FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

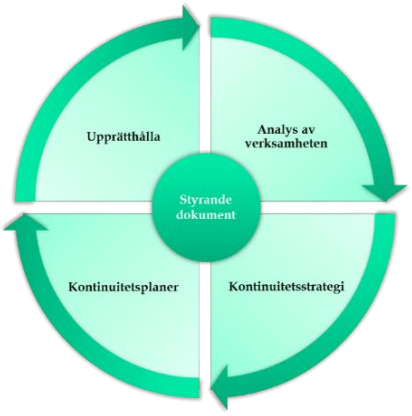
FSPOS Vägledning för Kontinuitetshantering

Version: 2013-12-16
FSPOS AG KON, Fokusgrupp Kontinuitetshantering

Sammanfattning

I FSPOS tidigare arbete[1] har ett behov av en vägledning i kontinuitetshantering identifierats. *FSPOS vägledning för kontinuitetshantering* syftar till att tillfredsställa detta behov genom att beskriva processen för kontinuitetshantering. Som ytterligare stöd till företag i den finansiella sektorn inkluderar vägledningen också mallar och exempel för arbetet med kontinuitetshantering. Vägledningen baseras på den internationella standarden inom kontinuitetshantering; *SS-ISO 22301:2012 – Samhällssäkerhet – Ledningssystem för kontinuitet*[2].

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, 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. 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 ska beskrivas konkret och tydligt för att kunna användas under en störning.

UPPRÄTTHÅLLA handlar om att utbilda, öva, 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.

---

[1] *Bland annat i rapporten Riskbild Stockholm (2011) och Vägledning för robust elektronisk kommunikation (2012)*

[2] *ISO 22301:2012 - Societal security - Business continuity management systems (Engelsk version)*

Innehållsförteckning

1. INLEDNING 4

1.1. LÄSANVISNINGAR 4
1.2. BAKGRUND 4
1.3. UTGÅNGSPUNKT 5
1.4. MÅLGRUPP 6

2. INTRODUKTION TILL KONTINUITETSHANTERING 7

2.1. VAD ÄR KONTINUITETSHANTERING? 7
2.2. NYTTAN MED KONTINUITETSHANTERING 8
2.3. KRAV PÅ KONTINUITETSHANTERING 10
2.4. KOPPLING TILL INCIDENT-, RISK-, OCH KRISHANTERING 12

3. PROCESS FÖR KONTINUITETSHANTERING 15

3.1. STYRANDE DOKUMENT 16
3.2. ANALYS AV VERKSAMHETEN 17
3.3. KONTINUITETSSTRATEGI 18
3.4. KONTINUITETSPLANER 19
3.5. UPPRÄTTHÅLLA 20

APPENDIX A - STYRANDE DOKUMENT 23

APPENDIX B - ANALYS AV VERKSAMHETEN 34

APPENDIX C - KONTINUITETSSTRATEGI 44

APPENDIX D - KONTINUITETSPLANER 49

APPENDIX E - UPPRÄTTHÅLLA 56

APPENDIX F - KONTINUITETSHANTERING FÖR IT-VERKSAMHETEN 60

APPENDIX G - BEGREPPSLISTA 68

APPENDIX H - REFERENSLISTA 70

1. Inledning

Denna vägledning har utvecklats av Arbetsgrupp Kontinuitetssäkring (AG KON) inom Finansiella Sektorns Privat-Offentliga Samverkan (FSPOS) i syfte att ge aktörer inom den finansiella sektorn stöd utifrån god praxis beträffande hur organisationen kan arbeta med utveckling, implementering och uppföljning av kontinuitetsarbetet. Många aktörer i den finansiella sektorn har verksamhet som är 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 (2013)*

1.1. Läsanvisningar

Vägledningen inleds med detta avsnitt, där bakgrund, utgångspunkt och målgrupp för dokumentet presenteras. Därefter ges en introduktion till kontinuitetshantering, där beskrivningar av nyttan med samt krav på kontinuitetshantering 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 (Appendix F) som beskriver hur kontinuitetshantering kan bedrivas för de IT-system och -tjänster som verksamheten är beroende av. Denna del är föreslagen att vidareutvecklas av FSPOS under 2014.

Avslutningsvis innehåller denna vägledning en ordlista med centrala begrepp och definitioner (Appendix G) samt en referenslista (Appendix H).

1.2. Bakgrund

FSPOS initierades 1 september 2005. Verksamheten inom FSPOS bygger på frivilligt arbete bland deltagarna som inkluderar medlemmar från både privat och offentlig sektor och det löpande arbetet bedrivs i ett antal arbetsgrupper. FSPOS vision är *"att samhällsviktiga finansiella tjänster alltid fungerar"*, och verksamhetsidén är *"att FSPOS ska stärka den finansiella infrastrukturen genom att samverka, öva, kartlägga och dela information, och på så sätt värna sektorn och samhället"*.

AG KON består för närvarande (2013) av tre fokusgrupper (kan ändras med tiden); FG Riskanalys och informationsdelning, FG Kontinuitetshantering och FG Finansiella tjänster. AG KON fick under 2013 i uppdrag av FSPOS styrelse att löpande värdera behovet av samt föreslå och genomföra sektorgemensamma aktiviteter med syfte att stärka robustheten i den finansiella infrastrukturen. Inom FG Kontinuitetshantering har arbetet under 2013 fokuserat på att utveckla denna vägledning för kontinuitetshantering.

1.3. Utgångspunkt

Behovet av stöd inom kontinuitetshantering har tidigare identifierats inom två av FSPOS arbetsgrupper, AG Kritisk Infrastruktur och AG Grundläggande Säkerhetsnivåer, där aktörer i finansiella sektorn har efterfrågat en tydlig och praktisk vägledning inom kontinuitetshantering.

För att identifiera sektorns behov inom kontinuitetshantering och för att hämta inspiration och goda exempel till vägledningen genomfördes inledningsvis en förstudie. Förstudien baserades dels på en intervjuundersökning med aktörer inom den finansiella sektorn, dels på resultatet av en workshop med FG Kontinuitetshantering och dels på 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 själva har utvecklat egna lösningar och tolkningar av standarder, vilket i sin tur medför att sektorns aktörer antingen saknar nödvändiga verktyg eller arbetar på olika sätt. En central utgångspunkt för vägledningen har därför varit att söka komplettera befintliga standarder och vägledningar inom området genom att beskriva *hur* arbetet kan genomföras.

Många av sektorns aktörer arbetar helt eller delvis enligt den brittiska standarden *BS 25999*, som utvecklades 2006. Sedan 2012 finns en internationell standard för kontinuitetshantering som beskriver kraven på god kontinuitetshantering, *SS-ISO 22301:2012 – Samhällssäkerhet – Ledningssystem för kontinuitet - Krav* (ISO 22301)[3]. En tillhörande vägledning, *SS-ISO 22313:2013, Samhällssäkerhet, Ledningssystem för kontinuitet – Riktlinjer (ISO 22313)*[4], beskriver något mer konkreta riktlinjer kring genomförandet av kontinuitetshantering. Ytterligare en standard innehåller riktlinjer kring kontinuitetshantering, kopplat till IT- och kommunikationsteknologi, *ISO/IEC 27031:2011– Guidelines for information and communications technology readiness for business continuity.*

Internationella standarder bidrar med en enhetlig och allmänt accepterad process, principer och terminologi. Nationella standarder utgår däremot ofta från de behov och omständigheter som är relevanta för det land standarden kommer från.

ISO-dokumenten överensstämmer i stor utsträckning med BS 25999, även om vissa skillnader finns. ISO 22301 och ISO 22313 lägger exempelvis ett större fokus på att organisationens kontext, den miljö och de förutsättningar som påverkar organisationen, finns tydligt beskrivna. I dessa standarder understryks även att avgränsningen av organisationens kontinuitetshantering bör kommuniceras till organisationens viktigaste intressenter. En relativt större vikt läggs i ISO 22301 även på att organisationens ledning

---

[3] *Denna standard är översatt från den engelska versionen: 22301:2012 - Societal security - Business continuity management systems - Requirements*

[4] *Svensk översättning saknas i dagsläget, den svenska versionen är densamma som den engelska: ISO 22313:2013 – Societal security - Business continuity management systems – Guidance*

kommunicerar sitt engagemang för kontinuitetshanteringen, bland annat genom en tydlig policy. Ett fåtal nya begrepp har även introducerats inom ISO 22301 och ISO 22313 jämfört med BS 25999, men i huvudsak är definitioner och begrepp i dessa ISO-standarder en återspegling av de som återfinns i BS 25999.

Denna vägledning utgår från ISO-standarderna för kontinuitetshantering, inklusive den terminologi som standarderna använder. Syftet med FSPOS vägledning har samtidigt inte varit att ta fram 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 dock tagits för att konkretisera standardernas innehåll, såsom *Good Practice Guidelines 2013* (GPG) från brittiska 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.

1.4. Målgrupp

Målgrupp 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, alternativt användas som en benchmark att jämföra sig mot. Andra finansiella aktörer har ännu inte uppnått en lika stor mognad. För dessa organisationer kan vägledningen användas för att från grunden utveckla, implementera och följa upp kontinuitetsarbetet. Vägledningen söker 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 att mogna inom kontinuitetshantering skiljer sig mellan olika organisationer.

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 och komma från bland annat lagkrav, 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 upprätthålls på en acceptabel nivå. Därigenom kan organisationen i förlängningen skydda intressenter, rykte, varumärke och värdeskapande aktiviteter. Avsnittet beskriver även ett antal krav 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 områden, såsom incident-, risk- och krishantering. Detta då de är överlappande och det ofta upplevs som svårt att separera de olika områdena.

2.1. Vad är kontinuitetshantering?

Förenklat kan kontinuitetshantering beskrivas som 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.[5]

Med detta menas att organisationen minskar sin sårbarhet och ökar sin motståndskraft mot olika händelser som kan påverka dess mest kritiska verksamhet. Aktuell vägledning kommer att utgå från denna definition, samt även i så stor utsträckning som möjligt använda begrepp och definitioner från ISO 22301.

Andra definitioner av kontinuitetshantering är snarlika denna och kortfattat kan kontinuitetshantering summeras som den process som säkerställer att organisationen har en robusthet för att driva den kritiska verksamheten på en tolerabel nivå oavsett vilka störningar som inträffar.

---

[5] *Definition enligt ISO 22301: "Holistic management process that identifies potential threats to an organization and the impact to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."*

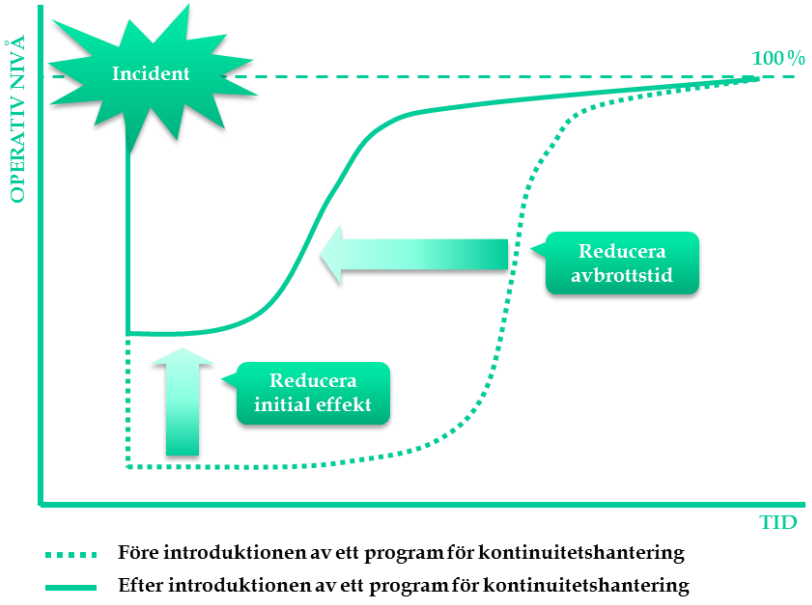
2.2. *Nyttan med kontinuitetshantering*

Nyttan med kontinuitetshantering kan dels beskrivas genom den effekt 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 processer eller kritiska produkter och tjänster, 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.

Ett sätt att visualisera nyttan med kontinuitetshantering illustreras i diagrammet nedan. Som visas i bilden[6] 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.



[6] *SS-ISO 22313:2013, Samhällssäkerhet, Ledningssystem för kontinuitet – Riktlinjer*

Även om det övergripande målet med kontinuitetshantering är att minska konsekvenserna av avbrott och avbrottstiderna 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 kundnöjdhet.

Ekonomisk nytta uppnås bland annat genom att svagheter elimineras 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 externa aktörer, exempelvis gällande el och elektronisk kommunikation. Kontinuitetshantering understryker behovet av externa beroenden och söker säkerställa sådana leveranser genom upprättande av lämpliga strategier och avtal. 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:[7]

- **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 delarna eller processerna. Kontinuitetshantering skapar mervärde till organisationen genom att bidra till stärkt måluppfyllnad, men gör detta med ett

[7] *Kontinuitetsplanering – en introduktion, Krisberedskapsmyndigheten (2006)*

strukturerat och effektivt arbetssätt som tydliggör ansvar och möjliggör optimeringar avseende investeringar.

