FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Appendix K – Test av kontinuitetsplaner

Version 1.0
FSPOS AG KON, Fokusgrupp Kontinuitetshantering

Dokumenthistorik

Utgåva	Datum	Kommentar
1.0	2020-03-23	Första utgåva av Appendix K – Test av kontinuitetsplaner publiceras i FSPOS Vägledning för Kontinuitetshantering

Bakgrund

Under 2013 utvecklade FSPOS arbetsgrupp för Kontinuitetssäkring en vägledning om kontinuitetshantering för aktörer i den finansiella sektorn. Vägledningen har sedan dess kompletterats i omgångar utifrån sektorns och de finansiella aktörernas behov. *FSPOS Vägledning för Kontinuitetshantering*[1] inkluderar ett antal appendix, bland annat detta appendix, *Appendix K – Test av kontinuitetsplaner*, som ger vägledning i hur finansiella aktörer utifrån god praxis kan genomföra tester av sina kontinuitetsplaner.

Den process för kontinuitetshantering som presenteras i detta appendix följer processen som presenteras i standarden ISO 22301 om ledningssystem för kontinuitetshantering.[2] Processtegen är således de samma som de processteg som presenteras i vägledningens huvuddokument, med skillnaden att detta appendix ger fördjupad vägledning för test av verksamhetens kontinuitetsplaner.

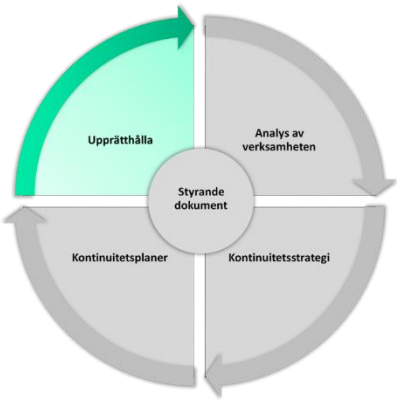
[1] *FSPOS Vägledning för kontinuitetshantering*, version 4.0 (2019).

[2] *SS-EN ISO 22301:2014.*

Innehållsförteckning

K.1. Introduktion

Appendix K – Test av kontinuitetsplaner (i fortsättningen nämnd Appendix K) utgör ett appendix till *FSPOS Vägledning för kontinuitetshantering*. Syftet med detta appendix är att komplettera befintligt material med ett fördjupat stöd avseende hur tester av kontinuitetsplaner kan planeras, genomföras och utvärderas. Appendix K tar utgångspunkt i processen för verksamhetens kontinuitetshantering som beskrivs i vägledningens huvuddokument. I vägledningen beskrivs hur genomförandet av tester är en del av arbetet med att *Upprätthålla* kontinuitetsförmåga, se *Figur 1*. Appendix K utgår från denna process, samt de termer och begrepp som beskrivs i huvuddokumentet och övriga appendix.



***Figur 1**: Kontinuitetshanteringsprocessen. Test av kontinuitetsplaner är en del av arbetet med att upprätthålla kontinuitetsförmåga.*

I FSPOS vägledning *6 steg till bättre övningar*[3] beskrivs en stegvis metod för planering, genomförande och utvärdering av övningar. Samma metod ligger till grund för upplägget i Appendix K då även tester kan utföras enligt dessa steg.

Dokumentets avgränsningar

Appendix K fokuserar på test av verksamhetens kontinuitetsplaner. I viss utsträckning kan beskrivna metoder och arbetssätt även appliceras vid test av IT-verksamhetens återställningsplaner för system/tjänster. Men för att erhålla ett komplett stöd för test av IT-verksamhetens återställningsplaner krävs ett mer fördjupat metodstöd.[4]

[3] *FSPOS vägledning 6 steg till bättre övningar (2018).*

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

Standarder och regelverk

Detta appendix ligger i linje med gällande ISO-standarder[5] för kontinuitetshantering. Vidare hämtas viss inspiration från *Good Practice Guidelines*.[6]

Appendix K utgår från ett antal föreskrifter, lagkrav och allmänna råd gällande test av kontinuitetsplaner. Läsaren bör beakta att lagar, föreskrifter och råd utvecklas löpande. Finansiella aktörer bör därför hålla sig uppdaterade kring förändringar i olika regelverk. Nedan ges exempel på ett urval av regelverk som rör test av kontinuitetsplaner. För en utförligare beskrivning av regelverket för kontinuitetshanteringsarbetet i stort, se avsnitt *2.3 Krav och förväntningar på kontinuitetshantering* i huvuddokumentet.

Finansinspektionen reglerar test av kontinuitetsplaner genom *Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker* (FFFS 2014:4) samt *Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut* (FFFS 2014:1). Enligt föreskrifterna ska berörda[7] aktörer, minst årligen, uppdatera och testa sina kontinuitetsplaner så att de är anpassade för verksamheten och dess förutsättningar.

