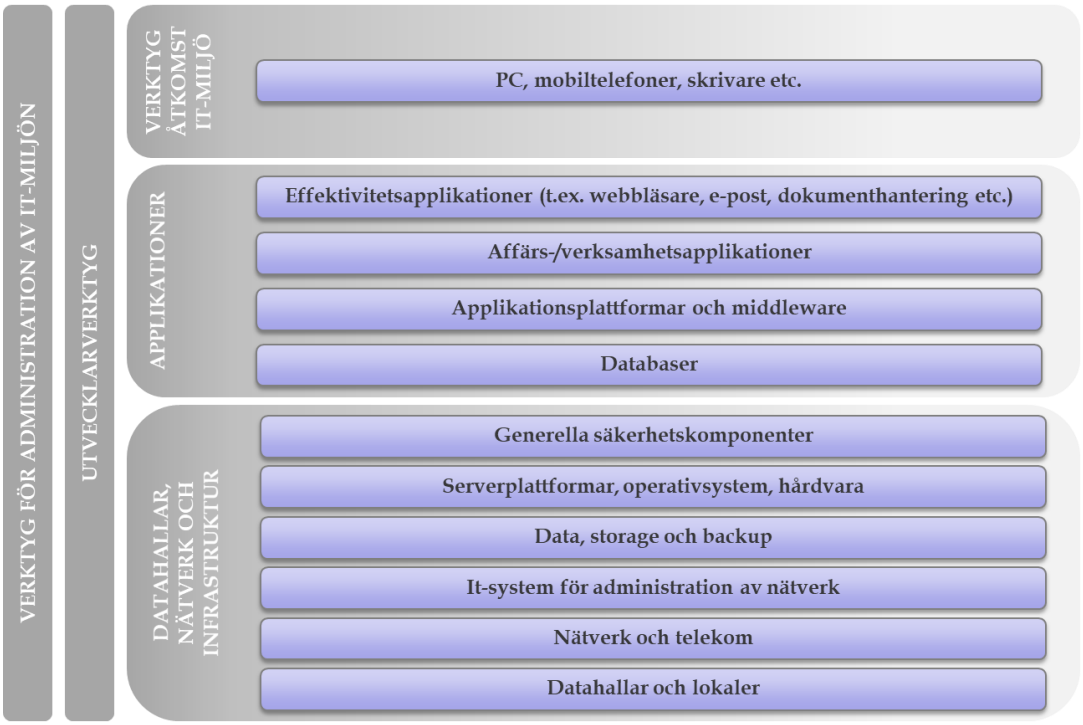
[47] *RTO - Recovery Time Objective (ISO 22313).*

[48] *SS-EN ISO 22301 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Krav.*

[49] *ISO/IEC 27031 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.*

F.1. Beskrivning av it-miljön

Innan första steget i kontinuitetsprocessen inleds kan it-verksamheten göra en kartläggning av it-miljön och beskriva hur den är strukturerad. Kartläggningen ger kunskap och samsyn om it-miljöns uppbyggnad och kan sedan användas som checklista för att säkerställa att inget förbises i genomförandet av konsekvensanalysen. I figuren nedan visas ett exempel på hur it-miljön kan beskrivas.



F.2. Analys av it-verksamheten

Kontinuitetsarbetet inom it genomförs i huvudsak på samma sätt som för den övergripande verksamheten. Skillnaden är som ett första steg i analysen för it-verksamheten, att aggregera de resurser som identifierats av den övergripande verksamheten istället för att identifiera kritiska processer. Analys av it-verksamheten genomförs enligt nedanstående figur.

Aggregering av resurser identifierade av verksamheten

Som ovan nämnts utgör de it-resurser som identifierats av verksamheten ingångsvärden för it-verksamhetens kontinuitetsarbete. Därför bör it-verksamheten inventera och aggregera samtliga resurser som identifierats av verksamheten och har koppling till it-verksamheten. För att säkerställa att ingen information förbises är det viktigt att för var och en av resurserna anges vilken/vilka verksamhetskritiska processer den stödjer och därmed vad dess mål för återställningstid baseras på.

Beroende på omfattningen av it-resurser som identifierats av verksamheten kan det krävas en gruppering för att underlätta och effektivisera arbetet med konsekvensanalysen. Det viktigaste är att säkerställa att samtliga it-relaterade resurser finns med, grupperingen kan sedan göras på lämpligt sätt. Ett exempel är att gruppera resurser baserat på vilka plattformar de ingår i, ett annat är att gruppera resurser som är likartade och därmed har många gemensamma underliggande beroenden.

Konsekvensanalys

Konsekvensanalysen syftar till att identifiera vilka underliggande it-resurser som behövs för att de resurser som verksamheten tidigare identifierat ska kunna fungera. I konsekvensanalysen definieras även mål för återställningstider och återhämtningspunkter[50] för de identifierade underliggande it-resurserna.[51]

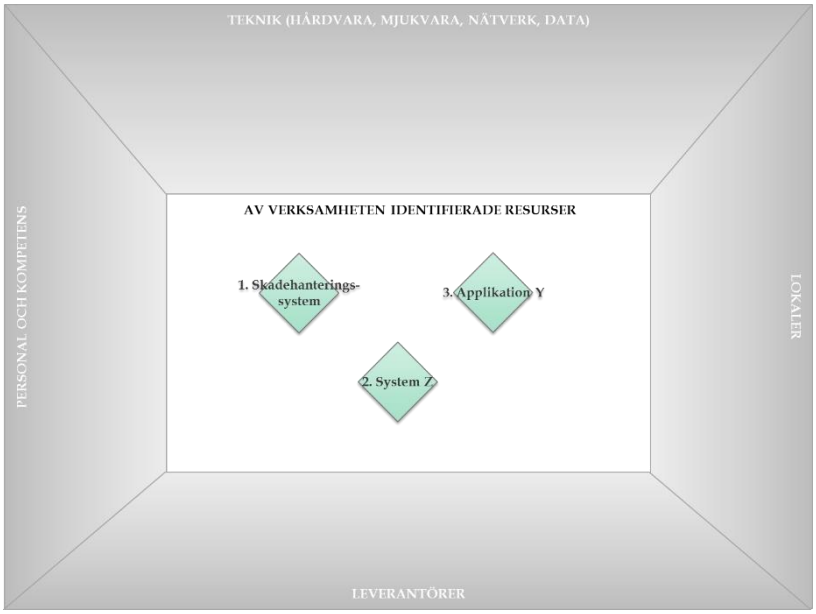
Konsekvensanalysen inleds med att numrera de resurser som verksamheten identifierat, om en gruppering gjorts kan numrering göras för varje grupp av resurser.

Konsekvensanalysen dokumenteras i en karta, beroende på omfattningen kan det göras en karta för hela it-verksamheten eller så görs en karta för varje grupp av resurser (enligt gruppering i föregående steg). I figuren nedan visas ett exempel på hur en karta kan se ut.

---

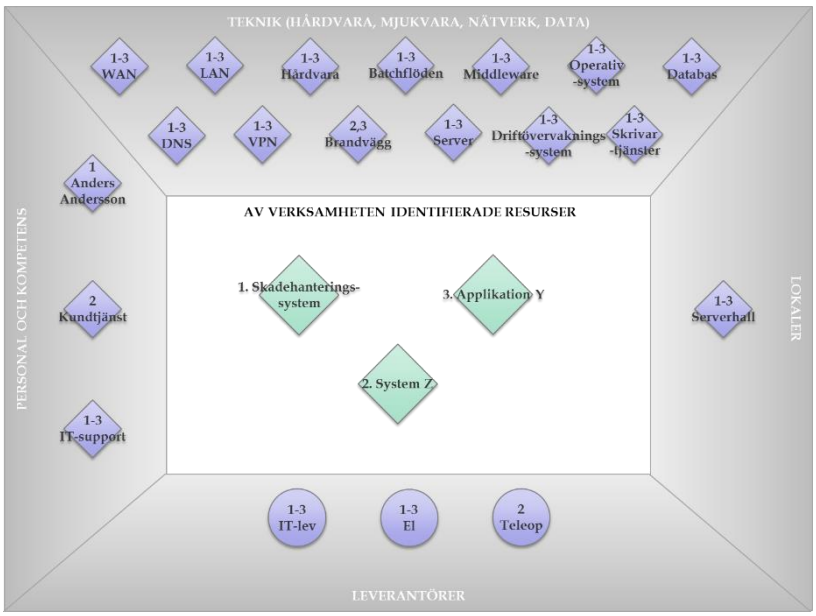
[50] *SS-EN ISO 22313 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Vägledning för implementering av ISO 22301. Mål för återställningspunkt RPO - Recovery Point Objective (ISO 22313).*

[51] *Konsekvensanalys kan också göras för it-verksamhetens tidskritiska processer, såsom exempelvis incidenthantering, i syfte att identifiera och analysera kritiska beroenden för dessa processer.*

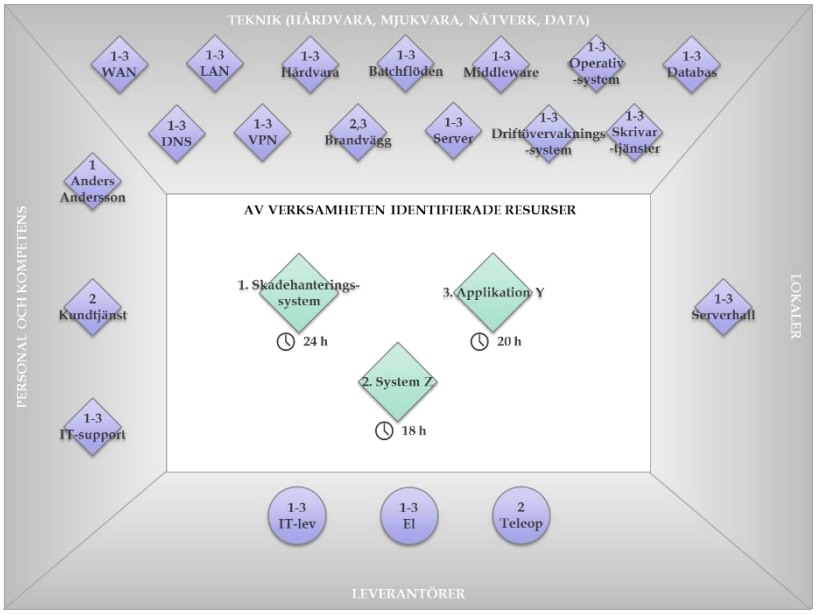


Analysen görs sedan genom att i tur och ordning gå igenom de resurser som verksamheten identifierat och identifiera beroenden till underliggande it-resurser. För att dokumentera vilka underliggande it-resurser som behövs för en resurs identifierad av verksamheten markeras de underliggande it-resurserna med det nummer som den aktuella resursen har. Det är viktigt att analysera underliggande beroenden i flera steg, för att säkerställa att samtliga it-resurser identifieras. Beroenden mellan underliggande it-resurser kan anges genom att rita pilar i kartan.

För att få struktur i identifieringen kan de underliggande it-resurserna kategoriseras utifrån kategorier som; personal och kompetens, lokaler, teknik och leverantörer. Om en beskrivning av it-miljön har tagits fram kan den användas som checklista för att säkerställa att alla viktiga beroenden har identifierats. Inom it-verksamheten finns ofta ett starkt nyckelpersonsberoende som är viktigt att fånga upp i konsekvensanalysen, använd gärna befintliga analyser t.ex. pandemiplanering. Nedan visas ett exempel på en karta där de underliggande it-resurser är identifierade.

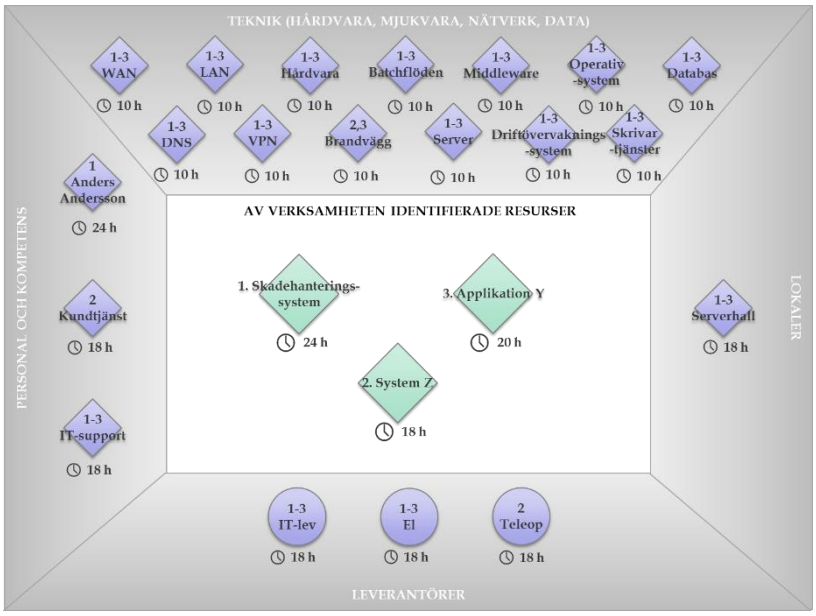


När underliggande beroenden till it-resurser har identifierats för samtliga resurser som verksamheten identifierat är nästa steg att fastställa mål för återställningstid för it-resurserna. Utgångspunkten för tidskraven är de tillgänglighetskrav som verksamheten har definierat för de identifierade resurserna. Nedan visas ett exempel på en karta med verksamhetens tillgänglighetskrav på de identifierade resurserna.



Mål för återställningstid för it-resurserna fastställs sedan genom att ta en it-resurs i taget och notera vilka av de av verksamheten identifierade resurserna som den stödjer, det lägsta tillgänglighetskravet styr vilket mål för återställningstid it-resursen får. Mål för återställningstid för it-resurserna måste sättas med en säkerhetsmarginal i förhållande till tillgänglighetskravet på den av verksamheten identifierade resursen.

När det finns beroenden mellan underliggande it-resurser är det även viktigt att beakta hela beroendekedjan inför fastställande av mål för återställningstid. I de fall där it-resursen har att göra med lagring av data är det också relevant att definiera krav på återhämtningspunkt (RPO) vilket innebär krav på hur gammal data maximalt får vara för att medge funktionalitet i den kritiska resursen från verksamheten. Nedan visas ett exempel på en karta där samtliga tidskrav finns dokumenterade, notera särskilt att mål för återställningstid för de underliggande tekniska resurserna har definierats kortare än tidskravet på de av verksamheten identifierade resurserna.



Att de tillgänglighetskrav verksamheten ställt används som utgångspunkt vid definiering av mål för återställningstider för it-verksamhetens kritiska resurser är viktigt dels för att uppnå tillförlitliga återställningsplaner och dels för att säkerställa att kriterier och rutiner för en specifik resurs är gemensamma inom hela organisationen. Det kan även vara bra att utvärdera om ställda tillgänglighetskrav är möjliga att möta utifrån it-verksamhetens perspektiv. Om inte bör detta kommuniceras till verksamheten som får utarbeta andra redundanslösningar.

Riskbedömning

Precis som för organisationens verksamhetsprocesser avslutas steget konsekvensanalys med att göra en riskbedömning. Riskbedömningen har till uppgift att bedöma respektive resurs befintliga redundans i relation till definierade mål för återställningstider. I de fall där förmågan anses bristfällig eller där redundansen inte lever upp till ställda krav bör åtgärder identifieras för att minska sannolikheten för att något inträffar som påverkar resursen alternativt minskar konsekvenserna om något ändå inträffar. Sådana åtgärder kan bland annat beröra personal, lokaler, tekniska komponenter eller externa leverantörer/tjänster.

Metoden för att genomföra riskbedömningen är densamma för it-verksamheten som för den övergripande verksamheten. I figuren nedan visas ett exempel på riskbedömning för informationsbärande resurser och informationstillgångar.

Kritisk resurs (endast informationsbärande resurser) - *Ange kritisk it-resurs* - *Ange it-resursens mål för återställningstid (RTO)* - *Ange it-resursens mål för återställningspunkt (RPO)* - *Ange den/de aktiviteter it-resursen stödjer* - *Ange de informationstillgångar som it-resursen hanterar och klassning*	**Risker som kan påverka tillgängligheten** - *Ange risker/händelser som påverkar tillgängligheten av it-resursen*	**Nuvarande redundans (kontinuitetsstrategier/-lösningar)** - *Ange nuvarande redundans i form av hantering vid inträffad risk/händelse + alternativ(a) lösning(ar)*	**Kan fastställda tidskrav mötas vid en störning/ett avbrott** - *Sätt ett kryss i fälten för att ange* JA, KANSKE *eller* NEJ *på frågan om fastställda tidskrav kan mötas vid en störning/ett avbrott, givet nuvarande redundans (kontinuitetsstrategier/-lösningar)*			**Behov av kontinuitetsplan** - *Utifrån bedömd riskbild, ange om it-resursen ska inkluderas i en kontinuitetsplan (JA/NEJ)* - *Om nej, ange skäl till varför it-resursen inte ska inkluderas i en kontinuitetsplan*	**Behov av ytterligare redundans (kontinuitetsstrategier/-lösningar)** - *Ange om befintliga risker med nuvarande redundans kan accepteras eller om det finns behov av att vidtaga ytterligare åtgärder för att stärka redundansen för it-resursen* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*	**Särskilda åtgärder för att bevara informationens skyddsvärden** - *Ange om det finns behov att vidtaga ytterligare åtgärder för att bevara informationstillgångarnas skyddsvärden utifrån (K)onfidentialitet, (R)iktighet, (T)illgänglighet* - *Utse ansvarig* - *Sätt en deadline för när åtgärden ska vara genomförd*
			JA	KANSKE	NEJ			
Skadehanteringssystem - *12 timmar (RTO)* - *8 timmar (RPO)* - *Mottagande av skadeanmälan, Skadereglering och information återförsäkrare, Utbetalning, Uppföljning* - *Skadeanmälan K2 R2 I3, Skadereglering K2 R2 T3*	Elavbrott	Finns reservkraft samt diesel för 3 dagars drift.	X			*JA*	Löpande test av reservkraft - *Ansvar: kontorschef* - *Deadline: ÅÅÅÅ-MM-DD*	Säkerställ att informationen är opåverkad om reservkraften inte längre fungerar - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD* Säkerställ rutiner för informationssäkerhet vid manuell skadereglering - *Ansvar: chef för skadereglering* - *Deadline: ÅÅÅÅ-MM-DD*
	Internet ligger nere	Kontakta IT-leverantör. Ingen alternativ internetförbindelse finns.			X	*JA*	Utred möjliga redundanslösningar - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD*	Säkerställ att informationen är opåverkad under hela avbrottet - *Ansvar: IT-chef* - *Deadline: innan årsskiftet* Säkerställ rutiner för informationssäkerhet vid arbete hemifrån - *Ansvar: chef för skadereglering* - *Deadline: ÅÅÅÅ-MM-DD*
	Skadlig kod	Anti-virusprogram finns, oklart om tillräckligt		X		*JA*	Se över befintlig redundanslösning - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD*	Säkerställ att isolerade backuper finns för att skydda mot förstörelse av ursprungliga data, samt att informationens skyddsvärden bevaras under hela återställnings-förfarandet från backup - *Ansvar: IT-chef* - *Deadline: ÅÅÅÅ-MM-DD*

F.3. Kontinuitetsstrategi för it-verksamheten

Liksom för övriga delar av verksamheten kan och bör kontinuitetsstrategier upprättas för it-verksamheten. De strategier som formuleras på it-nivå ska syfta till att möjliggöra för de kritiska it-resurserna att möta de tidskrav som identifierats av den övergripande verksamheten. Utformningen av strategier baseras på de krav som verksamheten, efter genomförd konsekvensanalys, ställt på de identifierade it-relaterade resurserna.

En tät dialog mellan övergripande verksamhet och it-verksamheten underlättar detta arbete. Kontinuitetsstrategierna för it-verksamheten kan även formuleras i samma dokument som kontinuitetsstrategierna för övriga verksamheten.