2.3. *Krav 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. Samtidigt bör beaktas att lagar, föreskrifter och råd utvecklas löpande och de som beskrivs i denna vägledning är endast 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 organisationer som är under tillsyn av Finansinspektionen i Finland gäller exempelvis ett antal bindande föreskrifter. Här ställs jämfört med Sverige hårdare krav på aktörers ansvar att kartlägga sina mest kritiska delar av verksamheten och upprätta kontinuitetsplaner.[8]

För myndigheter under regeringen ger Myndigheten för samhällsskydd och beredskap (MSB) allmänna råd om att kontinuitetsplaner för informationsförsörjningen bör upprättas, samt att planerna bör hållas uppdaterade och övas så att de blir ett naturligt inslag i ledning av informationssäkerhetsarbetet.[9] Därutöver nämner MSB i sitt förslag till *Vägledning för identifiering av samhällsviktig verksamhet och konsekvensbedömning* att kontinuitetshantering utgör en viktig del av ett systematiskt säkerhetsarbete, inom ramen för identifiering och skyddande av samhällsviktig verksamhet.[10] Här ges även förslag till hur beroendekartläggning och konsekvensbedömning kan genomföras för samhällsviktig verksamhet.

För så kallade Financial Market Infrastructures (FMI), som faciliterar clearing, avveckling och registrering av ekonomiska och andra finansiella transaktioner, har CPSS/IOSCO[11] fastställt principer som bland annat ställer krav på kontinuitetsplaner. Planerna ska behandla händelser som utgör en betydande risk för större avbrott och ska

---

[8] *Finanssivalvonta (2010), Standard 4.4b Hantering av operativa risker – Föreskrifter och allmänna råd, Kap 6.4.*

[9] *Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter om statliga myndigheters Informationssäkerhet (MSBFS 2009:10)*

[10] *MSB (2013) Vägledning för identifiering av samhällsviktig verksamhet och konsekvensbedömning (remissversion)*

[11] *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.*

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.[12]

Under 2013 antog Europaparlamentet och rådet ett nytt ett direktiv[13] och en förordning[14] som syftar till att införa Basel 3 i bindande rättsakter inom EU och harmonisera 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"*.[15]

Krav på kontinuitetshantering hos kredit- och värdepappersinstitut återfinns även i EBA:s (European Banking Authority) riktlinjer gällande intern styrning och kontroll (GL 44). 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.[16]

Baserat bland annat på Basel 3 och GL 44, har Finansinspektionen föreslagit nya föreskrifter och allmänna råd om hantering av operativa risker och om styrning, riskhantering och kontroll i kreditinstitut som föreslås träda i kraft 2014. Dessa föreskrifter kommer att beröra vissa aktörer i den finansiella sektorn. I de föreslagna 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]

För försäkrings- och återförsäkringsorganisationer ställer Solvency II[18] krav på att bolaget vidtar rimliga åtgärder för att säkerställa kontinuitet i verksamheten. Detta

---

[12] *CPSS/IOSCO (2012), Principles for financial market infrastructures, Principle 17, s. 100.*

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

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

[15] *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*

[16] *EBA (2011), EBA Guidelines on Internal Governance (GL 44), s. 45.*

[17] *Finansinspektionen (2013), Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut, 2 kap 8 §, s. 4.*

[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.*

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 mer 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.

2.4. Koppling till incident-, risk-, och krishantering

En vanlig frågeställning kring kontinuitetshantering är hur den förhåller sig till angränsande områden såsom incident-, risk- och krishantering. Svårigheten att separera de olika områdena beror på att de ofta är överlappande och på en övergripande nivå syftar till att förebygga och hantera oönskade händelser som äventyrar organisationens måluppfyllnad. En fråga som ofta förekommer i detta sammanhang är huruvida särskilda processer behövs för de olika områdena, eller om kontinuitetshanteringen även inbegriper incident-, risk- och krishantering.

Ett kortfattat svar på dessa frågor är att områdena delvis har olika fokus och angreppssätt, vilket kräver annorlunda metoder och kompetenser. I mindre organisationer kan ansvar för områdena ibland ligga hos samma person, medan det hos större organisationer ofta är delegerat till olika personer i olika delar av organisationen. Utgångspunkten bör dock vara att incident-, risk, kris- och kontinuitetshantering betraktas som skilda men kompletterande områden och arbetet bör därför inte utföras i stuprör.

Incidenthantering

En incident definieras av ISO 22301 som en situation som kan vara eller som skulle kunna leda till avbrott, förlust eller kris. 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 ”near-misses” 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[20] definierar en incident 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[21], där

---

[19] *European Commission, Solvency II (2009/138/EC), Directive Article 41. 4.*
[20] *Information Technology Infrastructure Library (ITIL)*
[21] *ISO 20000 – International IT Service Management Standard*

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.

Riskhantering

Riskhantering handlar om att hantera osäkerheter genom att systematiskt identifiera, analysera, utvärdera och behandla[22] de risker som påverkar organisationens mål. Riskhantering utgör en central del i den strategiska styrningen av organisationen. Riskhanteringen fokuserar därmed på ett bredare urval av risker än kontinuitetshantering och en vanlig utgångspunkt i riskhantering är att först identifiera potentiella händelser/hot och därefter analysera deras sannolikhet och konsekvens.

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 och aktiviteter. Risker och sårbarheter som identifieras inom kontinuitetshantering är endast sådana som har en direkt koppling till organisationens värdeskapande 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.

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. 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

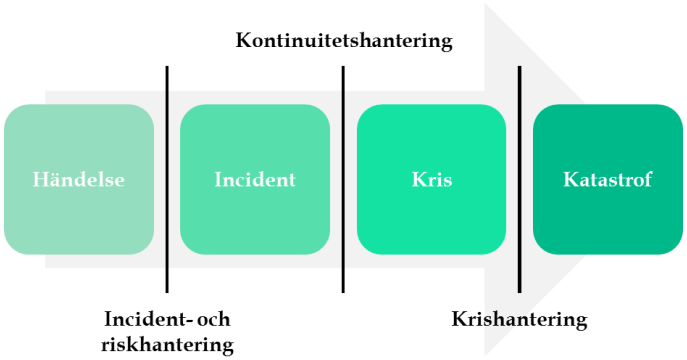
---

[22] *ISO 31000 – Risk management – Principles and guidelines*

inte nödvändigtvis innebära, att den kritiska verksamheten är avbruten och avviker från vad som anses som 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 behöver aktiveras.

Fokusområden för incident-, risk-, kris- och kontinuitetshantering

Organisationer bör arbeta med såväl incident-, kris-, risk- 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 sedan arbeta 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 (istället för hotet/orsaken) och därefter arbeta för att skapa robusthet i dessa delar. Riskhantering och kontinuitetshantering är komplement till varandra och organisationen behöver arbeta med båda.

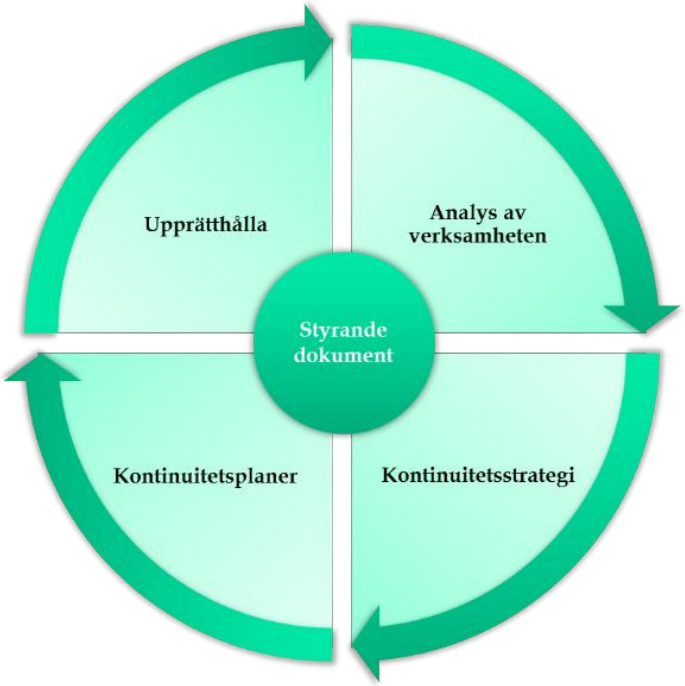
Incidenthantering fokuserar inte på händelser av särskild påverkansgrad eller grad/kännedom av sannolikhet. Incidenter fångas upp, varav vissa hanteras eller av annan anledning aldrig leder till någon större påverkan för verksamheten. På så vis kompletterar incidenthanteringen övriga områden genom att ha ett brett fokus som stödjer såväl risk-, kris- och kontinuitetshantering. 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.

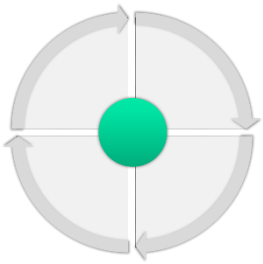
3. Process för kontinuitetshantering

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.

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 nedanstående illustration. 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 mål, organisation, rutiner, processer, system och kultur för kontinuitetshantering. En tydlig avgränsning bör även genomföras och kommuniceras avseende vad kontinuitetshanteringen omfattar inom organisationen. Utgångspunkten bör vara att analysera de delar av verksamheten som är de mest tidskritiska. Styrande dokument bör säkerställa att personer med rätt kompetens, exempelvis inom kontinuitetsmetodik, IT och avtalsskrivning, involveras i arbetet.

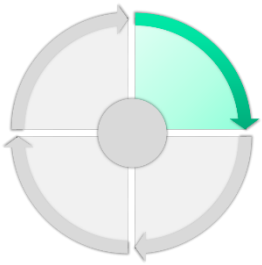
Det är viktigt att det finns en gemensam syn på verksamhetens riskbenägenhet, det vill säga var gränsen går för vilka konsekvenser som är acceptabla. Detta kan definieras genom en kriteriemodell där olika konsekvenskategorier (exempelvis ekonomi och rykte/varumärke) och konsekvensnivåer (obetydlig, märkbar, allvarlig) definieras, därefter beskrivs var gränsen för vad som är acceptabelt går. I exemplet nedan är gränsen för vad som är acceptabelt angiven med den svarta linjen mellan nivåerna märkbar och allvarlig. Med detta menas att konsekvenser inom ekonomi och rykte/varumärke accepteras upp till det som beskrivs inom nivån märkbar. Konsekvenserna inom nivån allvarlig accepteras inte.

	Obetydlig	**Märkbar**	**Allvarlig**
Ekonomi	Förlust < 500 000	Förlust < 5 000 000	Förlust > 5 000 000
Rykte/varumärke	Ingen förlust av kunder	Förlust av låg andel kunder	Förlust av stor andel kunder

I exemplet används tre konsekvensnivåer. Kriteriemodellen skulle även kunna använda ett större annat antal nivåer om det skulle anses lämpligt att segmentera analysen ytterligare, exempelvis genom att använda nivåerna *obetydlig*, *märkbar*, *allvarlig* och *katastrofal*. På ett liknande sätt kan fler konsekvenskategorier än ekonomi och rykte/varumärke läggas till i kriteriemodellen, baserat på vilka områden organisationen anser lämpliga.

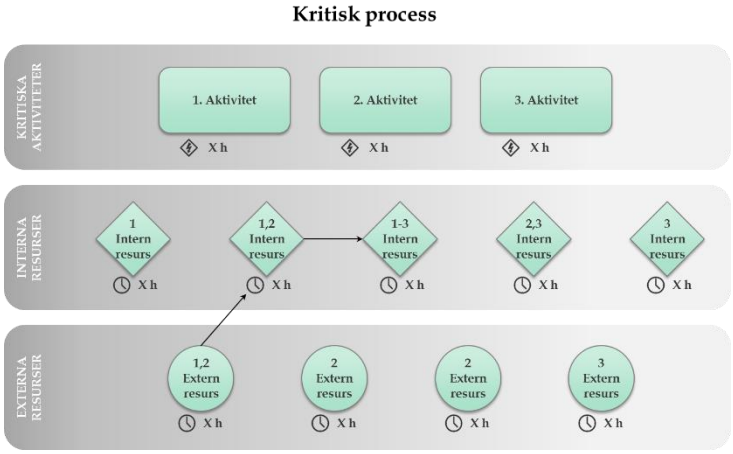
I FSPOS vägledning benämns det huvudsakliga styrande dokumentet policy. Inom vissa områden, exempelvis för avgränsning, kan det ibland vara motiverat att ge mer detaljerade beskrivningar i ett separat styrande dokument. Det är dock viktigt att förhållandet mellan detta dokument tydligt framgår i policyn samt att en tydlig referens till avgränsningen ges i policydokumentet.

3.2. *Analys av verksamheten*



Analysen genomförs för att skapa kunskap om organisationens kritiska verksamhet. I analysen kartläggs verksamheten genom att kritiska processer identifieras. Identifieringen görs med utgångspunkt i vilka processer som är viktiga för att organisationen ska kunna uppnå sina verksamhetsmål samt eventuella legala krav som organisationen har för sin verksamhet. I detta arbete är det bra att inventera eventuellt arbete som tidigare gjorts inom organisationen som processkartläggningar eller återstartsrutiner för kritiska IT-system.

De kritiska processerna bryts ned i aktiviteter samt interna och externa beroenden. Detta görs genom att analysera varje affärskritisk process och identifiera kritiska aktiviteter. För att kunna utföra de identifierade kritiska aktiviteterna krävs i sin tur både interna och externa resurser såsom personal, system, lokaler och leverantörer. För varje aktivitet identifieras därmed de interna och externa resurser som behövs för att utföra respektive aktivitet.



När kritiska aktiviteter samt interna och externa resurser identifierats för varje affärskritisk process är nästa steg att definiera den maximalt tolerabla avbrottsperioden[23] för varje aktivitet.

För att definiera maximal tolerabel avbrottsperiod för en aktivitet används den tidigare utvecklade kriteriemodellen som definierar organisationens riskbenägenhet. Den längsta tid som ett avbrott kan fortgå, utan att konsekvenserna blir så allvarliga att de enligt

[23] *MTPD - Maximum Tolerable Period of Disruption (ISO 22301) / MAO – Maximum Acceptable Outage (ISO 22301)*

kriteriemodellen definieras som oacceptabla, är den tid som är aktivitetens maximalt tolerabla avbrottstid.

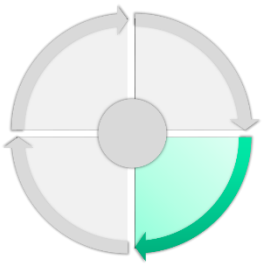
En aktivitets maximalt tolerabla avbrottsperiod avgör sedan vilket mål för återställningstid[24] som ställs på respektive resurs. Med detta menas den tid inom vilken resursen måste kunna återställas till normal funktion efter ett avbrott. Ofta sätts krav på återställningstid med en säkerhetsmarginal i förhållande till den maximalt tolerabla avbrottsperioden. I de fall där resursen har att göra med lagring av data är det också relevant att definiera krav på återhämtningspunkt[25] vilket innebär krav på hur gammal data maximalt får vara för att medge funktionalitet i den kritiska aktiviteten.

Slutligen görs en riskbedömning för att få en djupare förståelse för risker och hot som är kopplade till de kritiska resurserna. Detta för att avgöra om befintliga lösningar är tillräckliga för att säkerställa leverans i nivå med behoven.

Utifrån riskbedömningen tas sedan beslut om vilka risker som måste minskas för att säkerställa att de maximalt tolerabla avbrottsperioderna för kritiska aktiviteter inte överskrids. Riskbedömningen kan även identifiera risker där den befintliga redundansen är onödigt hög.

Sammantaget skapar konsekvensanalysen och riskbedömningen kunskap om verksamhetens kritiska delar samt hur sårbara dessa är vilket utgör underlag för utformningen av kontinuitetsstrategier.

3.3. Kontinuitetsstrategi



Kontinuitetsstrategier utgör gemensamma principer som möjliggör för organisationen att välja lämpliga sätt att förebygga och hantera hot mot de prioriterade aktiviteterna och resurserna. Valda kontinuitetsstrategier ska säkerställa att prioriterade aktiviteter och resurser fungerar inom de uppsatta tidskraven. Kontinuitetsstrategier sätts på en övergripande nivå och utgör en inriktning för vilka kontinuitetslösningar 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. Strategierna kan ta sikte på att hantera störningar före, under och/eller efter att de inträffar. Strategier <u>före</u> en störning syftar till att förebygga och/eller minska sannolikheten för önskade händelser, strategier <u>under</u> en störning syftar till att skapa så små avbrott som möjligt i verksamheten under en störning och strategier <u>efter</u> en störning syftar till att minska konsekvenserna av en störning efter att den inträffat.

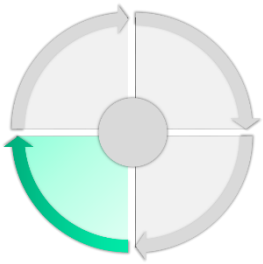
---

[24] *RTO - Recovery Time Objective (ISO 22301)*
[25] *RPO - Recovery Point Objective (ISO 22301)*

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 aktivitet eller beroende de söker upprätthålla.

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 såväl hur kontinuiteten i identifierade kritiska resurser ska upprätthållas, hur resursen återställs vid störningar samt hur återgång till normalläge ska ske då resurserna åter fungerar som normalt.

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?*

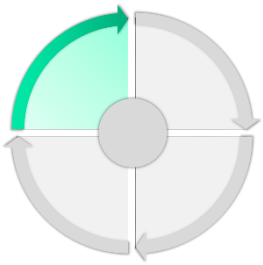
Återgångsrutiner - *Hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen?*

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. Kontinuitetslösningarna 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 skadehantering och återförsäkring).

För var och en av kontinuitetslösningarna ska roll- och ansvarsfördelning beskrivas samt nödvändig kontaktinformation anges.

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

3.5. *Upprätthålla*

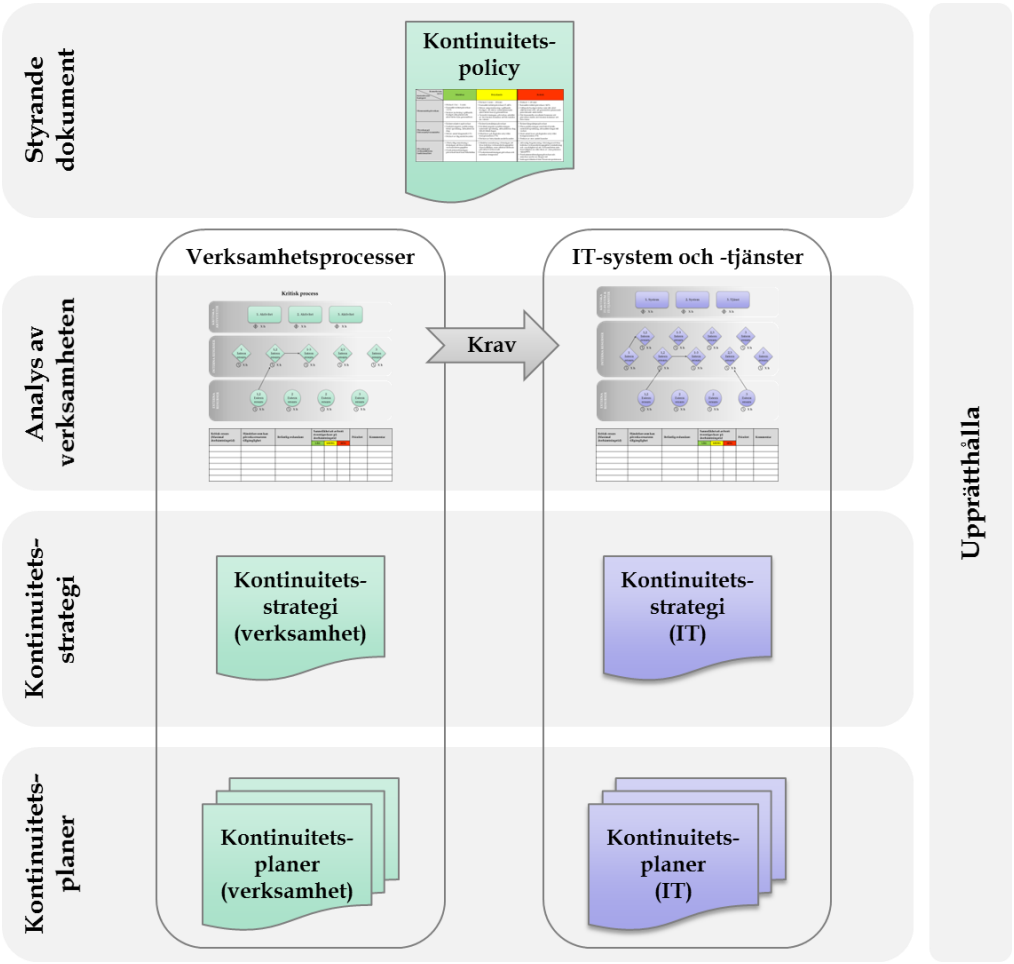


Liksom med andra verksamhetsprocesser så måste arbetet med kontinuitetshantering kontinuerligt upprätthållas och förbättras. Detta kan exempelvis ske genom granskning och revidering av styrande dokument, genomförda analyser och utvecklade kontinuitetsplaner utifrån förändrade förutsättningar. Ett annat sätt att upprätthålla och förbättra kontinuitetsarbetet är genom utbildningar och övningar 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. 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 och bör genomföras för olika nivåer av organisationen och med olika syften baserat på målgruppens behov och roll i arbetet.

Test, övning och utbildning 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 dels fördjupande beskrivningar och dels förteckningar över begrepp samt referenser, 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.

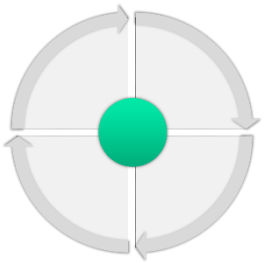
Appendix E innehåller en mer djupgående beskrivning av det femte steget i kontinuitetshanteringsprocessen; **Upprätthålla**. Målgrupp för avsnittet är samtliga som ska arbeta med kontinuitetshantering i verksamheten, men särskilt beslutsfattare som ansvarar för utveckling och upprätthållande av kontinuitetsarbetet.

Appendix F innehåller en övergripande beskrivning av kontinuitetshanterings-processen 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 utgörs av en begreppslista.

Appendix H utgörs av en referenslista.

Appendix A - Styrande dokument



Eftersom omvärlden ständigt förändras är det nödvändigt att kontinuitetsarbetet regelbundet revideras. För att säkerställa detta behöver styrande dokument för arbetet med kontinuitetshantering utvecklas, implementeras och hållas levande. I FSPOS vägledning benämns det huvudsakliga styrande dokumentet *policy*. Benämningen på det styrande dokumentet kan dock variera från organisation till organisation, exempel på benämningar är riktlinje eller instruktion. Organisationens policy för kontinuitetshantering är det övergripande styrdokumentet som på en strategisk nivå (av organisationens ledning) definierar hur kontinuitetshanteringsarbetet leds och administreras samt ger en tydlig inriktning om hur kontinuitetshanteringsarbetet genomförs.

För vissa områden, såsom kontinuitetshanteringens avgränsning, kan vissa organisationer välja att beskriva detta i ett separat dokument. Enligt ISO 22301 bör dock policyn i så fall ge inriktning om en sådan gränsdragning samt hänvisa till den mer detaljerade avgränsningen.

Policyn bör även belysa processen, rutiner och metod för kontinuitetshantering. Därutöver bör roller och ansvar för arbetet förtydligas för att säkerställa att tillräckliga resurser stödjer arbetet. Beroende på organisationens storlek och behov, kan även mer detaljerade beskrivningar för dessa områden läggas i separata mer omfattande dokument. Viktigt är dock att referenser till dessa dokument görs i det övergripande styrande dokumentet och att dessa beskrivningar finns tillgängliga för dess målgrupp.

A.1. Introduktion och organisationens kontext

Policy för kontinuitetshantering definieras i ISO 22301 som syfte och inriktning som uttrycks av organisationens ledning. Viktigt är att organisationens syfte och mål med kontinuitetshanteringen klargörs. Syftet med policyn är att kommunicera till relevanta intressenter vilka principer som organisationen eftersträvar inom kontinuitetshantering. Därmed bör policyn vara relativt kärnfull och pedagogisk. En alltför omfattande och detaljerad policy riskerar att förvirra mottagaren och bli oanvändbar. Policyn bör vara tydlig med centrala begrepp och definitioner. En tydlig definition bör bland annat göras av kontinuitetshantering. Även om definitionen som används kommer från denna vägledning eller om referens görs till exempelvis ISO 22301 bör begreppet klargöras så att hela organisationen har samma utgångspunkt.

Policyn beskriver inriktning för omfattningen av kontinuitetshanteringsarbetet, det vill säga den avgränsning som gjorts av vilka verksamhetsdelar som arbetet bör täcka. Vidare beskrivs här hur arbetet organiseras och leds. Organisationens ledning bör stå som ansvarig för policydokumentet, vilket utgör en viktig signal om ledningens engagemang och att kontinuitetshantering prioriteras.

För att uppnå tydlighet bör organisationen belysa varför kontinuitetshantering genomförs, samt även vilken kontext organisationen verkar inom. Detta kan beskrivas i en inledande översikt av policyn. Med detta menas att organisationen har en uppfattning om vilka interna och externa faktorer som påverkar dess mål och därigenom ställer krav på kontinuitetshantering. Inom ISO 22313 redogörs för en rad sådana faktorer. Interna faktorer kan utgöras bland annat av vilka värdeskapande produkter och tjänster som organisationen levererar, hur kontinuitetshanteringsarbetet organiseras samt vilka mål, policys och rutiner man har för verksamheten i övrigt.

Externa faktorer kan utgöras av drivkrafter och förväntningar från intressenter såsom kunder, partners, leverantörer och distributörer. 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.[26] För att skapa en tydligare bild över dessa faktorer kan en kartläggning göras över organisationens intressenter och dess förväntningar. Intressenternas förväntningar kan se olika ut för normalläge och vid ett avbrott och det kan därför finnas anledning att belysa förväntningarna i båda dessa lägen. Vid kartläggningen kan en prioritering göras för att tydliggöra vilka intressenter som är särskilt styrande för organisationen.