Vid val av vilka strategier som ska implementeras måste tillgängliga resurser analyseras och eventuella glapp mellan målsättningar och möjligheter att nå dem måste meddelas till högsta ledning för beslut om eventuella investeringar i ytterligare redundanslösningar. En kostnad-nyttoanalys bör göras som ett steg i att hitta de mest kostnadseffektiva lösningarna. Vanliga begränsningar för implementering av identifierade strategier är exempelvis:

1. budget
2. tillgång till resurser
3. tekniska begränsningar
4. organisationens riskbenägenhet
5. regleringar och lagar

Kontinuitetsstrategierna för it-verksamheten kan till exempel vara riktade mot:

- Personal och kompetens: exempelvis spridning av kunskaper genom att dokumentera hur kritiska ICT-tjänster genomförs eller användandet av multikompetent personal.
- Lokaler: exempelvis alternativa lokaler. I dessa fall är det viktigt att beakta säkerheten på den alternativa platsen, vilka som har tillträde etc.
- Teknik: exempelvis antal platser med teknisk utrustning, digital tillgång till dessa platser, redundanslösningar för el- och telekommunikationsförsörjning.
- Data: exempelvis hur ofta backup ska genomföras samt hur lagring och förmedling av data ska ske.
- Leverantörer: exempelvis lagring av redundant utrustning hos partner, kontrakt som möjliggör korta leveranstider vid störningar eller redundanslösningar gällande el och telekommunikationer.

Beslut om vilka strategier som ska användas bör ske på högsta ledningsnivå och som stöd kan, liksom för de övergripande kontinuitetsstrategierna, exempelvis en tabell enligt nedan användas. I denna anges olika strategier baserat på hur kritiska de olika resurserna är.

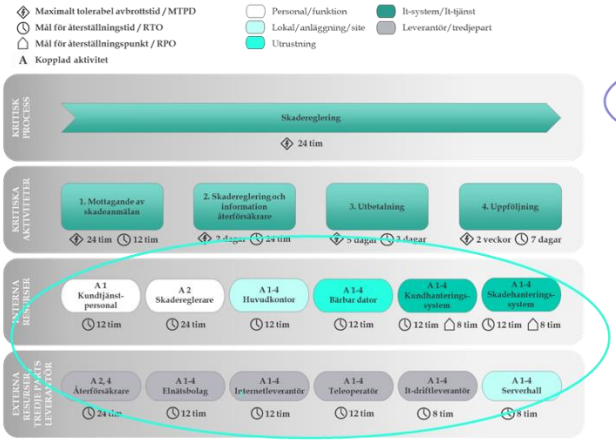
PRIORITERING / KRAV	GULD Avgörande betydelse	SILVER Stor betydelse	BRONS Mindre betydelse
Mål för återställningstid	*< 2 timmar*	*2-24 timmar*	*>24 timmar*
Övergripande strategi	*Upprätthåll alltid*	*Återställ idag*	*Återställ*
Driftställen	*Geografiskt separerade hallar*	*Geografiskt separerade hallar*	*Ett driftställe*
Lagring	*Synkron spegling*	*Asynkron spegling*	*Verifieras per IT resurs*
Krav på återhämtningspunkt	*2 timmar*	*8 timmar*	*24 timmar*
Backup	*2 ggr/timme**	*1 ggr/dygn*	*1 ggr/vecka*
Jour	*Ja, svar inom 5 minuter 24/7/365*	*Ja, svar inom 1-2h 24/7/365*	*Nej*
Krav på revision och test av återställningsplaner	*•Återställningsplan revideras och samtliga lösningar testas minst årligen eller vid större förändringar i IT-miljön*	*•Återställningsplan revideras och samtliga lösningar testas minst årligen*	*•Återställningsplan revideras årligen •Test av återställningsplan vid större förändringar*
Krav på eskalering och rapportering vid avbrott	*•Omedelbar eskalering till central krisledning •Fullständig utredning och rapportering av inträffat avbrott*	*•Eskalering till central krisledning •Fullständig utredning och rapportering av inträffat avbrott*	*•Eskalering till IT:s krisledning •Utredning och rapportering av inträffat avbrott*

* *Om krav på återhämtningspunkt är kortare än back-up frekvensen krävs tillgång till transaktionslogg, snapshot eller motsvarande.*

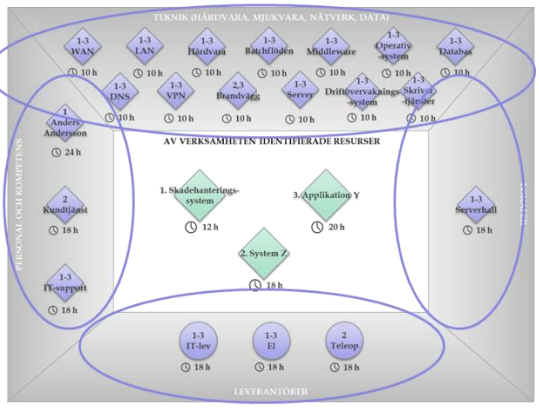
F.4. Återställningsplaner

Inom it-verksamheten används begreppet återställningsplaner[52] istället för kontinuitetsplaner, men arbetsprocessen för upprättandet är densamma som för kontinuitetsplaner för verksamheten. Återställningsplaner ska upprättas för de it-resurser som identifierats i konsekvensanalysen.

Återställningsplanerna har till uppgift att skapa en beredskap och förmåga att hantera oönskade händelser. Tidskraven baseras på den konsekvensanalys som gjorts av it-verksamheten vilka i sin tur baseras på de krav som fastställts av den övergripande verksamheten.



Fokus i kontinuitetsplaner för verksamheten



Fokus i återställningsplaner för it-verksamheten

I återställningsplanerna beskrivs konkreta och tydliga kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner för var och en av de identifierade kritiska it-resurserna. Det är också viktigt att beskriva beroenden mellan olika it-resurser för att säkerställa återställning genom hela beroendekedjan.

En mindre organisation kan välja att ha en samlad plan som innehåller alla kontinuitetslösningar som krävs för att upprätthålla och återställa kritiska resurser i it-verksamheten vid störningar. En stor organisation kan istället välja att dokumentera kontinuitetslösningarna i flera olika planer, där planerna exempelvis delas upp enligt den gruppering av resurser som tidigare genomförts. Det är också viktigt att planen/planerna finns lättillgängliga för samtliga som kan tänkas komma att ha behov av dem för att upprätthålla och återställa resurser vid en störning.

Enligt ISO 27031 bör återställningsplaner för it-verksamheten innehålla information om syfte och mål, ansvar och roller, kriterier för aktivering av planen, dokumentägare och rutiner för uppdatering, kontaktlistor samt detaljerade beskrivningar av reserv-, återställnings- och återgångsrutiner. Detta innehåll korrelerar väl med de kontinuitetsplaner som upprättas för övriga delar av verksamheten[53].

---

[52] *Andra vanliga benämningar är disaster recovery-, back-up- eller återhämtningsplaner.*

[53] *ISO/IEC 27031 - Guidelines for information and communication technology readiness for business continuity.*

Hantering av störningar och incidenter är alltid förenat med viss osäkerhet. Det är därför viktigt att fastställa tydliga riktlinjer för eskalering inom it-verksamheten. Detta föreskrivs även i ISO 27031. Riktlinjerna består dels i ansvar och rollfördelningar och i tydliga kriterier.
Vad gäller eskalering bör riktmärket vara att aktivera planerna för tidigt snarare än för sent. Nedanstående tabell presenterar ett exempel på fastställda kriterier för bedömning av hur allvarlig en incident är, exempelvis genom bedömningsskalan grönt, gult och rött.

	GRÖNT	GULT	RÖTT
Oplanerat driftstopp	• *Oplanerat driftsstopp i tidskritiska tjänster som bedöms kunna vara upp till 1 timmar och som påverkar hela eller delar av verksamheten.*	• *Oplanerat driftsstopp som bedöms kunna vara längre än 1 timmar och som påverkar hela eller delar av verksamheten och även påverkar slutkund.*	• *Oplanerat driftsstopp som fastställt kommer att pågå under minst 3 timmar och som påverkar hela eller delar av verksamheten och slutkund.* • *Om liv är i fara*
Åtgärder	• *Felsök enligt felsökningsrutin och återställ enligt plan*	• *Felsök enligt felsökningsrutin och återställ enligt plan* • *Rekommendation till ledningen att höja beredskapen inom organisationen pga. förhöjd risk.* • *Vid avhjälpt fel utreds och utvärderas händelsen*	• *Kris deklareras och krisledningen tar över ansvaret* • *Felsök enligt felsökningsrutin och återställ enligt plan* • *Vid avhjälpt fel utreds och utvärderas händelsen*

F.5. Upprätthålla

Övervaka, upptäcka och analysera hot

Vid planering för it-kontinuitet är det vanligt att man utgår från scenarioplanering, där exempel på scenarier kan vara logiska fel, hårdvarufel, pandemi och växla till alternativ anläggning för it-drift.

Organisationen bör upprätta en process för att löpande övervaka och upptäcka hot, exempelvis inom nedanstående, men inte uteslutande dessa, områden:

1. Personalomsättning, kunskaper och kompetens
2. Lokaler i vilka det finns it-utrustning
3. Förändringar i it-miljön
4. Budget
5. Externa tjänster och leverantörer
6. Tekniska sårbarheter

Granskning och revidering

För att på ett strukturerat och enkelt sätt kunna följa upp effektiviteten i kontinuitetsarbetet kan kriterier definieras. Dessa kriterier kan vara både kvantitativa och kvalitativa och mätas med hjälp av ”key performance indicators” (KPI:er). Kvantitativa kriterier kan inkludera exempelvis antalet incidenter som inte upptäckts innan en störning inträffat eller den tid det tar innan en incident upptäcks alternativt åtgärdas. Kvalitativa kriterier kan mätas genom exempelvis enkäter eller genom återkoppling från användare eller intressenter.

Ett annat lämpligt sätt att säkerställa att arbetet med kontinuitetshantering i it-verksamheten når uppsatta mål och ligger i linje med framtagen strategi är att genomföra intern granskning. En plan kan ange kriterier, omfattning, metod och frekvens för dessa uppdateringar. I planen ska också outsourcingpartners inkluderas. Vidare ska granskningar ske då större förändringar skett i it-verksamheten, vilka kan påverka de återställningsrutiner som finns för kritiska resurser. Resultaten från granskningar ska dokumenteras och kommuniceras till högsta ledningen.

Kontinuitetsplaner ska inte vara fristående från den dagliga verksamheten. Årsprocessen för planering av it-kontinuitet bör vara tydligt kopplade till den dagliga verksamheten. För att kontinuitetsperspektivet ska komma in naturligt i andra it-processer är det lämpligt att inkludera kontrollpunkter för säkerhet i andra it-processer. I förändringsprocessen är det t.ex. lämpligt att inkludera en kontrollfråga om kontinuitetsdokumentationen för att säkerställa att ändringar i it-miljön inte sker utan att dokumentationen har uppdaterats. För företag som har en etablerad problemprocess sker vanligen utredningar/analyser av allvarliga incidenter i den processen. Det är viktigt att säkerställa att utredning av grundorsak till allvarliga incidenter också belyser kontinuitetsperspektivet och att slutsatser som framkommer återförs till kontinuitetsprocessen.

Test

Organisationen bör testa sina återställningsplaner och de rutiner som beskrivs regelbundet. Syftet med testerna är att utröna huruvida

1. It-resursen kan upprätthållas/återställas oavsett hur allvarlig incidenten är
2. Återställningsrutinerna för it-miljön är tillräckliga för att möta verksamhetens tillgänglighetskrav
3. Rutinerna för återgång till normalläge fungerar som avsett
4. Det finns okända tekniska brister

För att säkerställa relevanta tester bör en teststrategi upprättas som tydligt visar hur organisationen över tid säkerställer förmåga att upprätthålla sina kritiska it-resurser. Teststrategin bör svara på vad organisationen vill uppnå och varför, hur organisationen ska nå dit, samt hur utvecklingen ska mätas.

Som komplement till den strategiska och långsiktiga teststrategin bör en specifik testplan tas fram. En testplan bör visa hur respektive identifierad kritisk it-resurs löpande ska testas. I testplanen dokumenteras förslagsvis testformat, förmågeområden, prioritering och målgrupp. Testplanen bör inkludera olika testtyper. Omfattning och frekvens av tester bör kopplas till hur kritisk resursen är, eller utifrån annan prioritering som angetts i fastställd teststrategi.

Nedanstående utgör exempel på fokus för tester:

1. dataåterställning: återställning av en fil eller databas på grund av korrupt data
2. återställning av en server
3. återställning av en större volym servrar (fysiska eller virtuella efter t.ex. operativsystemhaverier)
4. återställning av en applikation eller it-tjänst (detta kan bestå av flera servrar, underapplikationer och infrastruktur)
5. failover-tester
6. nätverkstester
7. fysisk säkerhet i datahallar, exempelvis brand- och översvämningssystem, utrymningsrutin etc.

F.6. Outsourcad it-verksamhet

Även om en organisation väljer att outsourca delar eller hela it-verksamheten är det viktigt att genomföra ett arbete kring it-verksamhetens kontinuitet för att säkerställa att organisationen kan leva upp till fastställda målsättningar. I avtalsskrivningar mellan leverantörer och beställarorganisationen kan - och bör - förtydliganden göras gällande ansvar och roller vid kontinuitetshanteringen (se Appendix G för djupare beskrivning).

Organisationer bör tillse att kritiska leverantörer kan understödja de åtgärder som behövs för att säkerställa att verksamheten fungerar på en acceptabel nivå, i enlighet med framtagen strategi för it-kontinuitet. När återställningar genomförs hos en leverantör är det även viktigt att i ett tidigare skede fastställa när återställningsprocessen är klar och organisationen kan återgå till normal verksamhet. Detta arbete genomförs i nära samverkan med leverantören. Om korrupt data förekommit kan exempelvis återgång till normal verksamhet förutsätta internt arbete med sådant som leverantören inte har förmåga att genomföra innan systemen är tillgängliga för användarna igen. Det kan till exempel röra sig om att verifiera att data är korrekt eller att transaktioner i verksamhetssystemen genomförs på rätt sätt.

Samarbete och dialog med leverantörer är centralt och det är även viktigt att genomföra gemensamma övningar och tester. Kontinuerliga rapporter från leverantören gällande incidenthanteringen kan vara behjälpliga vid det interna kontinuitetsarbetet. Detta eftersom incidenthanteringen många gånger sker utan att den ger direkt effekt på verksamheten och därmed inte alltid når beställarorganisationen för kännedom.

Återställningsplan för tjänst/system/resurs X

Denna återställningsplan beskriver de reserv-, återställnings- och återgångsrutiner som används för att för att säkerställa kontinuiteten i tjänst/system/resurs X. Återställningsplanen tar sin utgångspunkt i de kravställningar som finns för it-verksamheten baserade på regelbundet uppdaterade konsekvensanalyser och riskbedömningar för den övergripande verksamheten. Denna plan ska utgöra ett stöd vid avbrottshantering och vid prioriteringar för att minska konsekvenserna av ett avbrott i kritiska tjänster/system/resurser.

Ansvarig för återställningsplanen förvarar den elektroniskt samt papperskopia på lämplig plats för att säkerställa att den alltid finns tillgänglig.

Innehållsförteckning:

1. Inledning

I denna återställningsplan beskrivs reserv-, återställnings- och återgångsrutiner för tjänsten X. Kontinuitetsplanen tar sin utgångspunkt i de kravställningar som finns för it-verksamheten baserade på regelbundet uppdaterade konsekvensanalyser och riskbedömningar för den övergripande verksamheten. Denna plan ska utgöra ett stöd vid avbrottshantering och vid prioriteringar för att minska konsekvenserna av ett avbrott i kritiska system/resurser.

2. Beskrivning av systemet/tjänsten

System/tjänst:

Kritisk(a) period(er):

RTO:

RPO:

Verksamhetens kravställare:

3. Kriterier för aktivering av planen

Vägledande princip: Tid som förloras i inledningen av en störning kan inte återfås. Det är därför alltid bättre att inleda åtgärder/aktivera återställningsplanen så snart som möjligt för att eventuellt avaktivera igen, än att invänta en viss mängd information/beslut från ledning etc.

Kriterier för aktivering av plan:

Händelser då planen aktiveras omedelbart:

Kontaktpersoner vid aktivering:

4. *Viktiga leverantörsavtal*

5. *Checklista återställning för olika scenarier*

Typ av händelse	Återställnings- och återgångsrutin
Korrupt data	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*
Hårdvarufel	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*
Växla till alternativ driftanläggning	Reservrutin: *(Hur arbetar vi på alternativa sätt under ett avbrott? Detaljerad beskrivning av reservrutin inklusive roller och ansvar)* Återställningsrutin: *(Hur växlar vi till alternativ driftanläggning efter ett avbrott? Detaljerad beskrivning av återställningsrutin inklusive roller och ansvar)* Återgångsrutin: *(Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)*

	Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

6. ***Enhet/personer ansvariga för återställning av tjänsten/systemet***

7. ***Planerade och utförda återställningstester***

8. ***Bilagor***

Appendix G - Kontinuitetshantering outsourcad verksamhet

Kontinuitetshantering handlar om att säkerställa att en organisations kritiska verksamhet kan fungera på en tolerabel nivå, oavsett vilka störningar som inträffar. I flera fall omfattar den kritiska verksamheten även verksamhet som outsourcats till en leverantör. Beställaren, med ansvar för kontinuitetshanteringen av dess samlade verksamhet, måste därför samarbeta med sina leverantörer för att säkerställa kontinuitetshantering även för den outsourcade verksamheten.

Appendixet riktar sig till samtliga som är involverade i processen för kontinuitetshantering för outsourcad verksamhet och därmed till såväl verksamhetsansvariga, säkerhetsansvariga, kontinuitetsansvariga som beslutsfattare och ledningsfunktioner. Underlaget kan även användas för att skapa en ökad medvetenhet internt i den egna organisationen om kontinuitetshantering i samband med beslut om outsourcing av verksamhet.

Appendixet bygger på intervjuer med aktörer inom finansiell sektor och på internationella standarder. Dokumentet betraktar outsourcing utifrån ett livscykelperspektiv, där den outsourcade verksamheten bör följas från dess att beslut om outsourcing fattas till att avtalet avvecklas.

G.1. Kontinuitetshantering och outsourcing

Kontinuitetshantering handlar om att säkerställa att en organisations kritiska verksamhet kan fungera på en tolerabel nivå, oavsett vilka störningar som inträffar. I vissa fall är hela eller delar av den kritiska verksamheten utlagd till externa leverantörer (outsourcing). Organisationen ansvarar dock fortfarande för kontinuitet i verksamheten och måste därmed arbeta med kontinuitetshantering såväl för den interna som för den outsourcade verksamheten.

Outsourcinglösningar blir alltmer förekommande ur ett internationellt och sektorsövergripande perspektiv[54]. I Sverige finns ingen detaljerad reglering av outsourcad verksamhet för privata finansiella aktörer. Regleringen utgår istället ifrån en principnivå genom ett angivet ramverk i form av föreskrifter som fastställer ett antal skall-krav, medan det är upp till de enskilda aktörerna att på egen hand svara för hur kraven efterlevs.

Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut[55] fastställer övergripande krav för utlagd verksamhet och ställer bland annat höga krav på den kompetens som ska finnas kvar inom organisationen. Ansvaret kan på så sätt aldrig flyttas ut från organisationen.

Den 30 september 2019 trädde Europeiska bankmyndighetens uppdaterade riktlinjer om utlagd verksamhet (outsourcing) i kraft – Guidelines on outsourcing arrangements.

---

[54] *Deloitte's Global Outsourcing and Insourcing Survey – 2014 and beyond.*

[55] *Finansinspektionen - Föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1).*

Riktlinjerna kan utgöra en god vägledning för alla slags företag inom finanssektorn – oavsett företagstyp; bank, kreditinstitut, betalningsinstitut, marknadsinfrastrukturbolag, försäkringsföretag. Riktlinjerna innehåller bland annat krav på interna styrningsarrangemang och riskhantering vid outsourcing[56].