A.2. Avgränsning och omfattning

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 delar av verksamheten samt att driva arbetet i projektform. Ambitionen bör dock vara att de huvudsakliga stegen och delarna i ett kontinuitetarbetet tas fram inom projektet eller projekten, om än i avgränsad form.

Avgränsning av arbetet är en viktig del kontinuitetshanteringen, där det tydligt bör klargöras vilka delar av verksamheten som ska omfattas i arbetet. Som noterats ovan bör policyn som minst ge en inriktning om kontinuitetsarbetets begränsningar. Även om vissa verksamhetsdelar lämnas utanför kontinuitetshanteringen, kan det vara lämpligt att ge inriktning om vad som förväntas av samtliga delar av organisationen inom området, exempelvis att en viss kunskap bör finnas hos samtliga medarbetare om organisationens arbete med kontinuitetshantering.

I vissa fall kan det vara motiverat att beskriva avgränsningen i ett separat dokument som policyn istället hänvisar till. Detta bland annat då det är viktigt att policyn inte blir för alltför omfattande. Avgränsningen kan även vara föremål för omfattande revideringar, i synnerhet i början av implementeringen av kontinuitetshantering, vilket ytterligare kan motivera att avgränsning presenteras separat. För mindre organisationer kan det samtidigt vara relevant att inkludera avgränsningen i sin helhet i policydokumentet, om

---

[26] *ISO 22313, avsnitt 4.1 samt 4.2.*

avgränsningen är att avse som relativt intakt och inte upptar alltför stort utrymme i dokumentet. Oavsett om avgränsningen beskrivs i policydokumentet eller i separat dokument, bör avgränsningen stämmas av med och beslutas av verksamhetens ledning.

Avgränsningen förutsätter att organisationen har en tydlig bild av kontexten den verkar inom. Avgränsning av vilka delar som bör inkluderas i kontinuitetsarbetet kan göras utifrån produkter eller tjänster, samt efter processer som utförs för att leverera produkterna eller tjänsterna. Den kan även göras organisatoriskt eller geografiskt där vissa avdelningar, enheter, eller länder inkluderas. Samtidigt bör arbetet inte utelämna en avdelning eller enhet som är kritisk för en produkt eller tjänst som inkluderats i arbetet. Värt att påpeka är att kontinuitetshantering är en process som svårligen byggs upp på en gång. Därför kan det vara en god idé att inledningsvis göra en relativt snäv avgränsning av vad som inkluderas i kontinuitetshanteringen för att därefter komplettera och bygga upp en mer heltäckande hantering.

Organisationen bör hitta en lämplig metod för att prioritera vilka delar av organisationen som ska ingå i kontinuitetshanteringen. Exempelvis kan olika typer av kostnad-nytta-analyser genomföras, eller SWOT-analys[27]. Inriktning torde även kunna ges från organisationens finansiella planering. Det kan även finnas krav eller önskemål från kunder eller från regelverk om att vissa delar ska täckas av kontinuitetshantering. Andra anledningar kan vara att särskilda produkter eller tjänster är särskilt tidskritiska eller genererar en stor andel av organisationens inkomster, eller att de anses samhällsviktiga. Organisationen kan också välja att inkludera vissa verksamhetsdelar med motiveringen att de har en hög riskexponering och därför bör belysas av kontinuitetshanteringen.

Avgränsningen bör även motivera varför vissa verksamhetsdelar eventuellt har uteslutits. En anledning kan vara att produkten eller tjänsten 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 inkomst 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 eller riktlinjer uppkommer.

[27] SWOT – Strengths, Weaknesses, Opportunities, Threats

A.3. 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 övriga delar av 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 sker avseende kontinuitetshanteringen. Roller och ansvar delas ofta in i strategisk, taktisk, och operativ nivå.

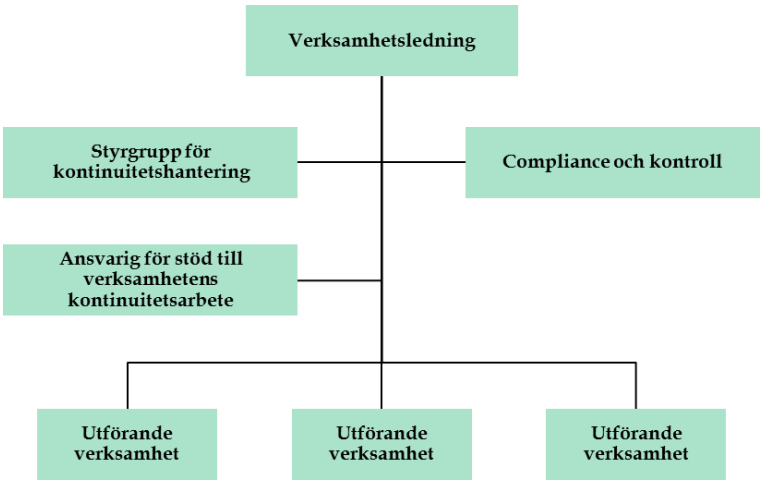
Med den strategiska nivån menas typiskt sett den högsta ledningen. Ansvar på denna nivå inkluderar ofta beslut av policyn och finansiering av kontinuitetsarbetet. Någon från ledningen bör ges ett övergripande ansvar för kontinuitetshanteringen och för arbetets effektivitet. Beroende på storlek och ambition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

Den taktiska nivån utgör kompetenscentra avseende kontinuitetshanteringen. Den taktiska nivån består av en person med det övergripande ansvaret för att stödja det arbete med kontinuitetshantering som bedrivs i verksamheten. 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 konkreta verksamhetsdelar 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 bör ha genomgått relevant utbildning. Ett exempel på hur roller och ansvar kan organiseras återges i diagrammet nedan. 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.



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.

Det är även av vikt att policyn tydliggör roller och ansvar gällande de olika slutprodukter som kommer ut av kontinuitetsarbetet. Detta kan inkludera, vem som ansvarar för respektive dokument, med vilken frekvens det ska uppdateras, vilken målgrupp det har samt var det finns sparat. Exempel på hur denna information kan formuleras i policyn ges i nedanstående tabell.

Dokument	Ansvar	Uppdatering	Målgrupp	Lagringsyta
• *Namn på dokument*	• *Vem beslutar?* • *Vem utvecklar?* • *Vem underhåller?*	• *Årligen?* • *Vid väsentliga förändringar?*	• *Kännedom för processansvariga?* • *Kännedom för samtliga inom organisationen?*	• *Var sparas dokumentet och i vilken form?*

A.4. Metod och rutiner

Policyn bör även beskriva vilka metoder och rutiner som är relevanta i arbetet med kontinuitetshantering. När organisationen tar fram en policy kan det här även vara nyttigt att lyfta fram standarder eller vägledningar som följs, såsom ISO 22301. Hänsyn bör även 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 även en gap-analys belysa hur policyn förhåller sig till eventuell benchmark i 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.

A.5. Kriteriemodell

I policyn fastställs även vilka typer av avbrott och konsekvenser som kontinuitetshanteringen söker motverka. Detta beslutas typiskt sett med stöd av en så kallad kriteriemodell. Det är viktigt att det finns en gemensam syn på verksamhetens riskacceptans, det vill säga var gränsen går för vilka konsekvenser som är acceptabla.

Format	• Utveckling av kriteriemodellen utförs med fördel genom en workshop • Viktigt att kriteriemodellen förankras inom hela ledningen
Deltagare	• Representanter från ledningen som har insyn i hela organisationen och har 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 definierar vilka konsekvenser som är acceptabla och oacceptabla

Vilka konsekvenser som organisationen anser vara acceptabla beskrivs genom kriteriemodellen där olika konsekvenskategorier (exempelvis ekonomi och rykte/varumärke) och konsekvensklasser (obetydlig, märkbar, allvarlig) definieras. Därefter beskrivs var gränsen för vad som är acceptabelt går. I exemplet nedan är gränsen för vad som är acceptabelt angiven med den svarta linjen mellan nivåerna märkbar och allvarlig. Med detta menas att konsekvenser inom ekonomi och rykte/varumärke är acceptabla upp till och med det som beskrivs inom nivån märkbar. Konsekvenserna inom nivån allvarlig bedöms inte som acceptabla.

	Obetydlig	**Märkbar**	**Allvarlig**
Ekonomi	Förlust < 500 000	Förlust < 5 000 000	Förlust > 5 000 000
Rykte/varumärke	Ingen förlust av kunder	Förlust av låg andel kunder	Förlust av stor andel kunder

I exemplet används tre konsekvensklasser. Kriteriemodellen skulle även kunna ange ett större annat antal klasser om det skulle anses lämpligt att segmentera analysen ytterligare, exempelvis genom att använda nivåerna *obetydlig*, *märkbar*, *allvarlig* och *katastrofal*. På ett liknande sätt kan fler konsekvenskategorier än ekonomi och rykte/varumärke läggas till i kriteriemodellen baserat på vilka områden organisationen anser lämpliga, exempelvis påverkan på verksamhetens funktionalitet. Vidare kan olika konsekvenskategorier vara relevanta endast för specifika delar av verksamheten. Därför kan olika kategorier läggas till/tas bort för specifika verksamhetsdelar. Viktigt är dock att de olika konsekvensnivåerna samt beslut om vilka konsekvenser som är acceptabla

eller inte beslutas på en strategisk nivå och utifrån verksamhetens målsättning/krav från intressenter/legala krav. Det är även viktigt att definitionerna av respektive konsekvensklass är mätbara, detta för att minimera möjligheten att göra egna tolkningar.

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 verksamhetsdelarna gör 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

Policy

Exempelstruktur

1. Introduktion
   - Syfte och mål
   - Bakgrund och organisationens kontext
2. Avgränsning och omfattning
3. Roller och ansvar
4. Metoder och rutiner
5. Kriteriemodell

Checklista innehåll

- Introduktion
  - Vad betyder kontinuitetshantering för organisationen?
  - Vad är målsättningen med kontinuitetshantering i organisationen?
  - Vilken är målgruppen för policyn?
  - Vilka interna drivkrafter styr arbetet, exempelvis kunders och partners förväntningar?
  - Vilka externa drivkrafter styr arbetet, exempelvis lagar/regleringar
- Avgränsning och omfattning (om detta ej presenteras i separat dokument)
  - Vilka produkter och tjänster omfattas?
  - Vilka kritiska processer omfattas?
  - Geografisk avgränsning?
- Roller och ansvar
  - Vilka resurser finns att tillgå i organisationen för att implementera kontinuitetshantering?
  - Vem är högst ansvarig?
  - Vem är ansvarig för implementeringen/ansvarig för att driva kontinuitetshanteringsprogrammet
  - Vem är ansvarig för support?
- Metoder och rutiner
  - Metodval
  - Följs någon standard?
  - Gap-analys mot standarder
- Kriteriemodell
  - Vilka kriterier utgår organisationen för?
  - Vilken är organisationens riskacceptans?

Kriteriemodell

Struktur

Konsekvens-nivå / Konsekvens-Kategori	Märkbar	Betydande	Kritisk

Exempel på innehåll

Konsekvens-nivå / 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*

Struktur för redogörelse av avgränsningar

Detta dokument beskriver omfattningen av kontinuitetshantering som drivs av [ORGANISATIONEN]

Kontinuitetshanteringen inom [ORGANISATIONEN] har anpassats till den internationella standarden Samhällssäkerhet - Ledningssystem för kontinuitet - Krav (ISO 22301:2012).

Kontinuitetshanteringen omfattar [TJÄNSTERNA X, Y OCH Z]. Dessa tjänster levereras från [ORTERNA X, Y OCH X]. De kritiska processer som omfattas inom kontinuitetshanteringen är [PROCESS A, B, C]. Kontinuitetshanteringen inkluderar alla aktiviteter samt interna och externa resurser som dessa kritiska processer är beroende av.

Detta avgränsningsdokument utfärdades den [XX MÅNAD XXXX] och kommer att ses över senast den [XX MÅNAD XXXX].

Undertecknat för [ORGANISATIONENS] räkning:

_____

Namnförtydligande: [FÖRNAMN, EFTERNAMN, BEFATTNING]
Datum: [XX MÅNAD XXXX]

Kartläggning av intressenters förväntningar/krav

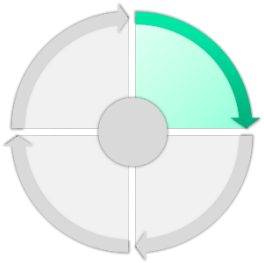
Process A

Intressenter	Förväntningar/krav vid normalläge	Förväntningar/krav vid avbrott	Prioritet
Kunder			
Investerare			
Anställda			
Leverantörer			
Tillsynsmyndigheter			
Partners			
Media			
…			
Bedömning genomförd av ……		Datum för bedömning ……..	

Process B

Intressenter	Förväntningar/krav vid normalläge	Förväntningar/krav vid avbrott	Prioritet
Kunder			
Investerare			
Anställda			
Leverantörer			
Tillsynsmyndigheter			
Partners			
Media			
…			
Bedömning genomförd av ……		Datum för bedömning ……..	

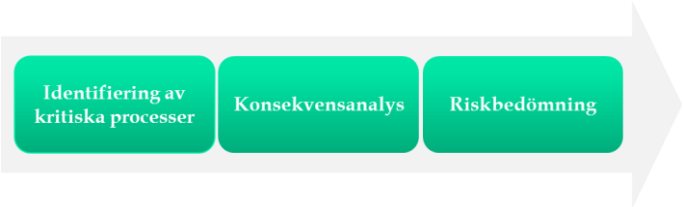
Appendix B - Analys av verksamheten



Eftersom en verksamhet syftar till att leverera produkter och/eller tjänster till sina kunder är det centralt att skapa en förståelse för hur avbrott i dessa leveranser påverkar verksamhetens operativa förmåga och möjligheten att uppnå fastställda verksamhetsmål. Verksamheten bör därmed fastställa, implementera och upprätthålla en strukturerad och dokumenterad process för att analysera verksamheten, dess underliggande beroenden samt befintlig redundans.

Steget analys av verksamheten syftar till att skapa en tydlig bild över verksamhetens kritiska processer, de processer som med hjälp av kontinuitetshanteringen ska upprätthållas på en tolerabel nivå. För var och en av de kritiska processerna genomförs en konsekvensanalys[28] som klargör hur beroendekedjorna ser ut samt vilka krav på tillgänglighet och kvalitet som bör ställas på processerna för att upprätthålla kontinuitet. Avslutningsvis inkluderar detta steg även en riskbedömning för att avgöra om de befintliga kontinuitetslösningarna är tillräckliga för att möta uppsatta krav på tillgänglighet. Genomförandet av detta steg skapar en förståelse för verksamheten och fastställer en utgångspunkt för det fortsatta arbetet med utveckling av kontinuitetsstrategier samt utveckling av 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 av verksamheten och använda dessa erfarenheter som ingångsvärden vid revision av policyn. Detta eftersom de initiala avgränsningarna och urvalet av verksamhets-/tjänsteområden kan behöva revideras efter att en första analys gjorts i verksamheten. Steget Analys av verksamheten kan delas in i tre delar:



[28] *BIA - Business Impact Analysis, ISO 22301*

B.1. Identifiering av kritiska processer

Det första steget i analysarbetet är att identifiera kritiska processer, för att sedan genom det fortsatta arbetet säkerställa att de alltid kan levereras. Identifieringen görs med utgångspunkt i vilka processer som är viktiga för att organisationen ska kunna uppnå sina verksamhetsmål samt eventuella legala krav som ställs på organisationen. Om verksamheten redan i policyn gjort avgränsningar på processnivå kan detta steg hoppas över, men om policyn enbart avgränsar på produkt-/tjänstenivå så behöver avgränsningen konkretiseras ytterligare i enlighet med detta steg. Dock ska identifieringen av kritiska processer utgå från innehållet i policyn samt den inriktning som fastställts där. Om verksamhetens kritiska processer har identifierats och beskrivits i tidigare arbete, exempelvis i genomförda processkartläggningar eller verksamhetsbeskrivningar, bör det underlaget tas med i kontinuitetsarbetet. Det är viktigt att urvalet av kritiska processer har stöd från verksamhetsledningen, annars riskerar arbetet att stagnera och de som är ansvariga för analysen blir inte benägna att avsätta tid, alternativt känner att de inte har tillräckligt mandat att driva arbetet i mål. Inför den fortsatta analysen är det bra att inventera eventuellt kontinuitetsarbete som tidigare gjorts inom organisationen, detta kan vara processkartläggningar eller återstartsrutiner för kritiska IT-system.

I arbetet med att identifiera kritiska processer kan olika typer av verksamhetsprocesser inkluderas, det är dock viktigt att säkerställa att det är faktiska processer som väljs ut och inte enbart styras av organisationsstrukturen. I ISO 22301 definieras en process som *"en grupp av samverkande eller varandra påverkande aktiviteter som omformar ingångsvärden till resultat"*[29], definitionen understryker med andra ord att en process bör bestå av en kedja av värdeskapande aktiviteter. Exempel på processer för finansiella aktörer kan exempelvis vara utlåning eller valutahandel för en bank samt skadehantering eller återförsäkring för ett försäkringsbolag.

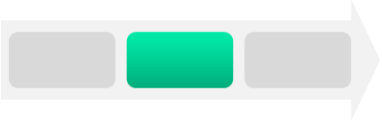
När konsekvensanalys genomförs för de utvalda kritiska verksamhetsprocesserna genereras kravställning gentemot kritiska interna stödprocesser som exempelvis IT-tjänster eller personalfunktioner. Stödprocesserna kan då i ett nästa steg analyseras vidare med utgångspunkt i verksamhetens identifierade krav. För IT-tjänster blir analysen ofta omfattande och en beskrivning av hur denna analys kan genomföras finns i Appendix F – *Kontinuitetshantering för IT-verksamheten*.

Avslutningsvis utses en processägare för varje process som därmed ansvarar för att genomföra efterföljande steg för processen. Processägaren bör i sin tur säkerställa att tillräcklig kompetens finns i form av personer med operativ kunskap om verksamheten samt eventuella experter kopplat till kritiska system eller andra områden.

---

[29] *Set of interrelated or interacting activities which transforms input into output (ISO 22301)*

B.2. Konsekvensanalys



Syftet med konsekvensanalysen är att identifiera de aktiviteter som stödjer att de kritiska processerna kan tillhandahållas, samt identifiera de interna och externa resurser som behövs för att aktiviteterna ska kunna utföras. Genom konsekvensanalysen fastställs hur långa avbrott som kan accepteras vilket ger stöd för prioritering vid återställning av identifierade aktiviteter. Aktiviteternas tidsgränser ställer i sin tur krav på hur länge de underliggande resurserna kan vara otillgängliga. Att ha kunskap om hur olika kritiska resurser kan påverka verksamhetens förmåga att utföra en aktivitet är central för att säkerställa kontinuitet i verksamheten.

Format	• Konsekvensanalysen utförs med fördel genom en workshop för respektive identifierad kritiska process • Som komplement kan intervjuer göras. Dessa riskerar dock ofta att bli tidskrävande och att man förlorar kontrollen över format och detaljgrad. Även enkäter kan användas men då kan i 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 tolerabla avbrottsperioder för aktiviteter samt mål för återställningstid för resurser

Första steget i konsekvensanalysen är att identifiera vilka kritiska aktiviteter som måste kunna utföras för att säkerställa att de kritiska processerna fungerar. Detaljeringsgraden för hur aktiviteter definieras kan ges stöd av hur komplexa avbrotts- och återgångsrutiner som aktiviteten har och om olika moment inom aktiviteten är olika tidskritiska. I figuren nedan visas hur de identifierade aktiviteterna kan presenteras i form av ett förenklat exempel för processen ”Skadehantering” för ett försäkringsbolag.

Skadehantering

Om en aktivitet innefattar moment som har olika lösningar vid avbrott och/eller är olika tidskritiska, så bör den delas upp i olika aktiviteter. Detta görs genom att analysera varje kritisk process och identifiera kritiska aktiviteter. Säkerställ även att samtliga aktiviteter numreras. Detta steg är grunden för hela analysen så det är viktigt att säkerställa att alla kritiska aktiviteter är med, men även att aktiviteter som inte är kritiska sorteras bort.

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)

För att kunna utföra de identifierade kritiska aktiviteterna krävs i sin tur både interna och externa resurser. Nedan ges några exempel på övergripande resurstyper som kan användas som en checklista för att alla typer har inkluderats.

Interna resurser:

- Personal och kompetens
- Lokaler, anläggningar och annan utrustning
- Informations- och kommunikationsteknik

Externa resurser:

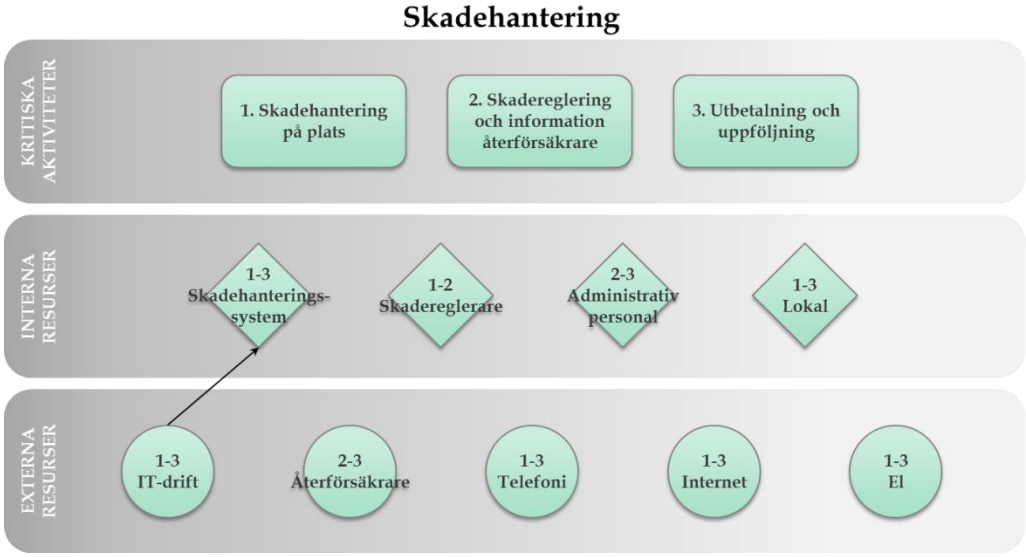
- Tjänsteleverantör
- Externa IT-system
- El
- Internet
- Telefoni

För varje aktivitet identifieras därmed de interna och externa resurser som behövs för att utföra respektive aktivitet. Resurserna bör definieras mer detaljerat än i exemplen ovan. För respektive resurs, notera även vilka aktiviteter som är beroende av den, genom att sätta aktivitetens siffra vid resursen. Genom att använda pilar kan specifika beroenden mellan resurser markeras i kartan.

TIPS FÖR GENOMFÖRANDE:

- Ta en aktivitet i taget och identifiera de interna och externa resurser som behövs för att genomföra aktiviteten
- Resurser som hänger ihop och är lika tidskritiska kan grupperas i kartan, tänk då på att skriva en kommentar om vad som ingår i resursen

Resultatet av identifiering av aktiviteter samt interna och externa resurser presenteras i en karta som visualiserar processens underliggande beroendekedjor. I figuren nedan visas hur de identifierade aktiviteterna och resurserna kan presenteras i för det förenklade exemplet "Skadehantering".



När kritiska aktiviteter samt interna och externa resurser identifierats för en kritisk process är nästa steg att definiera hur långa avbrott som kan tolereras i respektive aktivitet, vilket benämns som den maximalt tolerabla avbrottsperioden. För att definiera maximal tolerabel avbrottsperiod för en aktivitet används den tidigare utvecklade kriteriemodellen som definierar organisationens riskacceptans.

	Obetydlig	**Märkbar**	**Allvarlig**
Ekonomi	Förlust < 500 000	Förlust < 5 000 000	Förlust > 5 000 000
Rykte/varumärke	Ingen förlust av kunder	Förlust av låg andel kunder	Förlust av stor andel kunder

Den längsta tid som ett avbrott kan fortgå, utan att konsekvenserna blir så allvarliga att de enligt kriteriemodellen definieras som oacceptabla, är den tid som är aktivitetens maximalt tolerabla avbrottsperiod.

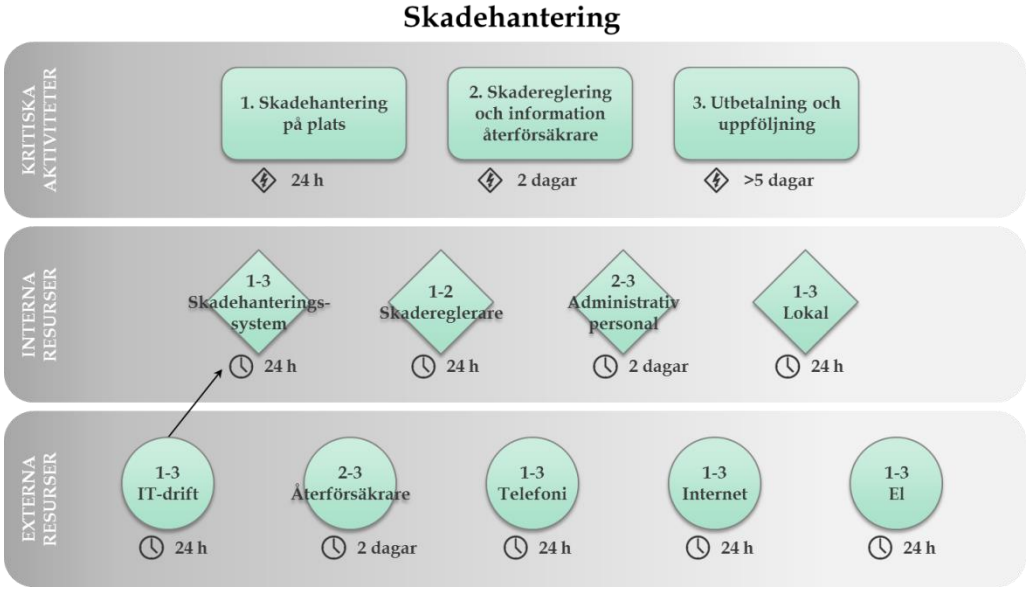
Skadehantering

De maximalt tolerabla avbrottsperioderna kan variera från minuter till månader beroende på vilken typ av aktivitet det handlar om, för mer tidskritiska aktiviteter bör den maximalt tolerabla avbrottsperioden specificeras med mer noggrannhet än för mindre tidskritiska aktiviteter. Ledtider kan ingå i bedömning av den maximalt tolerabla avbrottsperioden, exempelvis att vissa aktiviteter måste startas om från början medan andra kan fortsätta direkt från den tidpunkt där avbrottet skett. Görs sådana bedömningar är det dock viktigt att antaganden och omständigheter tydligt noteras och lyfts fram. Om det finns en "kalenderrelation" där konsekvenserna är mer påtagliga vid olika tidpunkter (månadsslut, årsslut, kontraktsperioder) ska analysen utgå ifrån att en eventuell incident faktiskt sker under dessa kritiska perioder.