I och med att detta appendix tagits fram innan EBA:s uppdaterade riktlinjerna trädde i kraft har detta appendix ännu inte uppdaterats utifrån EBA:s kravställning. Detta appendix har genomgående hämtat inspiration från internationella standarder[57], Solvens II[58], Basel[59] samt Finansinspektionens föreskrifter FFFS 2014:1[60]. Appendixet fokuserar på outsourcing ur ett kontinuitetsperspektiv. På så sätt finns varken en ambition att ge en heltäckande bild av outsourcing som företeelse eller att beakta andra outsourcingaspekter vid sidan av kontinuitetshantering. Många av de resonemang som presenteras beskriver outsourcad it-verksamhet till följd av att detta var ett vanligt förekommande exempel som nämndes under intervjuerna. Samma resonemang kan dock appliceras oavsett vilken verksamhet som en beställare väljer att outsourca, exempelvis verksamhet kopplad till personalhantering, lokaler etc.

Outsourcing ur ett livscykelperspektiv

Detta appendix betraktar outsourcing utifrån ett livscykelperspektiv. Inför outsourcing genomförs en analys kring om outsourcing är ett lämpligt alternativ för den utvalda verksamheten, vilka leverantörer som finns, fördelar och nackdelar med outsourcing etc. Analysen följs av ett beslut och därefter upprättas avtal med vald(a) leverantör(er). Under avtalsperioden sker löpande uppföljning och samverkan och slutligen upphör avtalsperioden (antingen i förtid eller vid i förväg definierad tidpunkt) och verksamheten återtas eller läggs ut på nytt avtal. De fyra faserna illustreras i nedanstående figur. ¨

Definition av outsourcingbegreppet

I Sverige används vanligen begreppet outsourcing som ett låneord för att beskriva det förhållande som uppstår när en organisation valt att lägga verksamhet (tjänster, processer, funktioner eller resurser) utanför den egna organisationen.

[56] *EBA - Guidelines on outsourcing arrangements (EBA/GL/2019/02).*
[57] *ISO/IEC 27036 - Information technology – Security techniques – Information security for supplier relationships.*
[58] *Europaparlamentets och rådets direktiv 2009/138/EG - Om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II).*
[59] *Basel Committee on Banking Supervision. Outsourcing in Financial Services.*
[60] *Finansinspektionen - Föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1).*

Outsourcing brukar definieras som det förhållande där en organisation överlåter till en annan aktör att utföra en verksamhet som organisationen skulle kunna ha i egen regi. Outsourcing kan på så sätt vara mer eller mindre omfattande. Det kan handla om allt från utläggning av enstaka tjänster eller resurser till outsourcing av hela affärsprocesser eller driftsmiljöer.[61]

Den internationella standarden om informationssäkerhet vid leverantörsrelationer, ISO 27036[62], beskriver outsourcing som inköp av tjänster (med eller utan produkter) där leverantörens resurser används för att utföra delar av beställarens verksamhet. Såväl Basel som Solvens II och FFFS 2014:1 belyser att outsourcing handlar om utlagd verksamhet som i annat fall skulle utföras av den egna organisationen. Basel lyfter fram att det kan handla om verksamhet som beställaren skulle kunna utföra vid tidpunkten för outsourcingbeslutet såväl som på sikt. Basel betonar även att den outsourcade verksamheten ska bestå i löpande verksamhet och att den kan utföras av annan part inom den egna koncernen såväl som av en extern leverantör.[63] Solvens II (som använder sig av begreppet ”uppdragsavtal”) lyfter i sin tur fram att det kan handla om verksamhet som genomförs direkt av en leverantör eller genom underentreprenad.[64]

I denna vägledning används begreppet outsourcing fortsättningsvis för att beskriva utlagd verksamhet som beställaren skulle kunna bedriva internt. Den finansiella aktören som väljer att outsourca en del av sin verksamhet benämns fortsättningsvis ”beställare” och aktören som åtar sig att leverera efterfrågad verksamhet benämns fortsättningsvis ”leverantör”.

Möjligheter och begränsningar med outsourcing

Precis som definitionen av outsourcing varierar mellan olika aktörer varierar också antalet outsourcinglösningar från single- och multisourcing till olika molnlösningar. Nyttan med outsourcing kan variera beroende på den lösning en beställare väljer för att såväl organisera som bedriva verksamheten i relation till leverantören.

Det är därmed problematiskt att presentera konkreta möjligheter och begränsningar som gäller för samtliga outsourcinglösningar. Exempelvis kan en vald outsourcinglösning som möjliggör tillgång till expertkunskap och konkurrensfördelar samtidigt medföra reducerad kontroll eller andra kort- eller långsiktiga begränsningar. Nedan presenteras ett antal aspekter som ofta lyfts fram vid bedömning av möjligheter och begränsningar med outsourcing.

Ekonomiska aspekter

Ett vanligt argument för outsourcing är att det bedöms som mindre kostsamt att outsourca än att på egen hand utföra verksamheten. Huruvida så alltid är fallet kan dock diskuteras. Å ena sidan är investeringskostnaden för en intern konkurrenskraftig lösning i många fall högre än en outsourcinglösning då en leverantör kan nå stordriftsfördelar och därigenom minska kostnaderna. Vidare kan beställaren fokusera sina resurser på kärnverksamheten vilket kan leda till effektivitetsfördelar och ökat resultat.

---

[61] *MSB - Upphandla Informationssäkerhet – en vägledning.*

[62] *Information technology — Security techniques — Information security for supplier relationships, ISO/IEC 27036.*

[63] *Basel Committee on Banking Supervision. Outsourcing in Financial Services.*

[64] *Solvens II (artikel 13 punkt 28).*

Slutligen kan en outsourcinglösning även t.ex. möjliggöra geografisk expansion vilken kan leda till ökade intäkter. Å andra sidan förutsätter en outsourcinglösning oftast att beställaren upprättar/behåller en intern organisation som innehar beställarkompetens avseende den outsourcade verksamheten, ansvarar för kontakt i det löpande arbetet och följer upp den outsourcade verksamheten. En sådan organisation kan, beroende på den outsourcade verksamhetens omfattning och komplexitet, vara kostsam och bidra till minskad lönsamhet. Denna kostnad underskattas ofta.

Kompetens hos leverantör och beställare

Tillgång till kompetens och expertis brukar nämnas som ett argument för outsourcing. Beställaren kan genom outsourcing få tillgång till kompetens, tekniska gränssnitt och lösningar som redan finns hos extern aktör, snarare än att behöva tillägna resurser till utveckling av detta internt. Exempelvis finns det internationella aktörer som specialiserat sig på olika delverksamheter där samarbete kan vara att föredra framför att utveckla kompetensen på egen hand. En nackdel kan å andra sidan vara att beställaren förlorar kompetens i samband med outsourcing av en process i och med att personal antingen förflyttas till leverantör eller slutar. Kompetensförlusten är i sig en utmaning för många beställare då kompetensen (som framförts ovan) behövs vid beställarorganisationen även om tjänsten som sådan outsourcats.

Det är lätt att undervärdera hur mycket tid och resurser som förutsätts finnas kvar inom den egna verksamheten även om en tjänst lagts ut till extern part. Detta gäller särskilt då outsourcing förflyttar verksamheten längre ifrån beställaren vilket i många fall minskar insynen i verksamheten och/eller ställer högre krav på uppföljning och kontroll.

Flexibilitet och innovation

Flexibilitet i kapacitetsutnyttjande kan underlättas i de fall en verksamhet outsourcats eftersom leverantörer ofta har möjlighet att skala upp/ner verksamheten. Detta kan vara betydligt svårare om verksamheten finns inom organisationen. Flexibilitet i verksamheten kan ge såväl operationella som ekonomiska fördelar.

Samtidigt kan innovation och utveckling av verksamheten begränsas vid outsourcing eftersom leverantören troligtvis inte har samma känsla och ansvar för utvecklingsinsatser som om verksamheten bedrivits i beställarens egen regi. Outsourcing kan på så sätt möjligen influera innovationsförmågan om nödvändiga utvecklingsinsatser för ett mer säkert och effektivt system avstannar och endast de mest nödvändiga uppdateringarna genomförs.

Kontroll över outsourcad verksamhet

En av de största begränsningarna med en outsourcinglösning är att kontrollen över den outsourcade verksamheten starkt begränsas. Det kan exempelvis handla om minskad insikt i hur känslig information lagras, vilka redundanta lösningar som finns eller hur ofta reservlösningar testas. Det är också möjligt att leverantören i sin tur lägger ut delar av sin verksamhet till ytterligare leverantörer. Leverantörskedjorna kan på så sätt bli långa och komplexa och därmed svåra att ha kontroll över. Till viss del kan kontrollpunkter och begränsningar skrivas in i avtal, men en lika fullständig kontroll som om verksamheten drivs internt är mycket svår att uppnå.

Summering

Nedan listas en summering av de fördelar som en intern lösning respektive en outsourcinglösning kan innebära.

Intern lösning	Outsourcinglösning
• Bibehållen kompetens inom den egna organisationen • Ökad förmåga till kontroll • Ökad förmåga till styrning av verksamheten • **Minskad risk för leverantörs-koncentrationer** • **Minskad risk för externa inlåsningseffekter**	• Möjlighet till stordriftsfördelar • Möjlighet att tillgå expertkompetens • Ökad förmåga till flexibilitet • Möjlighet till ökad redundans genom ett större utbud av säkerhets- och kontinuitetslösningar • Ökad möjlighet till snabb utveckling av nya tjänster

G.2. Analys och beslut

Inför att en verksamhet ska outsourcas krävs en noggrann analys för att säkerställa att ett välgrundat beslut fattas. Bland annat bör en analys av vilken verksamhet som ska outsourcas genomföras, på vilket sätt outsourcingen ska ske och vilka risker för kontinuiteten i verksamheten som outsourcingen kan innebära. Detta gäller oavsett om det är befintlig eller ny, kompletterande, verksamhet som avses. Detta kapitel syftar till att ge stöd till analysen inför ett beslut om outsourcing.

Som ett ingångsvärde är det, ur ett kontinuitetsperspektiv, av vikt att personer från olika delar av verksamheten och med olika perspektiv deltar i analysen. Funktioner såsom systemägare, affärsägare, stödverksamheter, it-drift/förvaltning, jurist, kontinuitetsansvarig, riskansvarig etc. bör bli involverade i beslutet om outsourcing. I hur stor utsträckning de olika funktionerna involveras varierar beroende på vilken tjänst som ska outsourcas och hur kritisk denna tjänst är.

Viktigt är dock att alltid inkludera såväl strategisk, taktisk som operativ nivå i beslutet. Ur ett kontinuitetsperspektiv är det viktigt att alltid även inkludera en kontinuitetsansvarig i beslutet.

Val av verksamhet för outsourcing

Utgångspunkten bör vara att verksamheten som outsourcas ska kunna fortsätta levereras enligt kunders/medarbetares/andra intressenters krav, lika effektivt eller effektivare än om verksamheten behålls internt.

Särskilt noggranna analyser krävs om det är verksamhet som kan betraktas som kärnverksamhet som ska outsourcas. Det finns många aspekter att beakta om kärnverksamhet outsourcas till annan part, men ser man till lagstadgade krav finns ingen begränsning för vilken verksamhet som kan outsourcas. Därmed är det möjligt att outsourca en så kallad kärnverksamhet så länge krav på verksamhetens funktion efterlevs. Samtidigt måste konstruktionen av affärsverksamheten givetvis vara begriplig för att tillståndet att bedriva verksamheten ska bestå.

Att göra en tydlig avgränsning för vad som är, eller bör utgöra, en beställares kärnverksamhet är dock inte alltid helt lätt. Särskilt i ett långsiktigt perspektiv då definitionen av beställarens kärnverksamhet kan förändras över tid, där det som idag inte är en kärnverksamhet mycket väl kan vara det om tio år eller tvärtom. Utvecklingen av mobila banktjänster utgör ett exempel; en verksamhet som möjligen initialt betraktades utgöra en stödtjänst för banker men som på förhållandevis kort tid växt till att bli en del av kärnverksamheten.

För finansiella aktörer begränsar reglerna[65] möjligheten att lägga över kritisk verksamhet till extern leverantör om:

- avtalet försämrar kvaliteten i företagsstyrningssystem,
- operativa risker ökar otillbörligt,
- tillsynsmyndigheternas möjlighet till kontroll begränsas eller,
- avtalet hindrar tillfredsställande service till beställarens kunder.

Därtill finns för försäkringsbolag en informationsskyldighet gentemot tillsynsmyndigheterna om en kritisk funktion eller verksamhet outsourcas samt en anmälningsplikt för finansiella aktörer om den outsourcade verksamheten genomgår väsentliga förändringar.[66] Detta, tillsammans med att förflyttning av delar av kärnverksamheten till extern aktör kan vara förenat med ett risktagande, tyder på att en beställare särskilt bör överväga om kritisk verksamhet bör flyttas över till en leverantör. Samtidigt kan det i vissa fall vara motiverat att göra just så, exempelvis för att nå viss expertkunskap.

Kontinuitetsanalys av den egna verksamheten

Kontinuitetsanalyser bör göras regelbundet i alla typer av organisationer, oavsett om verksamheten är föremål för outsourcing eller inte. Syftet är att förebygga och/eller minska konsekvenserna av störningar i verksamheten genom att ha kännedom om befintliga beroenden, hur störningar påverkar beställarens verksamhet i sin helhet samt vilka reservlösningar som finns eller bör implementeras. För verksamhet som outsourcas möjliggör dessutom en genomförd kontinuitetsanalys väl underbyggda och relevanta kravställningar på leverantörerna. I detta avsnitt beskrivs kortfattat hur en kontinuitetsanalys av verksamheten bör ske. För ett mer utförligt stöd i hur en kontinuitetsanalys bör genomföras, se *FSPOS Vägledning för kontinuitetshantering*.

Kontinuitetsanalysen inleds med en kartläggning av verksamhetens kritiska processer, aktiviteter och resurser. I analysen kartläggs verksamhetens kritiska processer, en process åt gången. För processen dokumenteras kritiska aktiviteter och tillhörande resurser (både interna och externa). För aktiviteterna och resurserna anges tidsgränser för hur långa avbrott som kan tolereras för respektive aktivitet (maximal tolerabel avbrottstid) samt mål för återställningstider. Tiderna sätts utifrån fastställda kriterier för när verksamheten drabbas av oacceptabla konsekvenser, exempelvis inom förtroende, ekonomi, servicenivå etc. I detta sammanhang är det viktigt att beställaren inte rakt av förutsätter att samma avbrottstider kan användas då verksamheten förflyttas till en leverantör.

---

[65] *Finansinspektionen - Föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1).*

[66] *Solvens II (Artikel 49).*

Istället bör beställaren noga analysera vilka effekter en eventuell outsourcinglösning får för angivna tider. Exempelvis kan outsourcing medföra längre ledtider och att den egna verksamheten behöver utökad tid efter att återställning hos en leverantör genomförts. Som beskrivet ovan är det viktigt att denna analys har genomförts innan beslut om outsourcing och att analysen ligger till grund för den senare kravställningen. Om kontinuitetsanalysen genomförs på en redan outsourcad verksamhet bör leverantören delta i analysen och ge ingångsvärden för de delar av verksamheten som ligger under dennes ansvar.

Kontinuitetsanalysen leder fram till att en eller flera kontinuitetsplaner kan tas fram för verksamheten och dess kritiska resurser. Kontinuitetsplanerna ska beskriva alternativa lösningar för de fall de kritiska resurserna blir otillgängliga och på så sätt möjliggöra för verksamheten att fungera på en tolerabel nivå, oavsett vilka störningar som inträffar. Lösningarna beskrivs med fördel i konkreta termer exempelvis genom rutiner och checklistor.

Planerna ska inkludera såväl intern som outsourcad verksamhet, även om de lösningar som beskrivs i planerna skiljer sig åt beroende på om verksamheten är intern eller outsourcad. Krav bör också ställas på leverantörerna att upprätta och underhålla egna kontinuitetsplaner för de processer/resurser de ansvarar för (se vidare avsnitt *4.2 Kravställning*).

Tips för genomförande:
- Utgå alltid från den egna verksamhetens funktion vid överväganden om outsourcing
- Avbrottsperioder som angetts för den egna verksamheten är inte nödvändigtvis desamma om en aktivitet eller process outsourcas till extern leverantör
- Säkerställ regelbundet uppdaterade kontinuitetsplaner för både intern och outsourcad verksamhet
- Använd FSPOS vägledning för kontinuitetshantering för stöd i analys av verksamheten

Riskanalys

Kontinuitetsanalysen bör kompletteras med en riskanalys där de risker som kan påverka kontinuiteten i verksamheten identifieras och vid behov åtgärdas. Ur ett bredare perspektiv bör riskanalysen täcka in alla typer av risker (strategiska, operativa, finansiella etc.), men inom ramen för detta appendix exemplifieras främst risker som bedöms kunna påverka kontinuiteten i en (outsourcad) verksamhet.

Riskanalysen och beställarens riskacceptans måste vara vägledande vid beslut om outsourcing. En riskanalys med kontinuitetsfokus leder till en djupare förståelse för de risker och hot som kan kopplas till verksamhetens kritiska resurser och avbrott i dessa. Exempelvis kan flytt av verksamheten till annat land – så kallad offshoring - vara att föredra för en typ av verksamhet medan samma lösning för en annan verksamhet kan vara mindre lyckad.

Att genomföra en riskanalys bör ses som en nödvändighet och kan ses utgöra en grund för uppföljning kring hur beställaren och leverantören hanterar riskerna i verksamheten, vilket även utgör ett krav från Finansinspektionen.[67] Verksamhetsansvariga för den verksamhet som övervägs outsourcas bör givetvis medverka för att se vilka effekter en eventuell outsourcing skulle medföra. Det är även av vikt att i riskanalysen betrakta outsourcingen på kort såväl som lång sikt.

Riskanalysen kan genomföras enligt ett antal steg som anges i den internationella standarden för riskhantering[68]; etablera kontext (riskacceptans), identifiera risker, bedöma sannolikhet och konsekvens för respektive risk, utvärdera riskerna och ta fram åtgärdsplaner för de risker som inte kan accepteras.

Nedan presenteras ett antal risker som mer eller mindre bedöms kunna påverka kontinuiteten i verksamheten och som därmed bör inkluderas i riskanalysen. Kontinuitetsansvarig ansvarar inte för att identifiera samtliga risker utan behöver ingångsvärden från riskanalyser utförda av andra personer och enheter inom organisationen. Listan är på intet sätt uttömmande utan bör kompletteras utifrån den egna organisationen och den outsourcade verksamhetens förutsättningar.

Risktyp	Riskexempel
Strategisk risk	• Verksamhet kan vara oförenlig med beställarens strategiska målsättningar. • Otillräcklig kompetens eller underlåtenhet vid tillsyn av leverantören.
Risk – i relation till beställarens anseende	• Dålig service från leverantören. • Kundinteraktion överensstämmer inte med den standard som beställaren fastställt för dess egen verksamhet. • Leverantörens metoder är inte i linje med metoder som fastställts av beställaren.
Risk – i relation till regelefterlevnad	• Lagar (ex. sekretess eller tillsyn) uppfylls eller efterlevs inte tillräckligt. • Leverantören har otillräckliga system och kontroller för efterlevnad.
Operativa risker	• Tekniska problem. • Otillräcklig finansiell kapacitet för att uppfylla sina skyldigheter och/eller tillhandahålla lösningar. • Oegentligheter eller fel.
Avvecklingsrisk	• Ändamålsenliga avvecklingsstrategier finns inte. Detta kan uppstå utifrån en övertro på ett företag, förlust av relevant kompetens inom den egna organisationen för att ta tillbaka verksamheten i egen drift samt kontrakt som gör en snabb avveckling mycket kostsam.

[67] *Finansinspektionen - Föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1) §10.*

[68] *Risk management - Principles and guidelines (ISO 31000).*

	• Begränsad förmåga att ta tillbaka outsourcad verksamhet till annat land på grund av brist på personal eller komptensbortfall.
Geografiska risker	• Politiska, sociala och legala förutsättningar kan addera risk. • Kontinuitetsarbetet blir mer komplext.
Kontraktuella risker	• Förmåga att verkställa kontrakt. • Vid förlagd verksamhet i annat land (offshoring) är ”val av lag” viktigt.
Tillgänglighetsrisker	• Potentiell begränsning i förmåga att tillhandahålla information till den egna organisationen och till tillsynsmyndigheterna. • Svårigheter för tillsynsmyndigheterna att förstå verksamheten som outsourcats. (överblick, insyn).
Koncentrationsrisker	• Reducerad kontroll för beställaren. • Systematiska risker för den finansiella sektorn som helhet.