TIPS FÖR GENOMFÖRANDE:

- För varje aktivitet ställs frågan "Hur länge kan aktiviteten ligga nere innan något av kriterierna i de röda kolumnerna uppfylls?", den tid som är svaret på frågan är den maximalt tolerabla avbrottstiden för den aktuella aktiviteten
- Notera motivering för satta tidskrav
- Tänk på att mäta mot samtliga konsekvenskategorier 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

En aktivitets maximalt tolerabla avbrottsperiod avgör vilket mål för återställningstid som ställs på respektive resurs. Med detta menas den tid inom vilken resursen måste kunna återgå till normal funktion efter ett avbrott. Ofta sätts mål för återställningstid med en säkerhetsmarginal i förhållande till den maximalt tolerabla avbrottsperioden. För resurser som är beroende av ytterligare resurser är det viktigt att ta hänsyn till hela beroendekedjan inför fastställande av mål för återställningstid för respektive resurs. Analysen genomförs genom att ta en resurs i taget och se vilka aktiviteter den stödjer, utgå ifrån de aktuella aktiviteternas maximalt tolerabla avbrottsperioder, mål för återställningstid för resursen måste då vara i nivå med den kortaste maximalt tolerabla avbrottsperioden. Detta steg genomförs för var och en av de interna och externa resurserna.

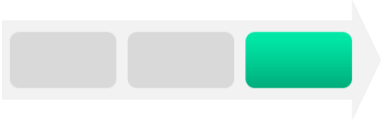


Det finns olika sätt att dokumentera resultatet av konsekvensanalysen. Ett sätt är att visualisera hur beroendekedjan ser ut genom att dokumentera beroendena i en karta, på samma sätt som exemplen i detta avsnitt. Resultatet av analysen kan även dokumenteras i ett Excelark där aktiviteter, interna och 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. De definierade tidskraven används som stöd för prioritering vid upprätthållande av aktiviteter samt återhämtning av resurser. Det är viktigt att konsekvensanalysen beskriver hur processens beroendekedjor ser ut i ett normalläge, det betyder att den inte ska inkludera reservlösningar som exempelvis reservkraft.

Konsekvensanalys för outsourcad verksamhet

Om organisationen har delar av den verksamheten utlagd på en extern leverantör är det viktigt att leverantörens kritiska aktiviteter inkluderas i konsekvensanalysen. Även om en leverantör ansvarar för att utföra vissa aktiviteter är det den egna verksamhetens ansvar att säkerställa kontinuitet även i dessa aktiviteter. Precis som med urval av interna aktiviteter handlar det om att hitta en balans i vilka externa aktiviteter som är av sådan kritisk karaktär att de bör inkluderas i analysen.

B.3. Riskbedömning



Som sista steg i analysen av verksamheten görs en riskbedömning för att få en djupare förståelse för risker och hot som är kopplade till de resurser som stödjer kritiska processer. Detta för att avgöra om befintliga lösningar är tillräckliga för att säkerställa att de identifierade tidskraven inte överskrids, men även för att identifiera eventuella single-point-of-failures. I en riskbedömning inom ramen för kontinuitetshantering läggs fokus på den konsekvens en störning eller ett avbrott har, och framförallt på att analysera hur sannolikt det är att ett avbrott överskrider resursens mål för återställningstid. Målsättningen med riskbedömningen är att värdera vilka avbrottsrelaterade risker som kräver åtgärder samt att för dessa identifiera åtgärder för att uppfylla kontinuitetsmål i enlighet med organisationens riskacceptans. Riskbedömningen görs på en mer operativ nivå och är mindre detaljerad än traditionell riskhantering som bedrivs inom verksamheten (eventuellt med stöd av ISO 31 000), se även avsnitt 2.4, *Koppling till incident-, risk-, och krishantering*, för förtydligande av skillnader mellan kontinuitetshantering och riskhantering.

Format	• Riskbedömningen utförs med fördel genom en workshop • Som komplement kan intervjuer göras. Dessa riskerar dock ofta att bli tidskrävande och man förlorar kontrollen över format och detaljgrad. 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

Riskbedömningen utförs genom att för respektive resurs:

1. Identifiera händelser som kan påverka tillgängligheten hos resursen
2. Identifiera den befintliga redundansen för resursen
3. Bedöma sannolikhet för att en händelse orsakar ett avbrott hos resursen som överstiger fastställt mål för återställningstid
4. Prioritera resurserna utifrån var åtgärder bör vidtas
5. För de resurser där ytterligare kontinuitetslösningar behövs, beskriv behovet som en kommentar samt utse ansvarig och deadline.

I figuren nedan visas ett förslag på hur riskbedömningen för de kritiska resurserna kan dokumenteras, detta genom ett exempel där riskbedömning gjorts för resursen Skadehanteringssystem vilket var en av de identifierade interna resurserna för den förenklade exempelprocessen Skadehantering.

Kritisk resurs (Mål för återställningstid)	Händelser som kan påverka resursens tillgänglighet	Befintlig redundans	Sannolikhet att avbrott överstiger mål för återställningstid			Prioritet	Kommentar
			LÅG	MEDEL	HÖG		
Skadehanterings-system (24 h)	Elavbrott	Finns reservkraft samt diesel för 3 dagars drift	X			3	Viktigt med löpande test av reservkraft (ansvar: kontorschef)
	Internet ligger nere	Ingen redundans finns			X	1	Utred möjliga redundanslösningar (ansvar: IT-chef, klart: innan årsskiftet)
	Skadlig kod	Virusprogram finns, oklart om tillräckligt		X		2	Se över befintlig redundanslösning (ansvar: IT-chef, klart: innan årsskiftet)

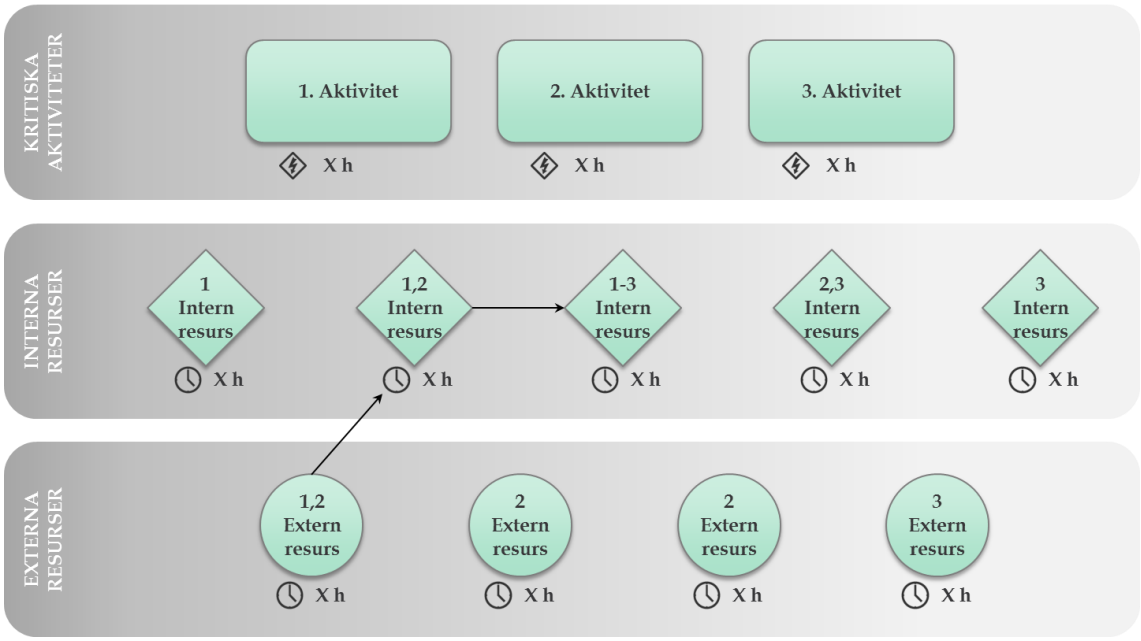
Utifrån riskbedömningen tas sedan beslut om vilka risker som måste minskas för att säkerställa att de maximalt tolerabla avbrottsperioderna för kritiska aktiviteter inte överskrids. Riskbedömningen kan även identifiera risker där den befintliga redundansen är onödigt hög.

TIPS FÖR GENOMFÖRANDE:

- De hot som tas upp syftar till att identifiera olika typer av redundanslösningar, så de kan med fördel grupperas
- Tänk på att vi bedömer sannolikheten att ett avbrott överskrider återhämtningstiden (inte sannolikhet att hotet inträffar)
- Notera utestående frågor, förslag på ytterligare reservlösningar samt övriga kommentarer. Utse gärna ansvarig samt sätt datum när respektive fråga ska vara hanterad.

Konsekvensanalys

Kritisk process

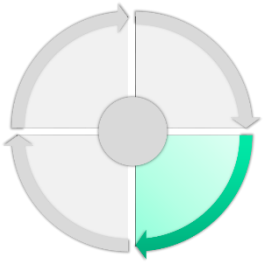


Kritiska aktiviteter / Kritiska resurser		Aktivitet 1	Aktivitet 2	Aktivitet 3	…	Kommentar
		X timmar	X timmar	X timmar		
Intern resurs 1	X timmar					
Intern resurs 2	X timmar					
…						
Extern resurs 1	X timmar					
Extern resurs 2	X timmar					
…						

Riskbedömning

Kritisk resurs (Mål för återställningstid)	Händelser som kan påverka resursens tillgänglighet	Befintlig redundans	Sannolikhet att avbrott överstiger mål för återställningstid			Prioritet	Kommentar
			LÅG	MEDEL	HÖG		

Appendix C - Kontinuitetsstrategi



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

Kontinuitetsstrategier sätts på en övergripande nivå och utgör en inriktning för vilka lösningar och åtgärder som ska implementeras. Kontinuitetsstrategier tjänar främst ett syfte vid storskalig kontinuitetshantering. Om kontinuitetsarbetet inleds på en liten del av verksamheten eller på lokal nivå kan strategier tas fram först senare i arbetet, då kontinuitetshanteringen implementeras i hela verksamheten. 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, resurser och beroenden har genomförts. 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 längre eftersom den innebär alltför stora risker, alternativt förändrar 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 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 tredje part 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.

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 med konkreta kontinuitetslösningar i händelse av avbrott.

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*	*2-5 dagar*	*2-24 timmar*	*0-2 timmar*
	Återhämta när lämpligt	*Återhämta*	*Återhämta snarast*	*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*

C.4. Kontinuitetsstrategier för outsourcad verksamhet

För de fall där organisationen är beroende av externa leverantörer exempelvis genom outsourcing bör kontinuitetsstrategierna inkludera hur identifierade krav ska kunna mötas för de kritiska resurser som levereras av en extern part. Detta bör göras genom att identifiera de krav som bör ställas på de externa leverantörerna, exempelvis i form av krav på robust utrustning och skalskydd, krav på att kontinuitetsanalyser ska delges eller krav på regelbundna, och eventuellt gemensamma, övningar och tester. Strategierna kan också inkludera att skaffa alternativa leverantörer. Det är viktigt att säkerställa att en leverantör inte utgör single-point-of-failure. Leverantörsstrategier inkluderar ofta en avvägning mellan få leverantörer med vilka organisationen har goda relationer eller många leverantörer med ytligare relationer.

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 värdera alternativa lösningar jämfört 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.

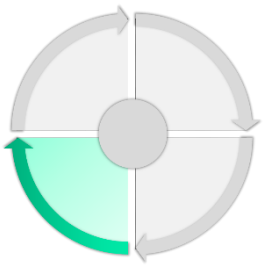
Exempel på struktur för kontinuitetsstrategi

1. Introduktion
2. Strategier för personella resurser
   a. Före
   b. Under
   c. Efter
3. Strategier för lokaler och utrustning
   a. Före
   b. Under
   c. Efter
4. Strategier för system och teknisk infrastruktur
   a. Före
   b. Under
   c. Efter
5. Strategier för externa leverantörer
   a. Före
   b. Under
   c. Efter
6. Strategier för övriga resurser
   a. Före
   b. Under
   c. Efter

Exempel på struktur för 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 kontinuitetsprocessen identifieras konkreta kontinuitets-lösningar som sedan beskrivs i kontinuitetsplaner. Viktigt är att de lösningar som beskrivs i dokumentet beskriver såväl hur kontinuiteten i identifierade kritiska resurser ska upprätthållas, hur resursen återställs vid störningar samt hur återgång till normalläge ska ske då resurserna åter fungerar som normalt.

Kontinuitetslösningarna beskrivs ofta som ett antal checklistor med tydliga beskrivningar av roller, ansvar och befogenheter, samt nödvändiga kontaktuppgifter. Kontinuitetsplanerna aktiveras vid behov för att kunna upprätthålla kritiska processer och möjliggöra för en snabb återgång till normal verksamhet. Kontinuitetsplanerna kan, men behöver inte, vara separata dokument, utan kan inkorporeras i befintliga planer och dokument. 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

Kontinuitetsplanen kan utgöras av ett eller flera dokument. Hur mycket och vilken information som paketeras i en och samma plan baseras på vilka de tänkta användarna är, vilket skulle kunna innebära en plan för varje process eller att planerna följer annan, befintlig organisationsstruktur. Det viktiga är att de tänkta användarna kan finna all relevant information i planen, samtidigt som, för dem icke relevant information återfinns i någon annan plan. På så sätt undviks både glapp och överlappning av information.

Nedan listas ett antal rubriker som bör 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 kontinuitetslösningar**

  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.

  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 skadehantering 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.

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 redogörs ett exempel på kontinuitetslösning för den kritiska resursen verksamhetens lokaler, 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 datorer.

Kritiska lokaler/utrustning (Mål för återställningstid)	**Kontinuitetslösningar**
Verksamhetens lokaler (8 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)
Datorer (2 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)

D.1. Kontinuitetsplaner för outsourcad verksamhet

Ett separat avsnitt i kontinuitetsplanen bör riktas mot externa leverantörer som outsourcad verksamhet. Dessa lösningar inkluderar ofta hur omfördelning till interna processer eller till alternativa leverantörer kan ske. Lösningarna beskrivs i konkreta termer exempelvis genom rutiner och checklistor. Kontaktuppgifter till de externa leverantörerna bör också anges tydligt i planen, samt vem inom den egna verksamheten som ansvarar för kontakten med leverantören. Reservlösningarna kan inkluderas i verksamhetens övergripande kontinuitetsplan(er) eller dokumenteras i en eller flera separata planer där inledningen baseras på olika typer av leverantörer eller utgår ifrån vem som har huvudsakligt ansvar för olika leverantörer.

Kontinuitetsplan för verksamheten

Denna kontinuitetsplan beskriver de reserv-, återställnings- och återgångsrutiner som används för att för att säkerställa kontinuiteten i prioriterad verksamhet, 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*
2. *Användning och eskalering av kontinuitetsplanen*
3. *Beskrivning av kontinuitetslösningar*
4. *Bilagor*

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 kontinuitetslösningar (beskrivs med fördel i checklisteformat)*

I denna kontinuitetsplan är kontinuitetslösningarna indelade enligt resurstyp.

Personal

Nyckelperson/funktion (mål för återställningstid)	**Kontinuitetslösningar**
Resurs A (X timmar)	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 återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*
Resurs B (X timmar)	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 återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

Lokaler och utrustning

Lokaler/utrustning (mål för återställningstid)	**Kontinuitetslösningar**
Resurs C (X timmar)	
Resurs D (X timmar)	

System och teknisk infrastruktur

System/teknisk infrastruktur (mål för återställningstid)	**Kontinuitetslösningar**
Resurs E (X timmar)	
Resurs F (X timmar)	

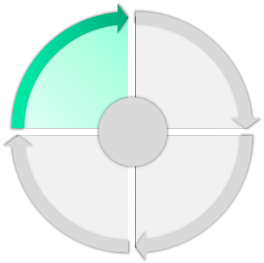
Externa beroenden/leverantörer

Externa beroenden/ leverantörer (mål för återställningstid)	**Kontinuitetslösningar**
Resurs G (X timmar)	
Resurs H (X timmar)	

4. *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 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 utbildningar och övningar 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, som nya IT-system, organisationsförändringar eller byte av leverantörer, bör en revidering göras. Revideringar kan till exempel göras för de styrande dokumenten eller i analys av verksamheten då större förändringar skett. Tänk på att revideringar av exempelvis styrande dokument, såsom kriteriemodellen, leder till att revideringar i de efterföljande stegen i kontinuitetshanteringsprocessen måste genomföras.

Revision och granskning kan genomföras både av interna och externa parter. Det bör, i de interna rutinerna, finnas en process för hur regelbundna interna granskningar ska ske. Det bör också vara tydligt definierat hur resultat från granskningar ska tillvaratas.

E.2. Övning

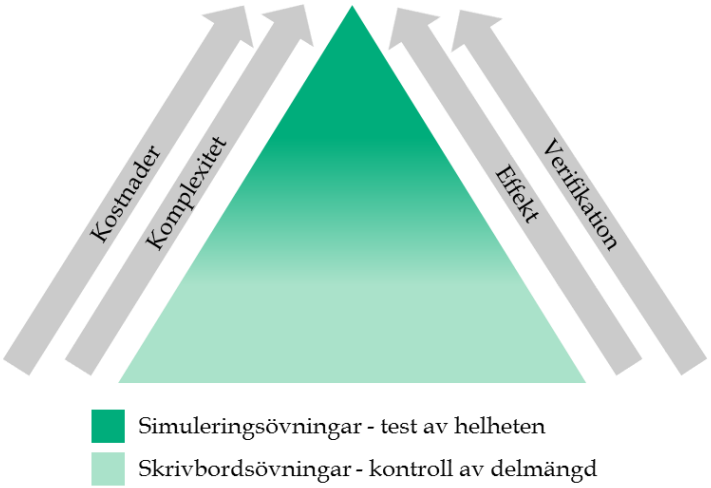
Det är utöver granskning och revidering viktigt att regelbundet öva och testa de implementerade kontinuitetsplanerna för att säkerställa att befintliga kontinuitetslösningar är tillräckliga för att möta de tidskrav som satts upp. Dessutom kan resultaten från övningar och tester leda till revidering av kontinuitetsarbetet.

Omfattning och frekvens av övning och test 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 testresurserna optimeras. En övningsstrategi för att säkerställa regelbundna och målinriktade övningar bör inkluderas i den övergripande kontinuitetsstrategin.

Övningar kan bland annat syfta till att:

- **Testa teknik och infrastruktur**
  - *Fungerar det?*
  - *Har vi tillgång till rätt lokaler, utrustning och teknik?*
- **Öka kompetens bland personalen**
  - *Är det rätt personal som är involverad – kompetens, förmåga, beslutsrätt?*
  - *Utveckla individers och gruppers förmåga*
  - *Testa förmågor under press*
- **Testa uppsatta tidskrav**
  - *Går tidskraven att möta?*
  - *Är befintliga logistik-/leverantörslösningar tillräckliga?*
- **Öka medvetenheten i organisationen**

Övning och testning av kontinuitetslösningar kan exempelvis göras för manuella rutiner eller för flytt till reservlokal. Tester av kontinuitetslösningar gällande system kan göras på olika sätt, exempelvis kan ”fail over” (vilket innebär automatisk övergång till ett annat redundant system då ordinarie system är ur funktion) testas genom att stänga ner ordinarie system och se om reservlösningen fungerar. Storleken på övningar kan variera, från lokala övningar för enskilda eller mindre grupper i organisationen till mer omfattande övningar för delar av eller hela organisationen. Övningar kan också genomföras tillsammans med externa aktörer såsom exempelvis leverantörer eller outsourcingpartners för att testa att de kan möta de krav som ställs på dem eller att de redundanslösningar de erbjuder är tillräckliga.



Beroende på organisationens vana av att arbeta med kontinuitetshantering samt tidigare erfarenheter av att öva kan och bör övningarnas komplexitet anpassas. För oerfarna övningsdeltagare lämpar sig så kallade skrivbordsövningar bäst. I sådan övas deltagarna främst genom att *diskutera* olika typer av ageranden utifrån ett givet scenario. Övningsformen är framför allt lärande. För mer erfarna övningsdeltagare kan en simuleringsövning vara lämplig. En sådan övning har ofta ett mer testande fokus och deltagarna ska, utifrån ett scenario, *agera* enligt de rutiner och instruktioner som finns.

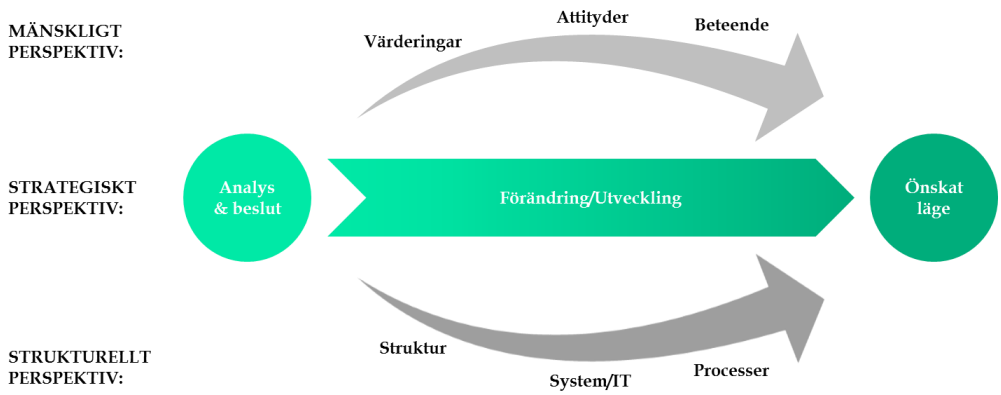
E.3. Utbildning

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 kontinuitetshanteringsarbete 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 och längre utbildningar som syftar till att förklara metoder och tillvägagångssätt.

E.4. Kultur för kontinuitetshantering

Test, övning och utbildning 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, ledningen har belyst vikten av och tilldelat tillräckliga resurser till arbetet, och kontinuitetshantering är integrerat i alla delar av verksamheten och utförs inte endast 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 ett beslut om önskat läge och tar fram tidplaner och 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 måste inkluderas, men glöms ofta bort, i förändringsprocesser. Det är viktigt att skapa förståelse bland medarbetare och andra intressenter kring varför och hur förändringen ska genomföras och hur den kan vara värdeskapande för de enskilda individerna.

Genomförande av förändring bygger på en insiktsfull integration av de tre perspektiven, där alla är viktiga för en effektiv implementering i organisationen. I ett kontinuitetshanteringsperspektiv kan det strategiska perspektivet beaktas genom exempelvis policyn, där beslut fattas om arbetets omfattning och om resurstilldelning. Det strukturella perspektivet kan beaktas genom framtagande av checklistor och mallar för de olika stegen i kontinuitetshanteringsprocessen eller inköp av IT-system som ska stödja arbetet. Det mänskliga perspektivet bör 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

Genom arbetet med kontinuitetshantering kommer krav att ställas på de resurser verksamheten är beroende av. IT-verksamheten är en av dessa resurser och specifika krav kommer därför att ställas på denna. I detta avsnitt presenteras hur dessa krav kan mötas genom ett systematiskt arbete med kontinuitetshantering, även i IT-verksamheten.

F.1. Analys av verksamheten

Konsekvensanalys

Baserat på de konsekvensanalyser som genomförts för de kritiska processerna kommer verksamheten att ha ställt tillgänglighetskrav på olika IT-system och -tjänster. För dessa system och tjänster behöver IT-organisationen utreda hur beroendekedjan ser ut. Den övergripande metoden är densamma som för verksamhetsprocesserna, skillnaden är IT-organisationens analys utgår från de aktuella systemen och tjänsterna istället för att utgå från processer och aktiviteter.

Innan konsekvensanalysen inleds måste verksamhetens krav på IT-system och -tjänster sammanställas, detta för att få en samlad bild över vilka system som ska inkluderas i konsekvensanalysen.

Första steget i konsekvensanalysen för IT är sedan att identifiera de interna och externa resurser som behövs för att kunna leverera respektive system/tjänst. Nedan ges några exempel på övergripande resurstyper som kan användas som en checklista för att alla typer har inkluderats.