Mot bakgrund av genomförda kontinuitets- och riskanalyser kan ett medvetet och välgrundat beslut om outsourcing genomföras. Analysen av den aktuella verksamheten kan och bör ligga till grund för de kravställningar som görs vid den senare eventuella upphandlingen.

Val av leverantör

När en verksamhet outsourcas är det viktigt att ha en kännedom om leverantören, såväl i det inledande skedet som under löpande avtal. Valet av leverantör bör utgå ifrån en genomförd analys och utifrån ett förtroende för att leverantören förvaltar den aktuella tjänsten på ett förtjänstfullt sätt. Detta avsnitt beskriver områden som är värda att tänka på inför val av leverantör.

Företagsbesiktning

Att göra en företagsbesiktning, en så kallad due diligence, av den bäst lämpade leverantören kan ses som en förutsättning för att gå vidare i dialog om avtalsskrivning. En företagsbesiktning kan vara mer eller mindre omfattande beroende på den verksamhet som övervägs outsourcas, men innehåller vanligen delområdena finansiell, legal, skatte- och teknisk besiktning. Att granska en tilltänkt leverantör är viktigt för att kontrollera att leverantören kan tillhandahålla tjänsten över en längre tid. Företagsbesiktningar kan med fördel genomföras regelbundet även under löpande avtal. Detta då det inte är säkert att ägarförhållanden och dylikt är desamma under en längre tidsperiod. Vidare kan det vara framgångsrikt att efterfråga och utvärdera referenser från de aktuella leverantörerna.

Leverantörskedjor

Inför ingående av avtal med en leverantör bör beställaren även undersöka om underleverantörer kommer att användas för tillhandahållande av den aktuella verksamheten. Långa leverantörskedjor kan minska insyn och tillgänglighet i verksamheten ytterligare samt öppna upp för andra sårbarheter i tjänsten. I de fall där leverantörskedjor förekommer bör företagsbesiktning göras även av underleverantörerna och de bör också finnas med i analysen av den egna verksamheten (se avsnitt 3.2).

Kravställningar bör formuleras redan vid upphandlingen

Leveransmässiga villkor avseende kontinuitetshantering bör inte endast stipuleras vid ingående av avtal med en viss leverantör utan bör finnas med som skall-krav redan vid upphandlingen och fungera som urvalskriterier för vilka leverantörer som är lämpliga att sluta avtal med. Kraven bör utgå ifrån den tidigare analysen av verksamheten och de krav som ställs på den egna organisationen (se avsnitt 3.2).

Konkurrensutsättning och koncentrationsrisker

En beställare kan välja att outsourca en verksamhet till en enskild leverantör att förvalta (single-sourcing), eller att dela upp verksamheten i mindre delar och använda sig av flera leverantörer för olika delverksamheter (multi-sourcing). Båda lösningarna ställer krav på fungerande samverkan med leverantören/leverantörerna, medan den senare lösningen även förutsätter ett beställaransvar för koordinering mellan de externa leverantörerna.

För vissa typer av tjänster kan det vara en fördel att använda sig av flera leverantörer för samma tjänst, dels ur säkerhetssynpunkt då verksamhet kan växlas över och dels utifrån en ekonomisk aspekt där flera leverantörer medför ökad konkurrens och lägre pris. Även om en beställare väljer att använda sig av flera leverantörer finns risk att flera andra organisationer använder sig av samma leverantörer. Detta förhållande kan utifrån ett sektorsperspektiv sammanfattas med begreppet koncentrationsrisker. Ett exempel utgörs av att en beställare upphandlar en leverantör för it-drift, en leverantör som även upphandlats för it-drift av flera andra finansiella organisationer inom sektorn.

Från Finansinspektionen finns inga krav relaterade till koncentrationsrisker. Detta är dock något som aktörer själva bör överväga innan de väljer att lägga ut verksamhet till extern part då de fortsatt är ansvariga för verksamheten och möjligen inte vet exempelvis vilken prioritetsordning deras verksamhet har vid avbrott hos leverantören. För den finansiella sektorn är koncentrationsrisker högst relevanta att analysera och hantera ur ett kontinuitetsperspektiv.

Tips för genomförande
- Genomför företagsbesiktningar både vid ingående av avtal och regelbundet under gällande avtal
- Undersök och vid behov begränsa, potentiella leverantörskedjor
- Ställ krav på alla delar av leverantörskedjan
- Fundera kring fördelar och nackdelar med single- respektive multisourcing
- Analysera och hantera eventuella koncentrationsrisker

G.3. *Upprättande av avtal*

Genom avtalsskrivningar som fastställer en tydlig ansvarsfördelning mellan beställaren och leverantören kan robustheten i den outsourcade verksamheten öka. Om rätt krav ställs och om beställaren har väl inarbetade rutiner för uppföljning och granskning kan outsourcing leda till bättre ”ordning och reda” och struktur på de utlagda tjänsterna än om de behållits internt. Samarbete och dialog med valda leverantörer vid såväl strategisk som operativ nivå är också centralt för att öka robustheten i den outsourcade verksamheten.

Detta kapitel syftar till att ge stöd vid upprättande (eller omförhandling) av avtal med outsourcingleverantörer.

Utgå från analys av verksamheten i kravställning

Finansinspektionens föreskrifter fastställer ett antal krav för outsourcingavtal gällande kritisk verksamhet, bland annat att beställaren säkerställer att regelverket följs och att leverantören har en strukturerad process för övervakning, men föreskrifterna ställer inte krav på hur kraven ska uppnås. På detta sätt gäller fortsatt principen om att de krav som ställs på bolagens egen verksamhet ska gälla även för outsourcad verksamhet. Hur detta genomförs är dock upp till de enskilda bolagen att svara för. Därmed blir beställarens kravställning vid avtalsskrivning viktig. Kravställningen bör utgå ifrån outsourcingens livscykel och bör därmed utgå från kontinuitets- och riskanalysen av den egna verksamheten. Kravställningar bör därtill vara tydligt preciserade i avtalet med leverantören, där tydlighet i begreppsdefinitioner vid avtalsskrivningen är centralt. Vid händelse av kris eller störningar är det av stor vikt att ha tydliga definitioner i avtalet av de åtgärder som ska vidtas och hur samverkan ska ske. Leverantörer har eventuellt ett incitament att definiera kris- och störningsbegreppen så brett som möjligt, medan en så tydlig definition som möjligt ligger i beställarens intresse.

Kraven bör inte enbart fokuseras till servicenivåer, utan bör exempelvis även inkludera hur dialog och kommunikation ska ske under löpande avtal samt hur och när avvecklingen av avtal kan ske.

Kravställning

I detta avsnitt ges exempel på kriterier som kan vara relevanta att inkludera i avtal med leverantörer. Viktigt att notera är att alla verksamheter och avtal är unika. Denna beskrivning är därför inte heltäckande utan beställaren måste säkerställa att samtliga relevanta kriterier är inkluderade i varje enskilt avtal.

Vid formulering av krav att inkludera i avtal är det viktigt att säkerställa att kraven i så stor utsträckning som möjligt är mätbara och med lämplig regelbundenhet är möjliga att följa upp.

Fastställande av en tydlig ansvarsfördelning

Som tidigare nämnts ligger ansvaret för verksamheten kvar hos beställaren även om verksamheten outsourcats. En risk med att outsourca är att ansvarskänslan minskar. Det är därför viktigt att det finns en medvetenhet kring att ansvaret för de verksamheter som outsourcats förblir hos beställaren. I avtalen är det viktigt att utse enskilda personer som ansvarar för den outsourcade verksamheten.

För att leverantörerna ska kunna upprätthålla robusthet i sina tjänster och därmed kunna leverera det de åtagit sig att leverera förutsätts att både beställare och leverantör utser kontaktpersoner samt underhåller listor med kontaktuppgifter och delger dessa till varandra.

Beroende på storlek och komplexitet på den outsourcade verksamheten bör ansvariga utses på strategisk, taktisk och operativ nivå. Exempel på ansvarsområden kan bestå i samverkan, teknik, ekonomisk uppföljning och granskning/revision. Det bör även tydligt framgå var den enes ansvar slutar och var den andres ansvar tar vid. Ansvarsfördelningen bör kunna styrkas med hänvisning till en formell arbetsbeskrivning där respektive funktions, tillika individs, ansvar finns noga beskrivet. Att säkerställa att en viss funktion har arbetstid och mandat att genomföra det ansvar som preciseras är också av vikt, inte minst då dessa uppgifter kan komma att efterfrågas av Finansinspektionen vid en granskning.

För förtydligande av roller och ansvar kan HUKI-modellen[69] användas. Modellen föreslår en ansvarsfördelning mellan beställare och leverantör utifrån de fyra ansvarsområdena: huvudansvariga, utförare, konsulterade och informerade, i förhållande till den outsourcade verksamheten.

Tips för genomförande:
- Ansvaret för verksamheten och leverans till kund stannar alltid kvar hos beställaren
- Roller och ansvar bör specificeras i avtalet
- Utdelat ansvar bör kunna dokumenteras i en formell ansvarsbeskrivning

Ansvar för underleverantörer och leverantörskedjor

Det ligger i beställarens intresse att säkerställa att avtalet reglerar ansvaret gentemot eventuella underleverantörer. Detta är särskilt viktigt eftersom de regelefterlevnadskrav som ligger på beställaren fortsatt är gällande även om delar av verksamheten förflyttas till extern(a) part(er), vilket förutsätter en kontrollverksamhet från beställarens sida. Beställaren kan genom avtalet fastställa om underleverantörer kan användas för hela eller delar av den aktuella verksamheten.

Beställaren kan även fastställa att leverantören måste meddela beställaren om leverantören har för avsikt att använda sig av ytterligare underleverantörer för den outsourcade verksamheten under löpande avtal. Detta är av betydelse då en ökning av antalet leverantörer kan få omfattade konsekvenser för den egna kontrollverksamheten. Vid sidan av att beställaren ska vara informerad kan avtalet även redogöra för att beställaren måste konsulteras och lämna sitt medgivande innan underleverantörer används för den outsourcade verksamheten.

Därmed ges möjlighet att genomföra t.ex. företagsbesiktningar och införa krav på kontinuitetshantering hos de aktuella underleverantörerna.

Leverantörskedjor är i många fall förekommande, vilket gör att kontrollen blir än svårare att behålla. Det krävs därför en avvägning av hur långt tillbaka i leverantörskedjan som beställaren bör ställa krav. Snarare än att ställa krav på leverantörernas underleverantörer regleras robusthet och redundans vanligen genom avtal med den egna leverantören, där påföljder för misslyckande att leverera utlovad tjänst beskrivs. Ett sätt att ställa krav på underleverantören är därmed att ställa krav på att leverantörerna ska ha höga krav på servicenivåer gentemot sina underleverantörer för att kunna garantera leverans i så stor utsträckning som möjligt.

[69] *Huvudansvarig, utförare, konsulterad, informerad. Kommer ifrån engelskans RACI (responsible, accountable, consulted, informed).*

Samverkan med leverantören

Vid fastställande av roller och ansvar bör även former för löpande dialog och kommunikation hanteras. Ett lämpligt sätt är att upprätta olika forum för samverkan med leverantören, exempelvis för kontinuitet, utbildning, säkerhetsfrågor, driftsfrågor etc. Beroende på den outsourcade verksamhetens omfattning och komplexitet kan dessa forum upprättas på olika nivåer.

Hur forumen ska drivas och upprätthållas bör också anges i avtalen genom tydliga angivelser av ansvar, form och frekvens. Mer om hur dialogen och samarbetet med leverantören kan genomföras presenteras i kapitel 5.

Införlivande av regelförändringar

Beställaren bör säkerställa att leverantören kan uppvisa en strategi för hur den outsourcade verksamheten anpassas till eventuella regelförändringar. En nyckel i detta arbete är en samsyn mellan beställare och leverantör om hur regelförändringar ska tolkas. Då det i många fall kan finnas delade meningar om vad en regel innebär bör det tydligt anges i avtalen vem som har tolkningsföreträde.

Lagring av information och informationssäkerhet

Då informationsförluster inte är acceptabla är det en förutsättning att ställa krav på redundans när det gäller lagring av information så att informationen inte försvinner vid händelse av störningar eller avbrott i tjänsten. För att säkerställa redundans vid outsourcade it-relaterade verksamheter kan exempelvis krav ställas på robust utrustning, skalskydd, speglad information, processer för releasehantering och geografiskt separata driftställen.

Avtalet bör även reglera hur leverantören hanterar känslig och konfidentiell information. Ett sätt att reglera detta är att säkerställa att det finns fastställda rutiner för hur leverantören hanterar känslig information samt att dess personal utbildas och övas regelbundet. Om beställaren outsourcar verksamhet som inkluderar lagring av personuppgifter, till exempel löneregister, måste dataskyddsförordningen (GDPR) tas i beaktande. Viktigt att notera är att det alltid är beställaren som är personuppgiftsansvarig. Datainspektionen är den myndighet som ansvarar för att behandlingen av personuppgifter sker på ett korrekt sätt.

Datainspektionen kan ställa särskilda krav på bland annat autentisering och kryptering vid hantering av känsliga personuppgifter, brottsuppgifter och sekretesskyddade uppgifter.

Vidare är det av vikt att redan vid upprättande av avtal tydliggöra vad som händer med den information som hanterats av en leverantör, då avtalet avbryts eller löper ut. Mer om informationshantering i samband med outsourcing ges i MSB-rapporten *Informationssäkerhet i upphandling*[70].

Fastställande av servicenivåer

Beställare bör ställa krav på sina leverantörer avseende tillgänglighet och service. Hur detta, rent tekniskt, uppnås lämnas ofta upp till leverantören att besluta. Kraven som ställs bör dels utgå från kontinuitetsanalysen och dels bero på ingångsvärden från leverantören för att säkerställa att kraven är möjliga att möta.

[70] *MSB - Upphandla Informationssäkerhet – en vägledning.*

För att säkerställa tillgänglighet, service och kvalitet i den verksamhet som outsourcats anges vanligen servicenivåer i leverantörsavtal. Dessa anges i delavsnitt i det övergripande leverantörsavtalet och benämns *Service Level Agreement (SLA)*. Vid sidan av att anpassa den outsourcade verksamheten utifrån beställarens behov tydliggör SLA:er även vilka mål som leverantören har att förhålla sig till och kan på så sätt även användas inom kontrollverksamheten vid uppföljning av verksamheten.

Beroende på hur kritisk den verksamhet som outsourcats är kan servicenivåerna skilja sig åt och vara mer eller mindre specifika. För vissa verksamheter kan det vara rimligt att specificera servicenivåer kopplat till olika resurser, medan det för andra verksamheter räcker att specificera servicenivåer för den samlade outsourcade verksamheten. Ju högre servicenivåer som anges desto dyrare, därför kan en avvägning genom kostnadsnyttoanalys även vara att rekommendera. Nedan presenteras ett antal vanligt förekommande parametrar som är att överväga att inkludera i avtalet och som är kopplade till begreppen: tillgänglighet, maximalt antal fel, servicetid och åtgärdstid.

Tillgängligheten för en outsourcad verksamhet eller tjänst beskrivs vanligen uttryckt i procent. Exempelvis innebär 90 % tillgänglighet att en verksamhet förväntas vara fri från avbrott 90 % av tiden.

Ett annat sätt är att uttrycka tillgängligheten inverterat, det vill säga som otillgänglighet eller som avbrottsperioder, vilket bland annat görs i Kammarkollegiets ramavtal för varor och tjänster som upphandlas ofta[71]. Ett exempel på hur tillgänglighet och otillgänglighet kan uttryckas i avtal följer enligt nedan presenterad tabell.

Tillgänglighet	Otillgänglighet (per år)	Otillgänglighet (per månad)
90 %	876 timmar	73 timmar
99 %	87,6 timmar	7 timmar 18 minuter
99,9 %	8,76 timmar	43 minuter 48 sekunder
99,99 %	52 minuter 33 sekunder	4 minuter 22 sekunder
99,999 %	5 minuter 15 sekunder	26 sekunder

I vissa fall kan det vara lämpligt att ställa mer specifika krav gällande tillgänglighet, exempelvis kan krav ställas på högre tillgänglighet då verksamheten är särskilt känslig för avbrott. Detta kan vara under särskilda dagar i månaden, vissa dagar på året, eller under vissa tider på dygnet. Beställare bör som krav eller i dialog med leverantören tydliggöra hur tillgänglighetstiden räknas ut samt gärna även kräva att få se historiska siffror på tillgänglighet innan avtal skrivs på.

För vissa tjänster är det lämpligt att ställa krav på maximalt antal avbrott. Särskilt då frekvensen av avbrott är mer viktigt för verksamheten än hur långa avbrotten är.

[71] *Exempel på Kammarkollegiets ramavtal med olika leverantörer finns på www.avropa.se.*

Beställare bör säkerställa att de tjänster som är särskilt känsliga för antalet avbrott garanteras en servicenivå med maximalt antal avbrott som kan accepteras. Maximalt antal avbrott bör precis som tillgänglighet även specificera vilken tidsperiod som gäller och leverantören bör även kunna uppvisa historiska siffror på antal avbrott hos den berörda tjänsten. Beroende på vilken verksamhet som outsourcats kan acceptansnivån för maximalt antal avbrott variera. Oavsett hur många avbrott som beställaren väljer att acceptera genom avtalet är det viktigt att säkerställa att beställare och leverantör har samma definition av begreppet ”avbrott”. Denna definition bör finnas med i avtalet, gärna med förtydligande exempel.

Krav bör även ställas på servicetid och åtgärdstid. Servicetid avser den tid som leverantören kan förväntas vara tillgänglig för att åtgärda eventuella avbrott. För mer kritiska tjänster, som har en högre servicenivå, är det vanligt och ofta lämpligt att ha servicetid dygnet runt alla dagar i veckan medan det för mindre kritiska tjänster är vanligt och ofta lämpligt att ha en mer begränsad servicetid. Servicetiden kan på så sätt variera från t.ex. ”*24/7 service*” till ”*service under kontorstid måndag till fredag 08.00-18.00*”, beroende på hur kritisk verksamheten anses vara.

Åtgärdstid är i sin tur den tid som passerar från det tillfälle då avbrottet anmäls eller upptäcks av leverantören, till dess att det är åtgärdat och verksamheten är återställd till normalläge.

Beställare bör se till att åtgärdstiden är tydliggjord i det avtal som upprättas och att åtgärdstiderna tillgodoser de krav som den egna verksamheten har, exempelvis genom *”Maximal åtgärdstid per avbrott under servicetid (timmar)”*. Kravställning på åtgärdstider gällande it-system bör ta hänsyn till hur lång tid det tar från återstart av systemet till dess att alla eventuella följdverkningar har hanterats.

Larm och eskalering

Det är vanligt att servicenivåer som anges i avtal avser drift i normalläge. Men det är fördelaktigt att särskilda krav på servicenivå vid kriser och extraordinära händelser specificeras i avtalet. Därmed är det även viktigt att avtalet tydligt anger vad en extraordinär händelse eller krisläge innebär, samt huruvida det är leverantören, beställaren eller båda två som kan avgöra om en sådan händelse föreligger. Även force majeure bör definieras i avtalet och vilken/vilka av parterna som har möjlighet att besluta om denna typ av händelse föreligger.

Tips för genomförande:
- En klausul om force majeure kan formuleras enligt nedan:
  - *”Om någon av parternas skyldigheter förhindras på grund av krig, naturkatastrof, strejk, lockout, blockad eller annan liknande omständighet vilken part inte kunnat förutse eller påverka och där konsekvenserna inte kunnat undvikas, ska den part som inte har möjlighet att uppfylla sina skyldigheter vara befriad från dessa så länge hindret föreligger.” *Inspiration från Kammarkollegiets leveransavtal inom Företagshälsovård*

Exempel på andra krav som kan ställas är att leverantören har rutiner för larmning och eskalering till beställaren samt vilka kriterier som gäller för larmning. Leverantören bör också ha utsett ansvariga för kontakt med beställaren vid störningslägen. Detta är särskilt viktigt vid multi-sourcing, där det kan vara lämpligt att genomföra möten med alla berörda leverantörer.

Avtalet bör även tydligt definiera vid vilken grad av störning beställaren informeras, hur informationen förmedlas och till vem, samt vilken information som ska delges. Avtalet kan exempelvis stipulera att leverantören ska delge vilka tjänster som har drabbats eller vad prognosen för avhjälpning är. Ibland kan kravet på information definieras i termer av löpande statusrapporter och för mindre kritiska tjänster kan det till exempel räcka med en rapportering vid avbrott och en rapportering vid det slutgiltiga återställandet av tjänsten. Beställare bör även säkerställa att leverantören alltid har en kontaktperson som handlägger inkomna ärenden.

Som beställare är det viktigt att ha en dialog med leverantören om hur man som kund prioriteras i en krissituation samt vilka möjligheter det finns att påverka denna prioritering. Leverantörer har ofta en prioritetsordning bland sina kunder, denna är dock sällan öppen och hur leverantören prioriterar framkommer först under, eller efter, en krissituation.

Viktigt är därmed att få leverantören att förstå vilken typ av verksamhet man driver och vilka konsekvenser ett avbrott i tjänsten får. Särskilt viktigt är detta om man driver samhällsviktig verksamhet, så att leverantören förstår omfattningen av de totala konsekvenser ett avbrott i verksamheten får.

Kontinuitetshantering och kontinuitetsplaner

Krav bör ställas på att leverantörer ska arbeta med kontinuitetshantering för kritiska verksamheter som outsourcats dit. Leverantörerna bör även ha säkerställt kontinuiteten för eventuella andra delar av dess verksamhet som vid avbrott kan påverka beställarens verksamhet.

Exempel på krav i relation till kontinuitetshantering kan vara att leverantörerna har genomfört processkartläggningar där kritiska delar av verksamheten identifierats, att maximalt tolerabel avbrottstid har identifierats och att kontinuitetsplaner för kritiska processer har tagits fram och regelbundet testas.

Med fördel ställs även krav på att beställaren får ta del av kontinuitetsplanerna och testresultat, detta även hos leverantörens underleverantörer.

Övningar och tester

Beställaren bör ställa krav på att leverantörer regelbundet genomför strukturerade övningar och tester av sina system och rutiner. Dessutom bör det kravställas att resultaten inklusive eventuella åtgärdsplaner delges beställaren. Övningar och tester kan genomföras på flera olika nivåer, bland annat genom:

- Övning av personal för att säkerställa kompetens och öka erfarenheter.
- Skarpa tester för att testa leverantörens kritiska system, processer och beroenden och utröna hur länge leverantören kan klara sig utan dessa utan att det påverkar berörda aktörer i större omfattning. Detta kan göras till exempel genom test av alternativt driftställe samtidigt som ordinarie verksamhet fortgår på ordinarie plats eller genom test av reservkraft för att säkerställa att diesel räcker enligt utlovat.
- Genomgång av checklistor och rutiner.

Övningars och testers frekvens och omfattning bör också beskrivas i avtalet. De finansiella aktörerna kan därtill ställa krav på att gemensamma övningar ska genomföras, det vill säga övningar där både finansiella aktörer och leverantörer deltar. Detta för att testa bland annat samverkan, kommunikationsvägar och informationsdelning. Slutligen bör beställaren också kräva att leverantören bidrar med stöd/information till övningar och tester som utförs av beställaren själv, men som berör den outsourcade verksamheten.

Tillsyn och revision

Krav bör formuleras i avtalet om att beställaren får genomföra granskningar och revisioner av leverantörens system, processer, rutiner, eller leverantörens uppfyllnad av andra delar av avtalet. Granskningen av avtalet kan och bör ske i flera dimensioner, med fokus på exempelvis struktur, process och resultat.

På strukturnivå granskas exempelvis de resurser som använts medan processnivån granskar hur dessa använts. Resultatnivån granskar avslutningsvis det resultat som uppnåtts.

Granskningar och revisioner kan antingen genomföras av beställaren själv eller av en tredje part som är betrodd av både leverantören och beställaren. En beställare kan med fördel avtala om att det är den egna organisationen som står för val av part för revision samt för egna platsbesök. Även när revision och annan granskning görs av extern part är det av vikt att inkludera dess regelbundenhet i avtalet.

I tillägg ska det vara möjligt för Finansinspektionen att genomföra tillsyn av den verksamhet som läggs ut. I de fall där leverantörskedjor används bör revision även vara möjlig att genomföra hos underleverantörer. Därtill bör beställaren avtala om att ta del av resultat från de granskningar och revisioner som leverantören själv genomför.

Delgivning av analyser

Det får antas att samtliga leverantörer regelbundet följer upp och analyserar sitt övergripande kontinuitets-, risk- och säkerhetsarbete. Beställare bör begära att få ta del av de sammanställningar som berör den outsourcade verksamheten, exempelvis i form av resultat från riskanalyser eller revision av kontinuitetsarbetet. På så sätt kan beställaren aktivt påverka dess leverantörer inom områden där risk- eller kontinuitetsarbetet inte är tillräckligt. Beställaren bör därtill kravställa att leverantören skriftligt redogör för hur de uppfyller de krav som fastställts i avtalet och hur ofta denna rapportering ska ske.

Sanktioner och hävning av avtal

För att skydda beställaren och för att motivera leverantören att uppfylla överenskomna servicenivåer är det viktigt att avtalet även specificerar villkoren för händelser då leverantören misslyckas att uppfylla de avtalade kraven. Då åsidosättanden kan bero på flera orsaker är det viktigt att beställaren i dialog med leverantören tydligt klargör vad som innebär åsidosättande av avtal och det är även viktigt att avtalet tydliggör vilka fall som avser ”force majeure” och vilka som inte gör det. Vid större avvikelser eller avbrott kan det vara svårt att påvisa vilken skada som åsamkats, därför är det en god idé att på förhand definiera vilka sanktioner som bör gälla.

Sanktioner vid åsidosättande kan definieras på flera olika sätt, exempelvis genom en direkt finansiell sanktion eller genom krediter för framtida leveranser av den berörda tjänsten. Vid sådana avsteg som leverantören kan åtgärda inom en rimlig tidsperiod är det naturligt att eftersträva en rättelse av avvikelserna i ett första steg. Vite kan i ett nästa steg användas som en påtryckning på leverantören i syfte att åstadkomma en rättelse. En hävning av ett avtal kan ses som en sista utväg vid grova och upprepade överträdelser.

Tips för genomförande:

- Ett bra verktyg som kan användas vid avtalsskrivning om olika sanktioner och dess eskalering är Kammarkollegiets vitesmodell.* Vitesmodellen ger beställaren styrmedel mot leverantören och utgår ifrån de servicenivåer som beställaren förväntar sig att leverantören ska svara mot. I modellen används en maximal procentsats för vite som varierar med ersättningens storlek. För en outsourcad verksamhet med två KPI:er och en maximal vitesprocentsats om 20%, skulle en beräkning av vite kunna se ut enligt följande:

Exempel – Vitesberäkning:

KPI 1 – viktprocent:	10 %
KPI 2 – viktprocent:	10 %
Summa månatlig vitesprocent:	20 %
Fakturerat belopp:	200 000
Vitesbelopp:	40 000

Ett annat verktyg som kan användas hävstång för att säkerställa att leverantören följer sina åtaganden kan vara att i avtalet definiera en möjlighet att gå över till en annan leverantör om avtalet inte följs. Avtalet kan exempelvis ge respektive part friheten att bryta avtalet då motparten ”grovt åsidosatt sina åtaganden”. Viktigt är då att avtalet även definierar vilka händelser som detta inkluderar.

Möjlighet till omförhandling och återtagning av verksamhet

Leverantörsavtal medför ofta långa bindningstider och/eller uppsägningstider. Sådana villkor gör det svårt att byta leverantör eller omförhandla befintliga avtal. Beställare bör därför säkerställa att avtalet inte utgör ett hinder för omförhandling eller byte av leverantör inom en rimlig tidsperiod, genom att noga utvärdera de villkor avseende bindningstider och uppsägningstider som erbjuds redan vid avtalsskrivningen.

Avtalet kan med fördel precisera regelbundna tidpunkter för omförhandling av avtal. Det ligger i såväl leverantörens som beställarens intresse att möjliggöra omförhandling av avtal då beställarens behov kan förändras över tid. En skrivelse i avtal kan exempelvis reglera att omförhandling av avtal görs en gång per år eller en gång vartannat år.

Möjligheten att ta tillbaka verksamhet om samarbetet fallerar bör inkluderas i avtalet. Exempelvis vid obestånd eller då det finns anledning att misstänka det. I de fall då avtalet hävs och den outsourcade verksamheten avvecklas eller återtas i egen regi bör en plan för avveckling finnas. I Finansinspektionens föreskrifter preciseras att avvecklingsplaner ska finnas samtidigt som föreskrifterna inte omfattar instruktioner om hur planerna ska formuleras. I avtalet med leverantören gäller det därför att fastställa vilket ansvar som gäller då ett samarbete avslutas samt hur tjänsten ska återtas och inom vilket tidsperspektiv.

Avtalet bör avspegla vad som förväntas av leverantören då outsourcingavtalet löper ut eller avslutas, exempelvis i form av vilken information som ska överlämnas eller vilka resurser och vilken kompetens som leverantören ska tillhandahålla under avvecklingsperioden. I avtalet kan även framgå att leverantören åtar sig att vara behjälplig vid förflyttning av tjänsten till annan part samt att inte blockera eller förhindra förflyttningen på något sätt. I vissa fall kan det även vara aktuellt att precisera vilka resurser som ska flyttas tillbaka.

För it-relaterade verksamheter kan det i detta sammanhang vara av vikt att definiera att resurser/tillgångar som utvecklats under tiden den outsourcade tjänsten löpt ska flyttas tillbaka i dess uppdaterade form.

För att säkerställa att den tid för avveckling som återges i avtalet är realistisk kan workshops anordnas med leverantören där avvecklingen diskuteras utifrån olika scenarier. Exempelvis kan det vid dialog med leverantören uppdagas att avvecklingen tar längre tid än vad som beskrivs i det ursprungliga avtalet. Mer om vad en beställare bör tänka på vid omförhandling och avveckling av outsourcad verksamhet presenteras i kapitel 6.

Flexibilitetsklausuler

Som påpekats tidigare förändras omvärlden, vilket kan kräva en regelbunden och eventuellt även en kontinuerlig anpassning av tjänster och härmed en flexibilitet hos leverantören som kan bli kostsam ur ett outsourcingperspektiv.

Med bakgrund av detta kan så kallade flexibilitetsklausuler användas, vilka underlättar anpassningen till förändrade omständigheter. Dessa bör dock ur ett kontinuitetsperspektiv användas med viss försiktighet, där beställaren säkerställs tolkningsföreträde.

G.4. Uppföljning och samverkan

För att säkerställa att verksamheten ligger i linje med beställarens behov förutsätts en fungerande samverkan mellan leverantören och beställaren samt att den outsourcade verksamheten följs upp och utvärderas regelbundet.

Kapitlet beskriver områden som är viktiga att beakta under gällande avtal. Genom en fungerande samverkan och en regelbunden och tydlig uppföljning läggs även grunden för en god kontinuitetshantering i förhållande till den outsourcade verksamheten.

Löpande samverkan och uppföljning

Beroende på vilken verksamhet som outsourcats, exempelvis storlek och hur kritisk verksamheten är, samt hur många olika leverantörer som används kan olika leverantörsstrategier komma att bli aktuella.

Leverantörsrelationer kan vara ytliga såväl som djupa, där ytliga relationer inte behöver innehålla någon löpande samverkan eller dialog utan endast uppföljning på exempelvis årsbasis enligt kraven i avtalet. Djupa leverantörsrelationer kan inkludera löpande (t.o.m. daglig) samverkan i upprättade forum med utpekade ansvariga från både beställare och leverantör. En djup relation med leverantör är att föredra om det är en kritisk verksamhet som outsourcats. Om många leverantörer används blir denna typ av leverantörsstrategi dock kostsam. En avvägning bör därför göras mellan att ha många leverantörer för att sprida riskerna men samtidigt minska möjligheterna till täta leverantörssamarbeten, eller att ha få leverantörer där samverkan sker mer kontinuerligt och på olika nivåer. Att använda sig av få leverantörer och samtidigt ha ytliga relationer med dessa bör endast vara ett alternativ för outsourcing av tjänster som inte är av kritisk betydelse för beställaren eller dess intressenter.

Samverkansforum för löpande dialog och uppföljning

Eftersom de finansiella aktörerna i stor utsträckning utför samhällsviktig verksamhet bör djupa leverantörsrelationer med löpande dialog mellan beställare och leverantör oftast vara att föredra. Ett sätt att uppnå tätt samarbete med leverantören är att upprätta samverkansforum där de åtaganden som fastställts genom avtalet följs upp.

Samverkansforumen kan exempelvis bestå i regelbundna möten där olika problemställningar fångas upp. Forumen kan arrangeras på strategisk eller operativ nivå och kan även anordnas för enskilda sakfrågor som anses prioriterade för den outsourcade verksamheten, exempelvis kontinuitetsfrågor.

Vid forumen bör de åtaganden som fastställts genom avtalet följas upp. Mötena bör formaliseras där respektive parts ansvar framgår tydligt. Som stöd vid uppföljning framtas med fördel olika checklistor.

Det är även viktigt att säkerställa att upprättade forum faktiskt fungerar. Ett stöd på vägen kan vara att utforma en samverkansmanual som instruerar i hur forumen ska hanteras. I manualen bör även kontaktuppgifter till parter inom den externa leverantören anges tydligt, samt vem inom den egna verksamheten som ansvarar för kontakten med leverantören i olika ärenden.

Uppföljningen som genomförs vid samverkansforumen bör grundas i en strategi för uppföljning som upprättas hos beställaren. Fokusområden för uppföljning kan med fördel skifta från år till år utifrån en långsiktig och gemensamt fastställd plan. Att, som tidigare påpekats, regelbundet ta del av resultat från leverantörens övningar och genomföra gemensamma övningar är också att föredra. Leverantören bör regelbundet avlämna analyser och rapporter till beställaren, i enlighet med vad som föreskrivits i avtalet. Analyserna och rapporterna bör bestå av skriftliga underlag då dokumentationen underlättar beställarens uppföljning. De skriftliga underlagen bör också kompletteras med muntliga redogörelser vid upprättade samverkansforum.

Checklistor och nyckeltal underlättar kontrollverksamheten

Det är viktigt att genomgående säkerställa att leverantören lever upp till de krav som preciserats i avtalet. Som beskrivet i avtalskapitlet är det därför av stor vikt att de krav som ställts i avtalet är möjliga att följa upp och mäta. För de aktörer som väljer att outsourca är det därmed viktigt att säkerställa att det finns tydliga interna rutiner och instruktioner på plats som möjliggör och underlättar uppföljning och kontroll. Detta är även ett krav från Finansinspektionens sida. Nyckeltal och KPI:er kan också användas inom kontrollverksamheten.

Från den beställande organisationen läggs resurser på att följa upp leverantörernas agerande. Det är därför av vikt att beställarorganisationen har en tydlig fördelning av ansvar för kravuppföljning inom den egna organisationen. Att outsourca en tjänst innebär att flera olika parter inom den egna organisationen är ansvariga för olika delområden, såväl för att upprätthålla relationen med leverantören som att kontrollera att avtalet efterlevs. Det kontraktuella ansvaret såväl som det driftsmässiga avtalet bör vara tydligt inom beställarens interna organisation och det bör finnas framtagna interna rutiner och stödmaterial, exempelvis checklistor. Checklistor kan utarbetas utifrån de krav som formulerats i avtalet, exempelvis för att säkerställa att leverantören har en kontinuitetsplan på plats. Dessa checklistor bör kontinuerligt följas upp och uppdateras.

Det finns även en revisionsstandard (ISACA) som används av externa revisorer för att granska leverantörer; denna handlar både om hur de fysiska anläggningarna ser ut och hur leverantörens verksamhet som helhet sköts. Vid uppföljningen kan med fördel den företagsbesiktning som genomfördes innan avtal om outsourcing slöts ses över eftersom ägarförhållanden, samhällets förväntningar (t.ex. etiska regler) och dylikt kan förändras över tid.

Samverkan och uppföljning vid störningar och avbrott

Beställaren bör informeras i de fall där leverantören eskalerat till kris och bör även kontaktas för att lämna sitt samtycke innan återställning av verksamheten efter inträffad kris. Under ett avbrott bör beställaren även få kontinuerlig information kring händelseförloppet, påverkan på den outsourcade verksamheten och hur leverantören arbetar för att återupprätta verksamheten. Incidentanalyser, från inträffade störningar och avbrott, bör komplettera den regelbundna rapporteringen, där beställaren bör upprätta en rutin för att säkerställa att identifierade brister åtgärdats.

G.5. Utveckling och avveckling

I vissa fall kan det vara motiverat att bryta avtalet helt med leverantören. Avveckling av en tjänst bör dock noga vägas mot vad det innebär att byta leverantör eller att ta tillbaka de utlagda tjänsterna internt. Vid byte av leverantör behöver mycket arbete genomföras såsom ny behovsanalys och uppdatering av krav. Därtill måste revision av den tidigare dokumentationen för den outsourcade verksamheten göras igen.

Kapitlet beskriver två områden som är viktiga att beakta vid omförhandling av avtal eller vid avveckling av outsourcad verksamhet: utvärdering och erfarenhetsåterföring.

Utvärdering

Att tillvarata lärdomar från samarbetet med leverantören är av vikt oavsett om avtalet löpt ut och är föremål för omförhandling, eller om den outsourcade verksamheten ska avvecklas eller återtas. Genom att tillvarata erfarenheter från samverkan med leverantören kan framtida kravställningar anpassas så att de är realistiska och att de svarar mot beställarens verksamhetsbehov.

Erfarenheter kan tillvaratas från genomförda samverkansforum såväl som från en självutvärdering kring hur verksamheten strukturerats, hur verksamheten utförts och vilket resultat som valt tillvägagångssätt medfört. Samtliga åtaganden som stipulerats i det tidigare avtalet bör även ses över och utvärderats, med uppgift att se om något åtagande bör utvecklas.

Vid tid för omförhandling eller byte av leverantör är det även av vikt att återgå till den interna analysen som gjordes innan beslut om outsourcing fattades. Där bör undersökas om någon/något av de förutsättningar och behov som lade grund för avtalsskrivningarna förändrats och om avtalsskrivningarna därmed bör utvecklas. Exempelvis kan behov av kontinuitet i tjänsten förändras om en resurs eller kompetenstillgång krävs under en specifik tid om dagen/månaden/året.

Tips för genomförande:
- Exempelfrågor som kan ställas vid utvärderingen:
    - Vad fungerade bra?
    - Vad fungerade sämre?
    - Vilka var de initiala behoven och förutsättningarna?
    - Har behoven och förutsättningarna förändrats?

Erfarenhetsåterföring

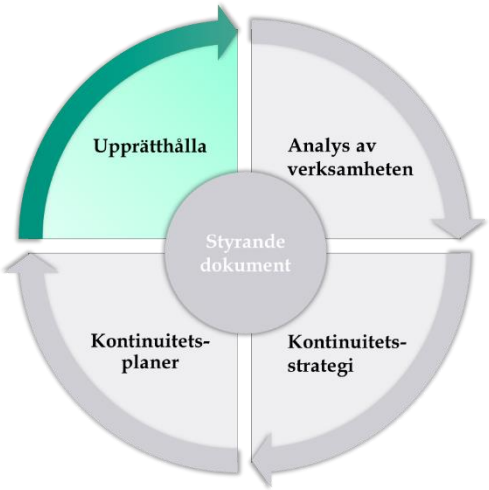
Det är viktigt att komma ihåg att det inte alltid är helt enkelt att återta eller flytta verksamhet som en gång outsourcats. Vid återtagning av verksamheten kan exempelvis nyrekryteringar och omfattande nyinvesteringar utgöra en förutsättning för att återtagandet av verksamheten ska kunna genomföras.

Appendix H - Test av kontinuitetsplaner

H.1. Introduktion

Appendix H – Test av kontinuitetsplaner (i fortsättningen nämnd Appendix H) ger utifrån god praxis finansiella aktörer en vägledning i hur de kan genomföra tester av sina kontinuitetsplaner. Appendix H ska ge ett stöd i hur tester av verksamhetens kontinuitetsplaner kan planeras, genomföras och utvärderas.