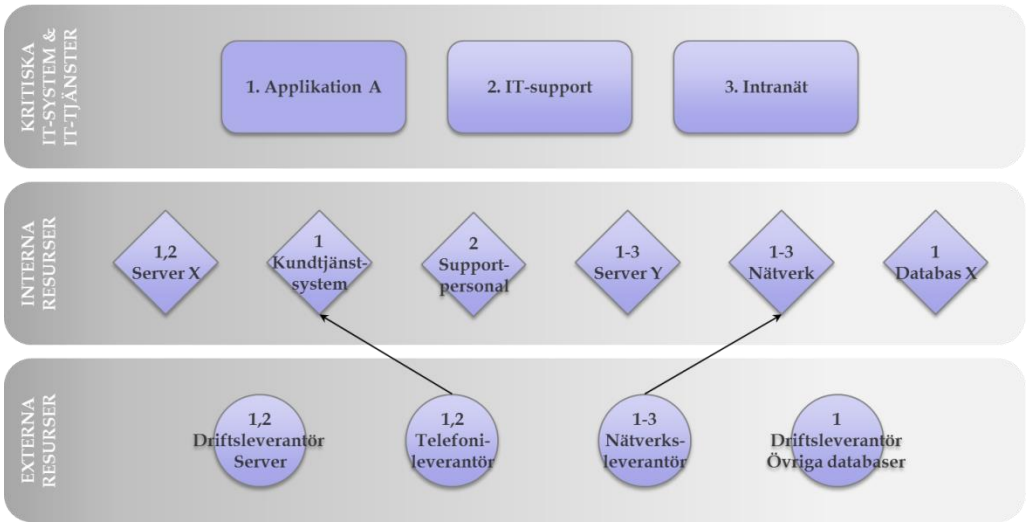
Interna resurser:

- Personal och kompetens
- Lokaler
- Servrar
- Databaser
- Nätverk
- Applikationer
- Informations- och kommunikationsteknik

Externa resurser:

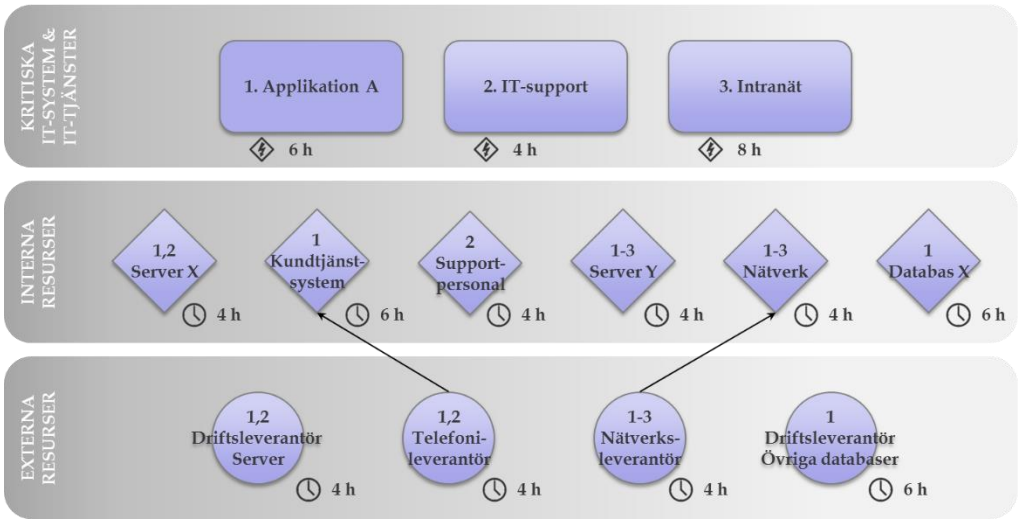
- Tjänsteleverantör
- Externa IT-system
- El
- Internet
- Telefoni

För respektive resurs, notera vilka system/tjänster som är beroende av den, genom att sätta systemets/tjänstens siffra vid resursen. Genom att använda pilar kan specifika beroenden mellan resurser markeras i kartan. Detaljeringsgraden av hur resurserna definieras kan ges stöd av hur komplexa avbrotts- och återgångsrutiner som resursen har.



De lägsta tillgänglighetskrav som verksamheten har ställt på respektive system/tjänst styr vilka mål för återställningstider som i nästa led ställs på de underliggande interna och externa resurserna. Där mål för återställningstid för ett system skiljer sig åt mellan olika delar av verksamheten styr det kortaste tidskravet vilka återställningsrutiner som måste finnas på plats.

Analysen genomförs genom att ta en resurs i taget och se vilka system/tjänster den stödjer, återställningstiden för resursen måste vara i nivå med det kortaste tillgänglighetskravet. Detta steg genomförs för var och en av de interna och externa resurserna. Även här sätts mål för återställningstid med en säkerhetsmarginal i förhållande till tillgänglighetskravet på systemet/tjänsten. För resurser som är beroende av ytterligare resurser är det viktigt att ta hänsyn till hela beroendekedjan inför fastställande av mål för återställningstid för respektive resurs. I de fall där resursen har att göra med lagring av data är det också relevant att definiera krav på återhämtningspunkt vilket innebär krav på hur gammal data maximalt får vara för att medge funktionalitet i den kritiska aktiviteten.



Riskbedömning

Precis som för organisationens verksamhetsprocesser avslutas steget Analys av verksamheten med att göra en riskbedömning för identifierade kritiska resurser. Metoden för att genomföra riskbedömningen är densamma även för IT-verksamheten (se Appendix B - *Analys av verksamheten* under avsnitt B.3. *Riskbedömning*).

F.2. Kontinuitetsstrategier

Liksom för övriga delar av verksamheten kan och bör kontinuitetsstrategier upprättas för IT-system och tjänster. Hur dessa strategier formuleras baseras på kravställning från verksamheten. Vilka krav som ställs på IT-verksamheten, liksom på övriga kritiska resurser, är ett resultat av den analys av verksamheten som genomförts i tidigare steg av kontinuitetsanalysen. De strategier som formuleras på IT-nivå ska syfta till att möjliggöra för de kritiska aktiviteterna och resurserna att möta de tidskrav som identifierats för den övergripande verksamheten. En tät dialog mellan verksamheten och IT-nivån bör ske i detta arbete. Kontinuitetsstrategierna för IT-verksamheten kan formuleras i samma dokument som kontinuitetsstrategierna för övriga verksamheten.

Vid val av vilka strategier som ska implementeras måste tillgängliga resurser analyseras och beslut fattas kring eventuella investeringar i ytterligare resurser. En kostnad-nyttoanalys bör därför göras.

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

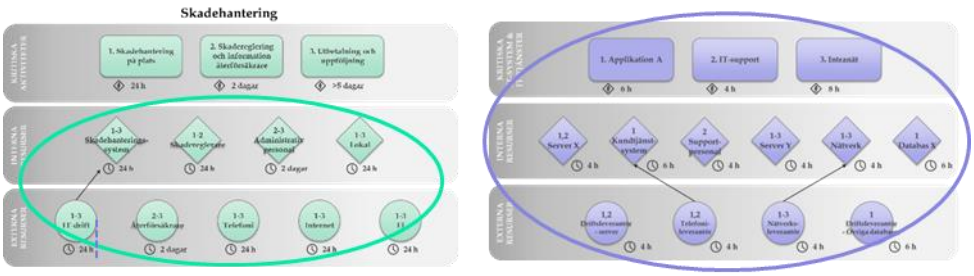
- Personal och kompetens: exempelvis spridning av kunskaper genom att dokumentera hur kritiska ICT-tjänster genomförs eller användandet av multikompetent personal.
- Lokaler: exempelvis alternativa lokaler. I dessa fall är det viktigt att beakta säkerheten på den alternativa platsen, vilka som har tillträde etc.

- Teknologi: 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 nyttjas kan, liksom för de övergripande kontinuitetsstrategierna, grundas på hur kritiska de olika resurserna är. Det kan sammanställas i en tabell enligt ovan, där de kritiska systemen och komponenterna grupperas enligt mål för återställningstider.

F.3. Kontinuitetsplaner

Kontinuitetsplaner ska upprättas även för de IT-system och -tjänster som verksamheten är beroende av. Inom IT-området är disaster recovery-, back up- eller återhämtningsplaner etablerade begrepp. Syftet med dessa typer av planer är att skapa en beredskap och förmåga att hantera oönskade händelser som innebär att de kritiska resursernas/systemens uppsatta tidskrav riskerar att överskridas. Tidskraven baseras på den analys som görs av IT-verksamheten och dess kritiska system och resurser. Denna analys bygger i sin tur på den analys som gjorts av den övergripande verksamheten där tidskrav ställs på de kritiska resurserna, och där IT-verksamheten identifierats som en kritisk resurs. På så sätt kravställer den övergripande verksamheten system och resurser i IT-verksamheten.



Fokus i kontinuitetsplaner för verksamheten

Fokus i kontinuitetsplaner för IT-system och - tjänster

Enligt ISO 27031 bör kontinuitetsplaner 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.

För de resurser och system som bedöms vara kritiska för verksamheten beskrivs kontinuitetslösningar i form av reservrutiner (exempelvis övergång till andra system, manuella rutiner eller back-up-lösningar), återställningsrutiner (beskrivning av hur de kritiska systemen ska återställas vid störningar) och återgångsrutiner (hur de kritiska systemen ska återställas vid störningar).

Beroende på IT-verksamhetens storlek och komplexitet kan en plan innehållandes återställningsrutiner och kontinuitetslösningar för samtliga system/resurser tas fram alternativt utvecklas flera planer där system/resurser grupperas enligt relevanta kriterier, exempelvis enligt hur olika system förhåller sig till och är beroende av varandra. För respektive system kan också uppdelningar på olika nivåer göras, exempelvis applikationsnivå, databasnivå, säkerhetsfunktioner, operativsystem, virtuella servrar, fysiska servrar och nätverk.

Kontinuitetsplan för IT-system och – tjänster

Denna kontinuitetsplan beskriver de reserv-, återställnings- och återgångsrutiner som används för att för att säkerställa kontinuiteten i system och resurser inom IT-verksamheten, oavsett vad som inträffat. 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.

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

Innehållsförteckning:

1. *Dokumentinformation*
2. *Användning och eskalering av kontinuitetsplanen*
3. *Beskrivning av kontinuitetslösningar*
4. *Bilagor*

1. *Dokumentinformation*

System/tjänst:	
Kritisk(a) period(er) för processen:	
Verksamhetens kravställare:	
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 kontinuitetslösningar (beskrivs med fördel i checklisteformat)***

System X

Resurser (mål för återställningstid)	**Kontinuitetslösningar**
Resurs A (X timmar)	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 återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*
Resurs B (X timmar)	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 återställer vi den kritiska resursen efter ett avbrott? Detaljerad beskrivning av återgångsrutin inklusive roller och ansvar)* Nödvändiga kontaktuppgifter: *(Vilka kontaktuppgifter behövs för att kunna utföra kontinuitetslösningarna?)*

Tjänst Y

Resurser (mål för återställningstid)	**Kontinuitetslösningar**
Resurs C (X timmar)	
Resurs D (X timmar)	

4. *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.
- Mall för statusrapportering:
  Klassificering av incidenter sker enligt ordinarie incidenthanteringsprocess, vid ett avbrott som påverkar tjänster finns följande checklista till stöd:

  a) Vilken tjänst är påverkad?
  b) Hur många användare eller kunder berörs?
  c) Vilka reservrutiner finns för aktuella tjänster?
  d) Vilka alternativ finns för att säkra tjänsten
  e) Vad görs för att klara situationen?
  f) Hur kan IT informera verksamheten?
  g) Riskerar IT att tappa kritisk data?
  h) Tid för ny statusrapportering

Appendix G - Begreppslista

Begrepp	Förklaring[30]
Incident	Situation som skulle kunna vara eller leda till avbrott, förlust, nödläge eller kris. (ISO 22301)
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 reserv-, återställnings- och återgångsrutin för en kritisk resurs.
Kontinuitetsplan	Dokumenterade rutiner som vägleder en organisation att efter avbrott reagera, återställa och återuppta verksamheten i en i förväg definierad omfattning. (ISO 22301)
Mål för återställningstid	Tid efter en incident inom vilken det är nödvändigt att en resurs återställs.
Kriteriemodell	Kriteriemodellen definierar vilka konsekvenser som är acceptabla och oacceptabla och är gemensam för hela organisationen.

[30] *Under 2014 kommer Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker samt Finansinspektionens föreskrifter och allmänna råd om IT-system, informationssäkerhet och insättningssystem att publiceras. Dessa föreskrifter kommer att innehålla ett antal definitioner som kan vara relevanta för denna vägledning. Eftersom vägledningen riktar sig till samtliga företag i den finansiella sektorn, vilket inte föreskrifterna kommer att göra, används ISO 22301 som referensdokument.*

Begrepp	Förklaring
Maximalt tolerabel avbrottsperiod	Tid det skulle ta för en negativ inverkan, som skulle kunna uppkomma som ett resultat av att inte tillhandahålla vara/tjänst eller utföra en aktivitet, att bli oacceptabel. (ISO 22301)
Policy	Organisations avsikter och inriktning, formellt uttalande av dess högsta ledning. (ISO 22301)
Process	En kedja av sammanhängande aktiviteter som utifrån en viss resursinsats producerar ett resultat.
Program för kontinuitetshantering	Pågående process för ledning och styrning med stöd från högsta ledningen och tilldelad lämpliga resurser för att införa och underhålla kontinuitetshantering.j (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.

Appendix H - Referenslista

- SS-ISO 22301:2012, Samhällssäkerhet, Ledningssystem för kontinuitet – Krav
- SS-ISO 22313:2013, Samhällssäkerhet, Ledningssystem för kontinuitet – Riktlinjer
- ISO/IEC 27031:2011, Guidelines for information and communication technology readiness for business continuity
- Information Technology Infrastructure Library (ITIL)
- Business Continuity Institute, Good Practice Guidelines 2013 – Global edition
- CPSS/IOSCO (2012), Principles for financial market infrastructures
- European Commission, Solvency II (2009/138/EC)
- ISO 20000, International IT Service Management Standard
- EBA (2011), EBA Guidelines on Internal Governance (GL 44)
- Finansinspektionen (2013), Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut
- FSPOS AG KI (2012), Vägledning för robust elektronisk kommunikation inom finansiell sektor, Bilaga A - Process för kontinuitetshantering
- Krisberedskapsmyndigheten (2006), Kontinuitetsplanering – en introduktion
- Finanssivalvonta (2010), Standard 4.4b Hantering av operativa risker – Föreskrifter och allmänna råd
- MSB (2009), Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters Informationssäkerhet (MSBFS 2009:10)
- MSB (2013) Vägledning för identifiering av samhällsviktig verksamhet och konsekvensbedömning (remissversion)
- SOU 2013:65 - Förstärkta kapitaltäckningsregler