Den process för kontinuitetshantering som presenteras i detta appendix följer processen som presenteras i standarden ISO 22301 om ledningssystem för kontinuitetshantering [72]. Processtegen är således de samma som de processteg som presenteras i vägledningens huvuddokument, med skillnaden att detta appendix ger fördjupad vägledning för test av verksamhetens kontinuitetsplaner. Appendix H tar utgångspunkt i processen för verksamhetens kontinuitetshantering som beskrivs i vägledningens inledande avsnitt. I avsnittet beskrivs hur genomförandet av tester är en del av arbetet med att *Upprätthålla* kontinuitetsförmåga, se *Figur 1*. Appendix H utgår från denna process, samt de termer och begrepp som beskrivs i huvuddokumentet och övriga appendix.



Test av kontinuitetsplaner är en del av arbetet med att upprätthålla kontinuitetsförmåga.

I FSPOS vägledning *6 steg till bättre övningar*[73] beskrivs en stegvis metod för planering, genomförande och utvärdering av övningar. Samma metod ligger till grund för upplägget i Appendix H då även tester kan utföras enligt dessa steg.

[72] *SS-EN ISO 22301 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Krav.*

[73] *FSPOS - 6 steg till bättre övningar.*

Dokumentets avgränsningar

Appendix H fokuserar på test av verksamhetens kontinuitetsplaner. I viss utsträckning kan beskrivna metoder och arbetssätt även appliceras vid test av it-verksamhetens återställningsplaner för system/tjänster. Men för att erhålla ett komplett stöd för test av it-verksamhetens återställningsplaner krävs ett mer fördjupat metodstöd.[74]

Förklaring till begreppen övning respektive test

Begreppen *övning* och *test* används såväl inom kontinuitetshantering som inom andra områden. I detta appendix beskrivs de två begreppen utifrån att de har skilda, men kompletterande mål och syften, se *Figur 2*. Övningar och tester kan genomföras i kombination eller som separata aktiviteter. Framtagna kontinuitetsplaner och dess kontinuitetslösningar bör både övas och testas för att säkerställa organisationens förmåga att effektivt hantera omfattande störningar eller avbrott.

Övning

Övning är en aktivitet för att träna, bedöma, tillämpa och utveckla organisationers förmåga och färdigheter. Övningar utgår från ett lärande och utbildande perspektiv, med fokus på att bygga upp en förmåga hos individer eller grupper snarare än att verifiera enskilda processer. Däremot kan en övning ha testande inslag. Detta styrs framför allt av hur målen och mätpunkterna för övningen definieras. Övningar kan till exempel genomföras för att klargöra roller och ansvar, för att förbättra samordning och kommunikation, samt för att identifiera resursbrister och förbättringsmöjligheter.[75]

Test

Test är en aktivitet för att bestämma helhet, kvalitet eller riktighet i det testade objektet. Den tydligaste skillnaden mellan övningar och tester är att tester innefattar moment av prövning och mätning, utifrån en förväntan om att det/de testade objekten antingen ska godkännas eller underkännas inom ramen för uppsatta mål och mätpunkter.[76] Tester används för att verifiera en eller flera utpekade förmågor eller planer, exempelvis för att bedöma om befintlig förmåga är tillräcklig eller om framtagna kontinuitetsplaner fungerar som avsett.

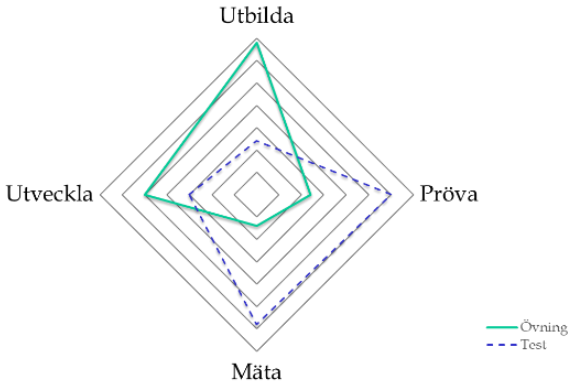
---

[74] *Detta appendix kan komma att kompletteras med ett fördjupat stöd avseende test av it-verksamhetens återställningsplaner för system/tjänster.*

[75] *ISO 22300 - Security and resilience – Vocabulary.*

[76] *ISO 22300 – Security and resilience – Vocabulary.*

En förutsättning för att kunna genomföra tester är att det finns etablerade förmågor och framtagna kontinuitetsplaner som går att verifiera. Tester kan även innefatta ett mått av lärande och utbildning då målgruppen för testet med stor sannolikhet ökar sin medvetenhet och förmåga under själva genomförandet.



Övningar fokuserar främst på utveckling av organisationens förmåga ur ett lärande och utbildande perspektiv. Tester fokuserar främst på att verifiera planer och förmågor genom att pröva och mäta utifrån ett förväntat resultat.

H.2. Test av kontinuitetsplaner

Förenklat kan kontinuitetshantering beskrivas som den process som säkerställer att organisationen kan driva sin kritiska verksamhet på tolerabel nivå, oavsett vilka störningar som inträffar. Med detta menas att organisationen minskar sin sårbarhet och ökar sin motståndskraft mot olika händelser som kan påverka dess mest kritiska verksamhet. Genom arbetet med kontinuitetshantering skyddas organisationens intressenter, rykte, varumärke och värdeskapande aktiviteter. Ett resultat av arbetet med kontinuitetshantering är att rutiner tas fram för hur verksamhetens kritiska processer ska kunna upprätthållas vid störningar eller avbrott, så kallade kontinuitetslösningar. Dessa kontinuitetslösningar dokumenteras i verksamhetens kontinuitetsplaner. Kontinuitetslösningar kan beskrivas på följande sätt:

- På olika nivåer: kontinuitetslösningar kan beskrivas för processen som helhet eller för de stödjande aktiviteter eller resurser som är kritiska för processens funktionalitet.
- På olika sätt: kontinuitetslösningar kan bestå av flera delar enligt nedan:
    - Reservrutiner - *Hur arbetar vi på alternativa sätt under ett avbrott?*
    - Återställningsrutiner - *Hur återställer vi den kritiska resursen efter ett avbrott?*
    - Återgångsrutiner - *Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen?*

I nedan redogörs ett exempel på en kontinuitetslösning för den kritiska processen kredithantering. I kontinuitetsplanen beskrivs kontinuitetslösningen i form av en instruktion för hur avdelningen kan arbeta på alternativa sätt under ett avbrott (reservrutin), hur arbetet med att återställa systemet hanteras (återställningsrutin) samt instruktion för hur verksamheten kan återgå till normalläge när systemet är tillgängligt igen (återgångsrutin).

Kritisk process: Kredithantering
Scenario: System X är otillgängligt

Reservrutin:
1. Kontakta berörda avdelningar:
- Utlåning
- Kreditrisk
- Utbetalningar

2. När berörda avdelningar kontaktas, försäkra att följande kommuniceras:
- Information från it gällande förväntad återställningstid och berörda processer.
- Använd manuella rutiner enligt beskrivning i rutindokument.

Återställningsrutin:
1. Inled dialog med it-avdelningen för att kontinuerligt inhämta information om:
- När förväntas systemet vara återställt?
- Är hela systemet nere, eller fungerar vissa delar av systemet?
- Finns alternativa sätt att inhämta data för verksamheten?

2. När systemet är återställt, verifiera att samtliga funktioner fungerar och all data i systemet är intakt.

Återgångsrutin:
1. Informera berörda avdelningar att verksamheten kan återgå till normal verksamhet.
2. Samla in all nödvändig information om:
- Vilka störningar i verksamheten som har uppstått och dess omfattning.
- Bedömd påverkan på kund.

3. Prioritera nödvändiga aktiviteter för att återgå till normal verksamhet och hantera påverkan på kund.

Nödvändiga kontaktuppgifter:
Ansvarig för Utlåning (se bilaga 3).
Ansvarig för Kreditrisk (se bilaga 3).
Ansvarig för Utbetalningar (se bilaga 3).
It-avdelningen (se bilaga 3).

Exempel på kontinuitetslösning.

För att verifiera kontinuitetsplanernas helhet, kvalitet och riktighet bör de regelbundet testas. Genom tester kan verksamheten bland annat säkerställa att befintliga kontinuitetslösningar är tillräckliga för att möta de tidskrav som definierats. Tester kan genomföras i större skala för en eller flera av verksamhetens kritiska processer, eller i mindre skala för enskilda kontinuitetslösningar. Baserat på testernas resultat bör planerna löpande revideras och uppdateras för att vara relevanta. Se vidare avsnitt *I.4. Planering, genomförande och utvärdering av test* för stöd i hur tester kan utföras.

Test av kontinuitetsplaner kan och bör innefatta samtliga av kontinuitetslösningarnas tre delar (reservrutiner, återställningsrutiner, återgångsrutiner). Detta bör göras antingen i gemensamma tester där flera målgrupper deltar, eller i separata tester för specifika målgrupper. Vidare bör underliggande beroenden, såsom it eller externa leverantörer, inkluderas i tester av verksamhetens kontinuitetsplaner i syfte att säkerställa ändamålsenlighet genom hela beroendekedjan.

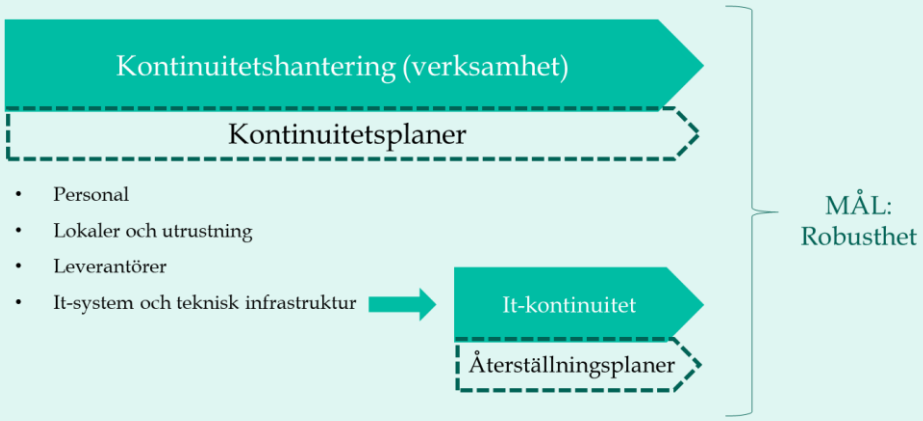
Test av kontinuitetsplaner kan bland annat syfta till att:

- Utvärdera organisationens förmåga att tillämpa kontinuitetslösningarna utifrån definierade tidskrav (*Maximalt tolerabel avbrottstid* för kritiska processer och aktiviteter samt *Mål för återställningstid* för kritiska resurser). Går tidskraven att möta?
- Kontrollera att de dokumenterade rutinerna i kontinuitetsplanen är relevanta, fullständiga och aktuella.
- Validera kontinuitetslösningarna utifrån de antaganden och förutsättningar som lösningarna bygger på.
- Kontrollera att resurser och kritiska beroenden som stödjer kontinuitetslösningarna är tillräckliga och funktionella.
- Utvärdera och stärka leverantörers kontinuitets- och återställningsförmåga.
- Identifiera områden för förbättringar eller avsaknad av information.
- Validera kompetens hos personal.
- Öka medvetenheten om kontinuitetsarbetet i organisationen.

Test av it-verksamhetens återställningsplaner

Genom kontinuitetshantering identifieras verksamhetens 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 tidskrav som verksamheten definierat för dessa resurser utgör viktiga ingångsvärden för it-verksamhetens kontinuitetsarbete. It-kontinuitetshantering syftar till att skapa robusthet och redundans i it-verksamhetens kritiska system/tjänster, baserat dels på kravställningar från verksamheten och dels på it-verksamhetens egna behov och analyser.[77] I figuren illustreras hur verksamhetens kontinuitetshantering och it-kontinuitetshantering tillsammans bidrar till organisationens robusthet.



Verksamhetens och it-verksamhetens arbete med kontinuitetshantering bidrar tillsammans till organisationens robusthet.

Kontinuitetslösningar för it-verksamheten beskrivs i specifika återställningsplaner för system/tjänster.[78] I återställningsplanerna beskrivs konkreta och tydliga kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner för var och en av de identifierade kritiska it-resurserna. Lösningarna kan exempelvis handla om back up-hantering, spegling av viktiga data samt incidentrapportering och incidenthantering. It-verksamhetens återställningsplaner för system/tjänster bör, liksom verksamhetens kontinuitetsplaner, testas minst årligen. Exempel på tester för it-resurser kan vara failover-tester eller återläsningstester.

[77] *Se vidare Appendix F – Kontinuitetshantering för it-verksamheten.*

[78] *Liksom i Appendix F – Kontinuitetshantering för it-verksamheten benämns i detta appendix it-verksamhetens återställningsplaner för system/tjänster. Andra vanliga benämningar är disaster recovery-planer eller back up-planer. Notera att återställningsplaner även ska upprättas för verksamhetens kritiska processer enligt FFFS 2014:4. It-verksamheten kan då även utgöra kritiska verksamhetsprocesser i verksamhetens kontinuitetsplaner.*

H.3. Skapa en teststrategi och testplan

Teststrategi

För att säkerställa relevanta tester bör en teststrategi upprättas som tydligt visar hur organisationen över tid säkerställer förmåga att upprätthålla sina kritiska processer. Teststrategin bör svara på vad organisationen vill uppnå och varför, hur organisationen ska nå dit, samt hur utvecklingen ska mätas. En beskrivning över hur organisationen ska genomföra tester tillsammans med it-verksamheten bör även inkluderas i teststrategin för att på så vis koordinera hur tester genomförs inom organisationen (se avsnitt test av it-verksamhetens återställningsplaner på föregående sida). Sammantaget bör teststrategin inkludera en beskrivning över hur planerade tester ska bidraga till organisationens förmågeutveckling.

Teststrategin kan vara en del av verksamhetens övergripande kontinuitetsstrategi, vilket beskrivs i huvuddokumentets avsnitt 3.3 samt i *Appendix C – Kontinuitetsstrategi.* Teststrategin kan också vara ett separat dokument där ingångsvärden och utgångspunkter för test av kontinuitetsplaner beskrivs mer utförligt. Teststrategin bör vara förankrad och godkänd av ledningen.

Nedan presenteras ett antal olika områden som kan vara relevanta att inkludera i en teststrategi.

Prioritering av processer för test

En beskrivning över hur verksamhetens processer har prioriterats för test kan ingå i teststrategin. Utifrån denna prioritering kan olika krav, exempelvis avseende frekvens eller omfattning för tester definieras.

I nedan utgör maximalt tolerabel avbrottstid för processen grunden för prioritering. Att prioritera processer utifrån maximalt tolerabel avbrottstid är vanligt. Även andra kriterier, såsom riskbedömning för processernas stödjande resurser eller processernas affärsbetydelse kan ligga till grund för prioritering.

Prioritering / Krav	**4 Liten betydelse**	**3 Medelhög betydelse**	**2 Stor betydelse**	**1 Avgörande betydelse**
Maximalt tolerabel avbrottstid för processen	*> 5 dagar*	*2-5 dagar*	*2-24 timmar*	*0-2 timmar*
Krav på test	*Kontinuitetsplanen med tillhörande lösningar bör testas minst 1 gång vartannat år genom dokumentationsgenom-gång.*	*Kontinuitetsplanen med tillhörande lösningar testas minst 1 gång årligen genom dokumentationsgenom-gång eller skrivbordsövning.*	*Kontinuitetsplanen med tillhörande lösningar testas minst 1 gång årligen genom skrivbordsövning eller annan testtyp.*	*Kontinuitetsplanen och tillhörande lösningar testas minst 2 gånger årligen genom skrivbordsövning, simulering eller annan testtyp.*

Exempel på modell för prioritering av processer för test.

Förmågeområden

För att möjliggöra effektiva tester som ger önskad effekt bör ett antal förmågeområden definieras. Alla relevanta förmågeområden för respektive process bör testas över tid för att säkerställa heltäckande och funktionella kontinuitetsplaner.

I tabellen nedan ges exempel på förmågeområden som kan vara aktuella att inkludera i en teststrategi. Områdena är till viss del överlappande men även kompletterande. Att ha definerade förmågeområden i teststrategin underlättar också framtagandet av mätpunkter för varje enskilt test.

Förmågeområde	Beskrivning
Kommunikation	Avser förmågan att kommunicera, såväl internt som externt, vid störningar och avbrott i kritiska processer.
Kompetens	Avser berörda funktioners förmåga att följa rutiner beskrivna i kontinuitetsplaner.
Ledning	Avser planernas ändamålsenlighet avseende rutiner för larmning, initiering av kontinuitetshantering samt eventuella andra åtgärder i syfte att åstadkomma inriktning och samordning.
Logistik	Avser olika typer av logistik-/leverantörslösningars möjlighet att upprätthållas vid störningar eller avbrott.
Medvetenhet	Avser medvetenhet om kontinuitetshantering samt gällande rutiner. Olika krav på medvetenhet bör ställas på individer/grupper. Exempelvis: • Processägare: bör ha full insyn i kontinuitetsplanerna. Processägaren är ytterst ansvariga för att planerna är ändamålsenliga. • Personer som kan komma att involveras i hanteringen: bör ha en god medvetenhet om sin egen roll och ansvar. • Personer som inte ingår i hanteringen: bör, på en övergripande nivå, ha medvetenhet om verksamhetens kontinuitetshanteringsarbetet samt gällande rutiner vid störningar eller avbrott.
Resurser	Avser möjligheten att kritiska resurser upprätthålls eller återställs som avsett. Gäller såväl personal, system, lokaler, utrustning samt leverantörer.
Samverkan	Avser förmågan att samverka, såväl inom organisationen som med externa aktörer, i syfte att hantera en störning eller ett avbrott i kritiska processer.
Tidskrav	Avser möjligheten att möta definierade tidskrav på process-, aktivitets- och resursnivå.

Exempel på förmågeområden att testa över tid.

Mognadsnivåer

Teststrategin bör också förklara hur organisationen stegvis ska stärka sin förmåga över tid. För att mäta organisationens mognadsnivå kan en modell likt mognadstrappan användas, se figur nedan. Mognadstrappan, eller annan modell, kan hjälpa till att identifiera eventuella brister i nuvarande teststrategi. Modellen kan även visa på nuvarande mognadsnivå samt utgöra ett bra underlag för beslut om önskad mognadsnivå.[79] Beslut om vilken mognadsnivå organisationen ska befinna sig på bör fattas av ledningen.

Exempel på modell för att mäta nuvarande samt önskad mognadsnivå.

I tabellen nedan ges exempel på hur beskrivningar för varje mognadsnivå (1-4) kan definieras.

Mognadsnivå	Beskrivning
Nivå 1	• Organisationen genomför sällan eller aldrig tester. Tester som genomförs görs ostrukturerat, utan tydliga målsättningar eller mätpunkter. • Kontinuitetsplaner inom organisationen saknas helt eller är bristfälliga.
Nivå 2	• Organisationen genomför tester utifrån en begränsad variation av testtyper. • Genomförda tester utvärderas utifrån målsättningar men dokumentationen och uppföljningen är bristfällig. • Organisationen har upprättade kontinuitetsplaner men är bristfälliga. Planerna uppdateras ej regelbundet.

[79] *ISO 22325 - Krishantering - Vägledning för förmågeutvärdering.*

Nivå 3	• Organisationen har en testsstrategi. • Organisationen genomför tester regelbundet för valda delar av organisationen. • Organisationen använder sig av ett varierat urval av testtyper för att även få in mer avancerade praktiska moment. • Uppsatta testmål utvärderas utifrån fördefinierade mätpunkter för att identifiera förbättringsområden. Resultatet dokumenteras och följs upp. • Organisationen har upprättade detaljerade kontinuitetsplaner för organisationens alla kritiska processer. Planerna uppdateras regelbundet.
Nivå 4	• Tester görs i samverkan med både interna och externa aktörer. Organisationen har en långsiktig teststrategi som tydligt beskriver hur verksamheten ska täcka in samtliga av de kritiska processer som ska testas, under ett bestämt tidsintervall. • Organisationen visar på hög mognadsgrad genom att dra lärdomar av tidigare tester, samt omsätter lärdomar till konkreta förbättringsåtgärder för att vidareutveckla och upprätthålla sin förmåga. • Organisationen behärskar alla former av testtyper och använder också resultatet från tidigare tester som ett ingångsvärde i testplaneringen. • Organisationen har upprättade detaljerade kontinuitetsplaner för organisationens alla kritiska processer. Planerna uppdateras regelbundet.

Exempel på definitioner för mognadsnivåer.

Testtyper

I teststrategin beskrivs de testtyper som organisationen avser använda. Valet av testtyper bör anpassas till målgruppens mognads - och ambitionsnivå.

Dokumentationsgenomgångar och skrivbordsövningar lägger fokus på diskussion, medan andra testtyper i olika grad inkluderar praktiskt testande och verifiering av kontinuitetslösningar. Dokumentationsgenomgångar och skrivbordsövningar har också generellt ett större inslag av övning än test. Dock bör både dokumentationsgenomgångar och skrivbordsövningar inkluderas i teststrategin för att täcka alla av organisationens behov. Skillnaden mellan testtyper rör främst komplexiteten i dess utformning samt dess övergripande syften. För en organisation med låg mognadsnivå eller för nya/uppdaterade rutiner bör tester initialt fokusera på att stärka personalens medvetenhet och förståelse.

Inom ramen för samtliga testtyper kan tester utföras på olika nivåer, d.v.s. tester kan fokusera på att testa kontinuitetslösningar på:

- Processnivå: förmågan att upprätthålla processen på en fastställd, tolerabel nivå eller att alternativa lösningar gör att processen fortfarande kan levereras på en tolerabel nivå. Test av kontinuitetslösningar på processnivå kan innefatta samtliga kritiska aktiviteter i processen och därigenom spänna över ett flertal olika funktioner och arbetsplatser, nationellt eller globalt. Ett exempel kan vara att testa hur en störning påverkar hela kredit- och utlåningsprocessen och alla dess funktioner på ett flertal kontor i Sverige och utomlands. Ett annat exempel kan vara att testa kontinuitetslösningar genom att låta processen i sin helhet utföras av tredje part.
- Aktivitetsnivå: förmågan att upprätthålla kritiska aktiviteter enligt fastställda, tolerabla nivåer eller att alternativa lösningar fungerar ändamålsenligt (exempelvis med stöd av manuella rutiner). Test av kontinuitetslösningar på aktivitetsnivå kan innefatta en eller flera kritiska aktiviteter i processen och därigenom begränsa omfattningen av testet. Exempelvis kan aktiviteterna för ansökan och utbetalning testas, medan resterande aktiviteter testas vid ett annat tillfälle. På så vis kan antalet involverade arbetsplatser och personer under testet begränsas.
- Resursnivå: förmågan hos enskilda resurser att bidra till möjligheten att upprätthålla de kritiska processerna. Även resurser som utgör kritiska beroenden till varandra bör inkluderas, såsom datahallar och externa leverantörer. Test av kontinuitetslösningar på resursnivå kan därför innefatta både test av enskilda resurser (exempelvis genom failover-test, flytt till reservarbetsplats, samt användning av fysiska nycklar istället för elektroniska lås) eller test av kontinuitetslösningar som innefattar beroenden mellan kritiska resurser (exempelvis ett it-systems beroende till personal eller externa leverantörers beroende av datakommunikation och elförsörjning).

Dokumentationsgenomgång

En dokumentationsgenomgång, även kallad *walk-through*, syftar till att på ett strukturerat sätt identifiera flaskhalsar och andra svagheter i kontinuitetsplanerna. Deltagare granskar och diskuterar stegvis i grupp varje del av kontinuitetsplanerna. På så vis kan eventuella brister i rutiner eller kontinuitetslösningar identifieras.

En dokumentationsgenomgång är ett lämpligt första steg vid introduktion av en ny plan eller vid uppdateringar av rutiner. Dokumentationsgenomgångar genomförs under ledning av planägare eller utsedd facilitator med stöd av framtagen checklista.

För genomförandet av en dokumentationsgenomgång behövs inget scenario. Istället leds gruppens diskussioner med stöd av framtagen checklista och frågeställningar.

Lämpliga förmågeområden att testa vid dokumentationsgenomgång: kompetens, medvetenhet och resurser.

Skrivbordsövning

Skrivbordsövningar lämpar sig väl för organisationer med låg mognadsnivå, samt som ett bra komplement för mer mogna organisationer. Skrivbordsövningar kan även genomföras för nya eller uppdaterade planer. Under skrivbordsövningar diskuterar deltagarna planernas ändamålsenlighet utifrån ett eller flera scenarier som påverkar en eller flera planer samtidigt. Skrivbordsövningar har framförallt ett lärande syfte, där deltagarna i lugn och ro ges möjligheten att reflektera och diskutera utifrån olika scenarier.

En skrivbordsövning bör genomföras under ledning av en facilitator. Övningen kan genomföras med olika svårighetsgrader, allt från ett enkelt scenario till en gradvis eskalering av ett scenario, vars konsekvenser påverkar flera av verksamhetens kritiska processer.

Lämpliga förmågeområden att testa vid skrivbordsövningar: kompetens, medvetenhet och resurser.

Simulering

För en mer mogen organisation kan en simulering vara lämplig. En simulering innebär att deltagarna får ta del av fiktiv scenarioinformation genom olika inspel och förväntas agera på samma sätt som de skulle gjort i en verklig situation. Den fiktiva informationen kan förmedlas med hjälp av ett så kallat motspel. Motspelet har till uppgift att föra scenariot framåt genom att förmedla inspel som på ett realistiskt sätt ska hjälpa till att testa hur processer och resurser fungerar i en realistisk situation. Motspelet leds av en utsedd motspelsledare. Testdeltagarna agerar utifrån den geografiska position som organisationen vanligen utgår från, samt använder de kommunikationsmedel och verktyg som normalt används. En simulering genomförs under kontrollerade former, vilket innebär att deltagarna endast kontaktar andra personer som ingår i testet eller i motspelet. Få fysiska åtgärder vidtas rent praktiskt. Istället simuleras de flesta åtgärder.

En simulering har ett mer testande fokus än en skrivbordsövning, och skarpa testande inslag kan förekomma, exempelvis genom test av manuella rutiner, verifiering av tekniska lösningar eller flytt till reservarbetsplats. För att mäta hur verksamheten klarar av varje steg under testet bör tydliga mätpunkter definieras och följas upp.

Lämpliga förmågeområden att testa vid simuleringar: kommunikation, kompetens, ledning, logistik, resurser, samverkan och tidskrav.

Funktionstest

Funktionstestning syftar till att testa organisationens funktionella enheter, antingen som enskild funktion eller som en del av den kritiska processen. Funktionstester genomförs i syfte att säkerställa att flera organisatoriska enheter fungerar tillsammans under störda förhållanden. Dessa enheter kan tillhöra olika kritiska processer och kan dessutom vara geografiskt skilda.

Tester av planerna görs då delvis skarpt eller i en för testet uppbyggd kontrollerad testmiljö med hjälp av verkliga resurser. Ibland inkluderas även externa leverantörer. Ett funktionstest är utformat för att kunna mäta alla stegen som utförs under testet. Därför bör tydliga mätpunkter definieras för att kunna mäta hur verksamheten klarar varje steg av testet.

En mer avancerad och tidskrävande variant av funktionstestning är parallell funktionstestning, vilket innebär att funktionstestning görs samtidigt som ordinarie verksamhet fortgår. Fördelen med parallell funktionstestning är att denna testtyp möjliggör för verksamheten att testa kontinuitetsplanernas funktionalitet genom att jämföra testdata och verklig produktionsdata. Denna testtyp kräver dock att samtliga rutiner är väl inövade och att samtliga deltagare har god kunskap i kontinuitetsplanerna.

Lämpliga förmågeområden att testa vid funktionstester: kommunikation, kompetens, ledning, logistik, resurser, samverkan och tidskrav.

Fullskaletest

Fullskaletester är den mest omfattande typen av test och innefattar testning av samtliga aspekter av befintliga kontinuitetsplaner. Vid fullskaletester sker ett flertal tester parallellt och bör inkludera så många kritiska processer som möjligt. Ett fullskaletest utförs alltid som ett verkligt realtidstest i produktionsmiljö medan ordinarie verksamhet fortgår. Målet med fullskaletester är primärt att verifiera om kontinuitetslösningarna fungerar som tänkt, samt om dokumentationen är tillräcklig. Sekundärt verifieras också huruvida personalen verkligen kan genomföra det som förväntas av dem inom bestämda tidsintervaller. Precis som vid funktionstester är det viktigt att tydliga mätpunkter definieras för att kunna mäta hur verksamheten klarar varje steg av testet. Omfattande planering är en förutsättning för att kunna genomföra denna typ av test så att den ordinarie verksamheten inte påverkas negativt om något skulle gå fel. Fullskaletester bör lämpligen utföras efter ett eller flera lyckade parallella funktionstester.

Lämpliga förmågeområden att testa vid fullskaletester: kommunikation, kompetens, ledning, logistik, resurser, samverkan och tidskrav.

Testplan

Som komplement till den strategiska och långsiktiga teststrategin bör en specifik testplan tas fram. En testplan bör visa hur respektive identifierad kritisk process löpande ska testas. I testplanen dokumenteras förslagsvis testformat, förmågeområden, prioritering och målgrupp (se mall för testplan). Testplanen kan med fördel vara en del av respektive process kontinuitetsplan, alternativt biläggas kontinuitetsplanen.

Testplanen bör inkludera olika testtyper. Omfattning och frekvens av tester bör kopplas till hur kritisk processen är, eller utifrån annan prioritering som angetts i fastställd teststrategi. Genom att kontinuitetslösningar för de mest kritiska processerna testas mer frekvent och omfattande än de mindre kritiska, kan på så sätt resurser optimeras.

Under hur lång tidsperiod testplanen ska sträcka sig beror till stor del på organisationen och dess ambitionsnivå, men vanligt är att cykeln löper över en 2 - 4 årsperiod. Testplanen bör vara förankrad och godkänd av ledningen. Planen bör också revideras varje år eller vid behov.

MALLAR FÖR GENOMFÖRANDE
- TESTPLAN -

	Kvartal	Process	Testtyp	Förmågeområden	Prioritering	Målgrupp	Ansvarig	Kommentar
År 1	Q1	Utbetalning av pensioner	Simulering	Ledning Samverkan Tidskrav	Avgörande betydelse (1)			
		Kundservice	Skrivbordsövning	Kompetens Medvetenhet	Stor betydelse (2)			
		Bolån	Funktionstest	Tidskrav Logistik	Avgörande betydelse (1)			
	Q2							
	Q3							
	Q4							
År 2	Q1							
	Q2							
	Q3							
	Q4							
År 3	Q1							
	Q2							
	Q3							
	Q4							

H.4. Planering, genomförande och utvärdering av test

Som beskrivs i inledningen utgår Appendix H från FSPOS vägledning *6 steg till bättre övningar.*[80] I detta kapitel har stegen för planering, genomförande och utvärdering anpassats till test. Se figuren nedan för samtliga steg i testplaneringen.

De sex stegen i testplaneringen.

Steg 1: Förankra testet

För att kunna genomföra framgångsrika tester behövs både ledningens och organisationens stöd. Detta gäller inte minst för att säkerställa tillgängliga resurser för planering och genomförande av testet, samt för en effektiv rapportering och implementation av åtgärder.

Innan planeringen påbörjas bör testet vara förankrat hos rätt personer på rätt nivå. Detta för att säkerställa acceptans och mandat, samt för att uppmärksamma dessa på vilka aktiviteter som planeras att genomföras. De personer som på olika sätt ska delta i testet bör förstå nyttan med aktiviteten, både för organisationen som helhet men också för dem själva som individer.

I förankringsarbetet kan följande information vara värdefull att förmedla:

- Syfte och mål med testet samt förväntat resultat.
- Testets målgrupp samt antalet deltagare.
- Tidpunkt för testet.
- Budget samt andra nödvändiga resurser för såväl planering, genomförande och utvärdering av testet.

Steg 2: Sätt ramarna för testet

Att sätta ramarna för testet handlar bland annat om att definiera testets syfte och mål, samt att utse lämplig målgrupp. Vidare bör en testorganisation (ansvariga för planering, genomförande och utvärdering) utses.

Definition av syfte och mål

Utifrån de förmågeområden som testet avser att utgå ifrån specificeras syfte och mål. Syftet ska beskriva varför testet ska genomföras, samt vara baserat på ett identifierat behov. Syftet ska också vara i linje med den övergripande teststrategin. Organisationen kan exempelvis ha behovet att testa ett särskilt förmågeområde, en identifierad risk, eller förändringar i organisationens omvärld som ställer nya krav.

---

[80] *FSPOS - 6 steg till bättre övningar. I detta appendix benämns steg* ***1 Förankra*** *(istället för Argumentera för övningen).*

Utifrån syftet formuleras specifika mål vilka tydliggör vad testet förväntas leda till. Definierade mål styr fortsatt planering av testet, liksom hur genomförande och utvärdering sker. Allt som görs under testet ska syfta till att målen uppnås. Målen ska vara enkla, mätbara och möjliga att uppnå. För att kunna åstadkomma detta bör antalet mål begränsas. Vid otydligheter eller vägskäl i planeringen ska målen alltid kunna användas som inriktning för det fortsatta arbetet.

Konkretisering av målen genom mätpunkter

För att ytterligare konkretisera målen kan mätpunkter användas. Mätpunkter är tänkta att underlätta bedömningen av måluppfyllelsen.

Mätpunkterna bedöms av en eller flera observatörer under testgenomförandet. För att underlätta bedömningen bör en checklista eller ett testprotokoll tas fram. Mätpunkter formuleras med fördel så att de går att besvaras genom ”ja”/”nej” eller ”godkänd”/”godkänd med kommentar”/”underkänd” eller liknande. Baserat på de uppställda mätpunkterna kan en sammanvägd bedömning av respektive mål göras och i förlängningen även av det uppsatta övergripande syftet.

Exempel på mätpunkter

Nedan ges ett antal exempel på mätpunkter utifrån de förmågeområden som presenterades i avsnitt H.3. *Skapa en teststrategi och testplan*.

Kommunikation
- Kontaktlistor i kontinuitetsplanen är uppdaterade.
- Alternativa kontaktvägar vid störningar i ordinarie system fungerar.

Kompetens
- Processägaren har mandat och kompetens att fatta de beslut som krävs för att aktivera planen.
- Berörda resurser har kompetens nog att genomföra kontinuitetslösningarna enligt plan.

Ledning
- Rutin för larmning och eskalering fungerar som avsett.
- Verktyg och system för larmning är funktionella.

Logistik
- Reservarbetsplatser fungerar som avsett.
- Externa leverantörer kan uppfylla sin del av kontinuitetslösningen.

Medvetenhet
- Personal i organisationen är medveten om de rutiner som gäller vid avbrott i system A.
- Processägare för process B har uppdaterat sin(a) plan(er) på regelbunden basis.

Resurser
- Det finns förmåga att distribuera personal, materiella resurser och kritiska system till reservarbetsplats enligt uppsatta tidskrav i plan.
- Kritisk resurs X kan upprätthållas med stöd av kontinuitetslösningar beskrivna i planen.
- Det finns alternativa arbetssätt som fungerar under minst 48 timmar vid avbrott i aktivitet Y.

Samverkan
- Samverkan med interna aktörer fungerar enligt rutiner beskrivna i planen.
- Samverkan med externa aktörer fungerar enligt rutiner beskrivna i planen.

Tidskrav
- Maximalt tolerabel avbrottstid för process 1 kan mötas med hjälp av beskrivna kontinuitetslösningar.
- Maximalt tolerabel avbrottstid för aktivitet 2 kan mötas med hjälp av beskrivna kontinuitetslösningar.
- Mål för återställningstid för resurs 3 kan mötas med hjälp av beskrivna kontinuitetslösningar.

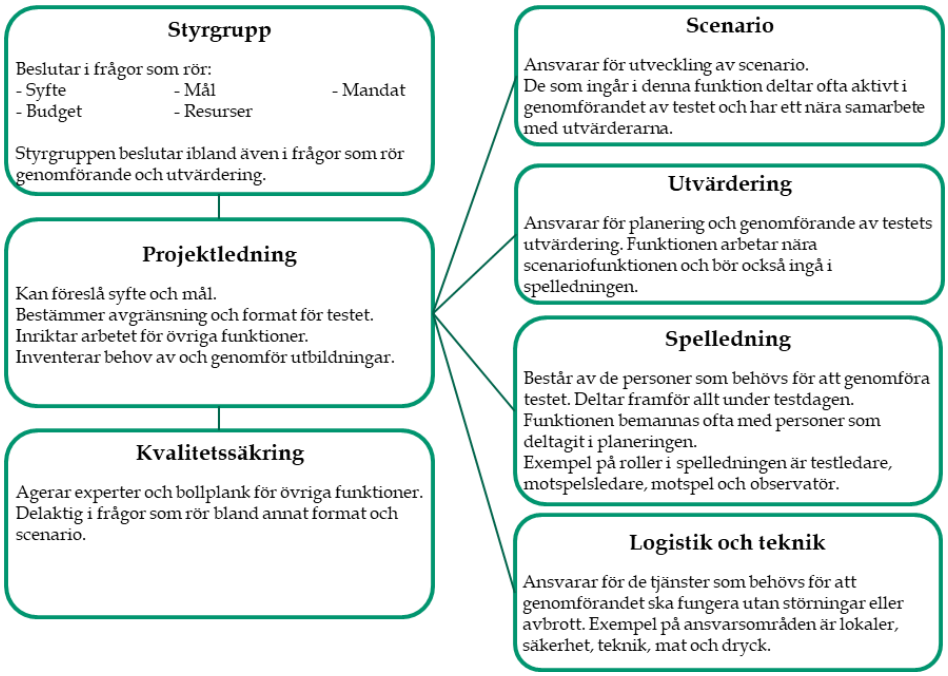
Utse relevant målgrupp

Ytterligare ett viktigt moment är att utse relevant målgrupp. Målgruppen för det specifika testet bör vara angivet i testplanen. För mindre komplexa testyper, såsom dokumentationsgenomgång eller skrivbordsövning, kan en snävare målgrupp utses. För simuleringar, funktions- eller fullskaletester, där hela processer eller ibland flera processer testas samtidigt, behöver ett större antal målgrupper involveras i testet. Dessa målgrupper kan utgöras av såväl processägare, personal från olika delar av den operativa verksamheten, personal från it-verksamheten samt externa leverantörer.

De aktuella målgrupperna bör i god tid vara informerade om testets syfte och mål, samt få vetskap om varför just de blivit utsedda att delta.

Utse testorganisation

Beroende på testets storlek och ambitionsnivå behöver en större eller mindre testorganisation utses. För mindre, enklare tester räcker det oftast med att testledaren ansvarar för alla steg i testet. För större, mer komplexa tester såsom simuleringar, funktions- eller fullskaletester behöver en utökad testorganisation utses för planering, genomförande och utvärdering. Exempel på roller som kan behöva ingå i en sådan testorganisation utöver testledare (del av spelledning) är en styrgrupp, scenarioansvarig, utvärderingsansvarig samt stödresurser för teknik, logistik och administration. Se figur nedan för exempel på testorganisation.



Exempel på testorganisation.

De roller som kan behövas under själva genomförandet av testet beskrivs i figuren nedan. Dessa utgör testets spelledning.

Roller i spelledningen.

Steg 3: Planera testet

I detta steg ingår att fatta beslut gällande vilka testtyper som ska användas, val av relevant scenario samt planering för utvärdering av testet.

Val av testtyp

Som beskrivs i avsnittet *Testtyper* kan tester variera från att vara mycket enkla, till mer omfattande och komplexa, med mer eller mindre praktiska inslag. Ett test som ska vara så realistiskt och verklighetstroget som möjligt kommer kräva betydligt fler resurser och en omfattande planering.

Testtyper bör väljas bland annat med hänsyn till organisationens mognad, resurstillgång, kunskap, storlek, komplexitet samt nisch inom den finansiella sektorn. Valda förmågeområden bör även beaktas i valet av testtyp.

Det är viktigt att organisationen utvecklar sin erfarenhet inom test innan avancerade testtyper genomförs. En testtyp som är för svår i förhållande till organisationens mognadsnivå kan leda till svårtolkade eller bristfälliga resultat.

Val av scenario

Baserat på syfte och mål, valda förmågeområden, testtyp samt den/de planer eller processer/resurser som ska testas utvecklas ett relevant scenario.

Om möjligt bör scenariot inkludera information som gör testet relevant för olika nivåer, d.v.s. att kontinuitetslösningar på processnivå, aktivitetsnivå och resursnivå kan verifieras. Scenariot bör också utgå ifrån organisationens egna identifierade kritiska beroenden.

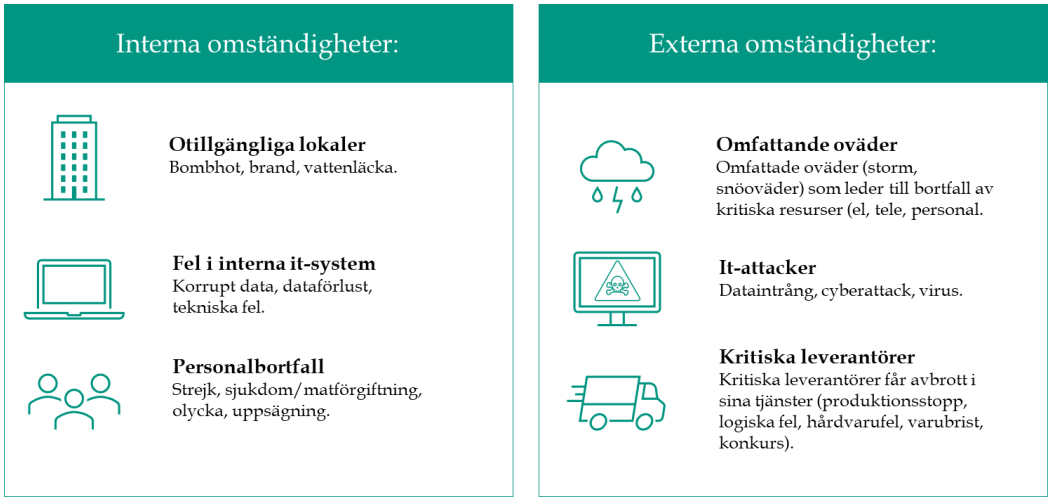
Ett exempel på beroende kan vara en organisations leverantörskedjor. Riskanalyser är också lämpliga att använda som inspiration vid scenarioutveckling. Det är dock viktigt att inte låsa sig fast vid redan identifierade risker. Hänsyn bör även tas till vad som sker i vår omvärld, med nya trender och hot.

Givet att kontinuitetshantering syftar till att upprätthålla en tolerabel nivå för kritiska processer oavsett vilka störningar som inträffar, bör scenariot i sig inte utgöra testets huvudsyfte. Fokus för testet bör istället läggas på organisationens förmåga att upprätthålla den/de testade kritiska processerna.

Scenarier kan behandla både interna och externa omständigheter. De kan beröra allt ifrån omfattande oväder som stegvis leder till bortfall av kritiska resurser, till kritiska leverantörer som får avbrott i sina tjänster, eller fel i interna it-system (exempelvis korrupt data, dataförlust eller tekniska fel). För fler exempel på övergripande scenarier se figuren nedan.

EXEMPEL PÅ SCENARIO OCH FRÅGESTÄLLNINGAR
Ett omfattande strömavbrott har drabbat ert huvudkontor på grund av ett oväder som dragit in över natten. Elbolaget meddelar att strömmen förmodligen inte kommer vara tillbaka på 48 timmar.

- Vilka kontinuitetsplaner behöver aktiveras med anledning av detta?
- Kan process X, Y och Z upprätthållas med stöd från dokumenterade kontinuitetslösningar?
- I de fall arbete behöver ske från alternativ arbetsplats, fungerar flytt till utsedd reservarbetsplats som avsett?
- Vad är viktigt för andra plan-/processägare att veta i detta läge?



Förslag på scenarier på en övergripande nivå.

Planera för utvärdering

Att utvärdera testet framgångsrikt är lika viktigt som att lyckas med själva genomförandet. Det är därför bra att i god tid innan genomförandet påbörja planering av utvärdering samt utse utvärderingsansvarig. Utvärderingsansvarig bör vara en person med tidigare erfarenhet av test. Utvärderingsansvarig utser en eller flera observatörer som kan hjälpa till att observera deltagarna under genomförandet av testet, samt vara med och stötta i det efterföljande utvärderingsarbetet.

Utvärderingsplaneringen bör ske tillsammans med ansvarig för övergripande planering (syfte och mål) samt scenarioplanering för att skapa förutsättningar för en god utvärdering. Även val av testtyp påverkar utvärderingsfunktionens metoder för hur observationer och bedömningar kan genomföras.

Den vanligaste metoden för utvärdering är att genomföra observationer med utgångspunkt från testets definierade mätpunkter. Ett framtaget testprotokoll underlättar dokumentationen under genomförandet av testet (se mall för testprotokoll). Denna typ av testprotokoll är särskilt användbart vid mer avancerade testtyper såsom simuleringar, funktions- eller fullskaletester.

För diskussionsbaserade testtyper används vanligtvis inget testprotokoll. Då används oftast istället en enklare checklista som preciserar vad i kontinuitetsplanen som ska gås igenom.

En utvärderingsdiskussion bör genomföras i direkt anslutning till varje genomfört test. Deltagarnas upplevelser och synpunkter utgör viktiga ingångsvärden till den samlade utvärderingen. Denna diskussion bör också dokumenteras och inkluderas i den avslutande testrapporten.

MALLAR FÖR GENOMFÖRANDE
- TESTPROTOKOLL -

Datum: XX-XX-XX **Scenario:** [Otillgängliga lokaler] **Plan/Process:** [Betallösningar]					**Sammanlagt resultat:** ○ ○ ○
Förmågeområde: [Tidskrav]					
Mål/mätpunkter	**Plan/Process**	**Kontinuitetslösningar (befintliga/nya)**	**Status:** Godkänd ○ Godkänd med kommentar ○ Underkänd ○	**Kommentar** Vilket stöd utgör kontinuitetsplanen? Är stödet från kontinuitetsplanen tillräckligt? Vad behöver utvecklas?	**Åtgärder**
Mål: Förmåga att uppfylla satta MTPD för den/de processer som testas.	**Betallösningar**		○ ○ ○		
Mätpunkt 1: Innehar förmåga att distribuera personal och materiella resurser till reservarbetsplats enligt uppsatta tidskrav i plan.	Betallösningar	Reservarbetsplats X	○ ○ ○		
Mätpunkt 2: Innehar förmåga att nyttja system på upprättad reservarbetsplats inom x antal timmar enligt uppsatta tidskrav i plan.	Betallösningar	Reservarbetsplats X	○ ○ ○		

Steg 4: Genomföra testet

Baserat på valet av testtyp, målgrupp och scenario genomförs testet enligt angivna ingångsvärden från testplanen.

Vid diskussionsbaserade skrivbordsövningar räcker det oftast att scenariot presenteras muntligt eller i form av en punktlista. Baserat på händelseutvecklingen diskuterar deltagarna hur de skulle agera i varje givet läge. Definierade frågeställningar hjälper till att driva diskussionerna mot uppsatta mål.

För simuleringar, funktions- eller fullskaletester behöver dock scenariot oftast presenteras på ett mer realistiskt sätt, d.v.s. att deltagarna får ta del av information om inträffade händelser på samma sätt som i verkligheten, exempelvis via epost eller fiktiv nyhetsrapportering. Ett motspel kan behövas för att förmedla informationen till testdeltagarna. Motspelet har som enda uppgift att föra scenariot framåt genom att förmedla inspel som hjälper till att testa hur processer och resurser fungerar i en realistisk situation.

Som testledare är det viktigt att säkerställa att testet går i rätt riktning mot testets uppsatta mål, samt att valda förmågeområden och processer/resurser utsätts för prövning.

Steg 5: Utvärdera testet

Vid avslutningen av varje test bör en utvärderingsdiskussion genomföras. Syftet med utvärderingsdiskussionen är att ge deltagarna möjligheten att dela erfarenheter så att viktiga lärdomar från testet kan identifieras. Utvärderingsdiskussionen är ett utmärkt tillfälle att fånga upp deltagarnas åsikter, tankar och förslag. Det är viktigt att påpeka att utvärderingsdiskussionen också är en del av själva testet och inte en frivillig aktivitet. Ett gott råd är att inte göra själva testdelen alltför lång, så att den avslutande utvärderingsdiskussionen hinns med inom satta tidsramar.

Utvärderingsdiskussionen bör anpassas efter testets omfattning och utformning. Om testet varit omfattande och involverat många personer kan utvärderingsdiskussionen med fördel genomföras i mindre grupper. Deltagarna har ofta lättast att dela med sig av sina tankar i en mindre grupp. Utvärderingsdiskussionen bör hållas på en relativt övergripande nivå, utifrån frågeställningar som:

- Vilket stöd utgjorde kontinuitetsplanen?
- Var stödet från kontinuitetsplanen tillräckligt?
- På vilket sätt behöver kontinuitetsplanen utvecklas?

Utvärderingsdiskussionen bör också inkludera en tydlig koppling till uppsatta mål och mätpunkter för att tydliggöra uppfyllandegraden av testets mål. Baserat på testledarens och observatörernas observationer, samt resultatet från utvärderingsdiskussionen sammanställs resultatet från testet i en testrapport. Rapporten bör innehålla förslag på konkreta åtgärder på kort, medellång och lång sikt för att förbättra de testade planerna (inkl. ansvarig och deadline för att implementera åtgärderna). Se tabell nedan för exempel på en enkel åtgärdslista.

Åtgärdsförslag	Ansvarig	Deadline	Kommentar

Åtgärdslista. Exempel på åtgärdslista att inkludera i rapport.

Rekommendationerna i testrapporten struktureras med fördel utifrån valda förmågeområden samt satta mål och mätpunkter. Rapporten bör ge en tydlig inriktning inom vilka områden organisationen ska prioritera sina insatser för att stärka eller bibehålla dess förmåga.

Testrapportens resultat och slutsatser bör distribueras till samtliga deltagare så snart som möjligt efter avslutat test.

Steg 6: Implementera och följa upp åtgärder

Utvärderingsresultat samt rekommendationer i testrapporten bör ligga till grund för en handlingsplan för granskning, uppdateringar och förbättringar av organisationens kontinuitetsplaner.

Handlingsplanen bestämmer hur rekommendationerna i testrapporten kommer att implementeras och tillämpas inom organisationen. Planen bör innehålla specifika förbättringsåtgärder för verksamhetens kontinuitetsplaner, en satt tidsram för när varje identifierad åtgärd ska vara genomförd, samt en statusindikator som visar på statusen för respektive åtgärd. Ansvaret för genomförandet av åtgärder bör fördelas på verksamhetens processägare och/eller planägare. En utveckling och förbättring i organisationen kan först ske då handlingsplanens åtgärder går från att ha identifierats och dokumenterats i testrapporten till att de också implementeras, och slutligen följs upp. Handlingsplaner bör följas upp i redan etablerade verksamhetsuppföljningsmöten för att hållas levande och uppdaterade.

H.5. Rapportering till ledning och styrelse

Rapportering av resultatet från genomförda tester av kontinuitetsplaner ska enligt Finansinspektionens föreskrifter ske minst årligen till ledning och styrelse.[81] Rapporteringen bör utgå ifrån fastställd teststrategi samt hållas på en sådan nivå att rekommendationer och åtgärdsförslag inte går att feltolka, samtidigt som rapporten till ledning och styrelse anpassas efter målgruppen. Till exempel bör rapporten inte innehålla alltför många tekniska termer och begrepp.

Regelbundenhet i rapporteringen är viktig för att upprätthålla kunskapen om vilka konsekvenser ett längre avbrott kan få inom organisationen. Rapporteringen ger också ledningen och styrelsen en god inblick i organisationens förmåga att upprätthålla och återställa kritisk verksamhet. Organisationen bör därför ha en rutin för hur ofta rapportering ska ske till ledning och styrelse.

En rapport till ledning och styrelse bör innehålla följande:

- Kort beskrivning av syfte, mål och mätpunkter för genomförda tester.
- Status på kontinuitetsplaner samt andel planer som är testade.
- Övergripande beskrivning av testade scenarier samt förklaring till valda scenarier kopplat till organisationens riskanalys.
- Beskrivning av vilka teststyper som genomförts.
- Förklaring till valda kritiska processer, samt varför vissa kritiska processer inte testats. Använd teststrategin som utgångspunkt.
- Information gällande resultatet av genomförda tester. Kort summering av de mest väsentliga slutsatserna för att ge en inblick över organisationens förmåga att upprätthålla kritiska processer.
- Utvecklingsförslag relaterade till identifierade brister.
- Status för åtgärder från tidigare genomförda tester.
- Genomförda åtgärder och dess eventuella påverkan för uppfyllande av etablerad teststrategi samt övriga verksamhetsmål.

[81] *Finansinspektionen - Föreskrifter och allmänna råd om hantering av operativa risker.*

Allmänna bilagor

Begreppslista

Generella begrepp

Begrepp	Förklaring
Aktör	Samlingsbegrepp för samtliga aktörer inom den finansiella sektorn som inkluderar både myndigheter och företag.
Incident	Situation som skulle kunna vara eller leda till avbrott, förlust, nödläge eller kris (ISO 22301).
Informationstillgång	Information och informationsbärande resurser som är av värde för en organisation. Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera.
Informationsbärande resurs	Vanligtvis it-system eller fysisk media (papper, CD-skiva, USB-minne, etc.) där processens information hanteras och lagras.
Konsekvensanalys	Process för analys av verksamhet och den effekt som ett avbrott skulle kunna ha för verksamheten (ISO 22301).
Kontinuitet	Förmåga hos organisationen att efter avbrott fortsätta tillhandahålla varor och tjänster i en i förväg accepterad omfattning (ISO 22301).
Kontinuitetshantering	Den process som skapar en robusthet i organisationen i syfte att bättre kunna hantera förluster av delar av, eller hela, den operativa förmågan och därigenom skyddar organisationens intressenter, rykte, varumärke och värdeskapande aktiviteter.
Kontinuitetslösning	Beskrivning av reservrutiner (*hur arbetar vi på alternativa sätt under ett avbrott?*), återställningsrutiner (*hur återställer vi den kritiska resursen efter ett avbrott?*) samt återgångsrutiner (*hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen?*).
Kontinuitetsplan	Dokumenterade rutiner som vägleder en organisation att efter avbrott reagera, återställa och återuppta verksamheten i en i förväg definierad omfattning (ISO 22301).
Kritisk process	De processer som behövs för att organisationen ska kunna bedriva sin mest centrala verksamhet. Kan även benämnas, affärskritiska, verksamhetskritiska eller väsentliga processer.

Begrepp	Förklaring
Kriteriemodell	Kriteriemodellen definierar vilka konsekvenser som är acceptabla och oacceptabla och är gemensam för hela organisationen.
Maximalt tolerabel avbrottstid (MTPD)	Den maximala tiden som processen/aktiviteten kan vara otillgängligt innan oacceptabla konsekvenser uppstår. På engelska Maximum tolerable period of disruption (MTPD) (ISO 22301).
Mål för återställningstid (RTO)	Tid efter en incident inom vilken det är nödvändigt att en aktivitet eller resurs återställs. På engelska Recovery Time Objective (RTO) (ISO 22301).
Mål för återställningspunkt (RPO)	Punkt till vilken det är nödvändigt att återställa den information/data som används av en it-resurs, för att göra det möjligt för resursen att återgå till normal leveranskapacitet. På engelska Recovery Point Objective (RPO) (ISO 22301).
Policy	Organisations avsikter och inriktning, formellt uttalande av dess högsta ledning (ISO 22301).
Process	En grupp av aktiviteter som samverkar eller påverkar varandra, och som använder underlag för att åstadkomma ett avsett resultat (ISO 22301).
Produkter och tjänster	Produkter och tjänster en organisation tillhandahåller sina kunder, mottagare och intressenter, exempelvis kortbetalning, personförsäkring och bolån. I ISO 22301 benämns detta för *Varor och tjänster* (ISO 22301).
Program för kontinuitetshantering	Pågående process för ledning och styrning med stöd från högsta ledningen och tilldelad lämpliga resurser för att införa och underhålla kontinuitetshantering (ISO 22301).
Resurser	Alla tillgångar, personer, färdigheter, teknik (innefattande anläggning och utrustning), lokaler, förråd och information (elektronisk och annan) som en organisation vid behov ska ha tillgänglig för sin verksamhet och för att nå sina mål (ISO 22301).
Riskbedömning	Analys av de risker som kan hota identifierade resurser samt bedömning om befintlig redundans är tillräcklig för att möta fastställda mål för återställningstid.
Robusthet	Förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenser om de ändå inträffar.
Strategisk konsekvensanalys	Analys för att fastställa vilka produkter och tjänster samt vilka av de stödjande processerna som ska inkluderas i kontinuitetsarbetet.

It-specifika begrepp

Begrepp	Förklaring[82]
AV-program	Antivirus-program
Back-up	Säkerhetskopia
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IDS	Intrusion Detection System
IKT	Informations- och kommunikationsteknologi
KPI	Key Performance Indicator
LAN	Local Area Network
Middleware	Mellanprogramvara
VPN	Virtual Private Network

[82] *Begreppslistan beskriver de förkortningar som använts i Appendix F - Kontinuitetshantering för it-verksamhet. För vidare hänvisningar, se Svenska datatermgruppens rekommendationer för hur datatermer bör hanteras på svenska. www.datatermgruppen.se*

Referenslista

- Business Continuity Institute, Good Practice Guidelines 2018 – Global edition (2018).
- Basel Committee on Banking Supervision, Outsourcing in Financial Services (2005).
- CPSS/IOSCO , Principles for financial market infrastructures (2012).
- Deloitte's 201, Global Outsourcing and Insourcing Survey – 2014 and beyond (2014)
- Direktiv 2013:36/EU, EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2013/36/EU om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag (2013).
- European Commission, Solvency II (2009/138/EC).
- European Banking Authority. EBA Guidelines on Internal Governance (GL 11) (2017).
- European Banking Authority. EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).
- Finansinspektionen, Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1).
- Finansinspektionen, Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4)
- FSPOS, 6 steg till bättre övningar (2017).
- Förordning (2022:524) om statliga myndigheters beredskap.
- Förordning (EU) nr 575/2013, FÖRORDNINGAREUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 575/2013.
- ITIL 2011 – Information Technology Infrastructure Library (2011).
- ISO 22301:2019, Security and resilience - Business continuity management systems — Requirements (2019).
- ISO 22313:2020 , Security and resilience - Business continuity management systems — Guidance on the use of ISO 22301 (2020).
- ISO/IEC 27031:2011, Guidelines for information and communication technology readiness for business continuity (2011).
- ISO/IEC 27036-1:2014, Information technology - Security techniques - Information security for supplier relationships (2014).
- ISO 22316:2017, Security and resilience - Organizational resilience - Principles and attributes (2017).
- ISO 20000, International IT Service Management Standard (2018).
- ISO 22300:2018, Security and resilience – Vocabulary (2018).

- Krisberedskapsmyndigheten, Kontinuitetsplanering – en introduktion (2006).
- Myndigheten för samhällsskydd och beredskaps (MSB:S), föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
- Myndigheten för samhällsskydd och beredskap (MSB:S), Upphandla Informationssäkerhet – en vägledning (2018).
- Myndigheten för samhällsskydd och beredskaps (MSB:S), verktygslåda för kontinuitetshantering https://www.msb.se/kontinuitetshantering (2020).
- RBFS 2023:3, Riksbankens föreskrifter och allmänna råd om företag av särskild betydelse för genomförandet av betalningar under fredstida krissituationer och vid höjd beredskap (2023).
- SOU 2013:65, Förstärkta kapitaltäckningsregler (2013).
- SS-EN ISO 22301:2019, Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Krav (2019).
- SS-EN ISO 22313:2020, Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Vägledning för implementering av ISO 22301 (2020).
- SS-ISO 31000:2018, Riskhantering - Vägledning (ISO 31000:2018, IDT) (2018)
- SS-ISO 22325:2016, Krishantering - Vägledning för förmågeutvärdering (2016).