Vidare finns krav i gällande PSD2[8] och EBA:s riktlinjer[9] som anger att verksamheter ska testa sina kontinuitetsplaner för att säkerställa driften av verksamheternas kritiska funktioner, processer, system, transaktioner och beroenden. Även enligt dessa regleringar ska tester genomföras minst årligen.

För försäkrings- och återförsäkringsorganisationer ställer Solvens II krav på att bolag vidtar rimliga åtgärder för att säkerställa kontinuitet i verksamheten. Detta innebär som minst att organisationen ska upprätta system, resurser och rutiner för kontinuitetshantering, samt att kontinuitetsplaner utvecklas och testas.[10]

För myndigheter under regeringen ger Myndigheten för samhällsskydd och beredskap (MSB) allmänna råd om att myndigheter ska ha rutiner för kontinuitetshantering som tydliggör hur verksamhetens informationshantering upprätthålls vid större störningar och avbrott, samt att planer regelbundet testas för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering.[11]

---

[5] *SS-EN ISO 22301:2014 och SS-EN ISO 22313:2014.*
[6] *The Good Practice Guidelines (2018) – BCI.*
[7] *FFFS 2014:1 och 2014:4 gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, kreditmarknadsföreningar och värdepappersbolag.*
[8] *EBA/CP/2017/04 Revised Payment Services Directive (EU) 2015/2366.*
[9] *EBA Guidelines on ICT and security risk management (2019).*
[10] *European Commission, Solvency II (2009/138/EC), Directive Article 41. 4.*
[11] *Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter om statliga myndigheters Informationssäkerhet (MSBFS 2016:1).*

Förklaring till begreppen övning respektive test

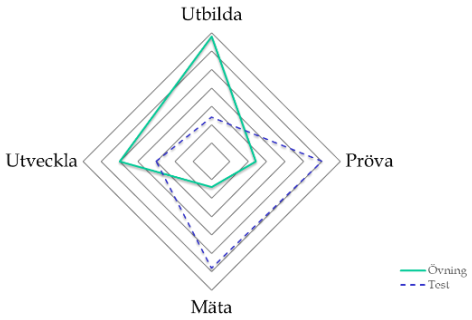
Begreppen *övning* och *test* används såväl inom kontinuitetshantering som inom andra områden. I denna vägledning beskrivs de två begreppen utifrån att de har skilda, men kompletterande mål och syften, se *Figur 2*. Övningar och tester kan genomföras i kombination eller som separata aktiviteter. Framtagna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

Övning

Övning är en process för att träna, bedöma, tillämpa och utveckla organisationers förmåga och färdigheter. Övningar utgår från ett lärande och utbildande perspektiv, med fokus på att bygga upp en förmåga hos individer eller grupper snarare än att verifiera enskilda processer. Däremot kan en övning ha testande inslag. Detta styrs framför allt av hur målen och mätpunkterna för övningen definieras. Övningar kan till exempel genomföras för att klargöra roller och ansvar, för att förbättra samordning och kommunikation, samt för att identifiera resursbrister och förbättringsmöjligheter.[12]

Test

Test är en process för att bestämma helhet, kvalitet eller riktighet i det testade objektet. Den tydligaste skillnaden mellan övningar och tester är att tester innefattar moment av prövning och mätning, utifrån en förväntan om att det/de testade objekten antingen ska godkännas eller underkännas inom ramen för uppsatta mål och mätpunkter.[13] Tester används för att verifiera en eller flera utpekade förmågor eller planer, exempelvis för att bedöma om befintlig förmåga är tillräcklig eller om framtagna kontinuitetsplaner fungerar som avsett. En förutsättning för att kunna genomföra tester är att det finns etablerade förmågor och framtagna kontinuitetsplaner som går att verifiera. Tester kan även innefatta ett mått av lärande och utbildning då målgruppen för testet med stor sannolikhet ökar sin medvetenhet och förmåga under själva genomförandet.



***Figur 2**: Övningar fokuserar främst på utveckling av organisationens förmåga ur ett lärande och utbildande perspektiv. Tester fokuserar främst på att verifiera planer och förmågor genom att pröva och mäta utifrån ett förväntat resultat.*

[12] *ISO 22300:2018 – Security and resilience – Vocabulary.*
[13] *ISO 22300:2018 – Security and resilience – Vocabulary.*

K.2. Test av kontinuitetsplaner

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

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

I *Figur 3* redogörs ett exempel på en kontinuitetslösning för den kritiska processen kredithantering. I kontinuitetsplanen beskrivs kontinuitetslösningen i form av en instruktion för hur avdelningen kan arbeta på alternativa sätt under ett avbrott (reservrutin), hur arbetet med att återställa systemet hanteras (återställningsrutin) samt instruktion för hur verksamheten kan återgå till normalläge när systemet är tillgängligt igen (återgångsrutin).

Kritisk process: Kredithantering
Scenario: System X är otillgängligt

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

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

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

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

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

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

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

Figur 3: *Exempel på kontinuitetslösning.*

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

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

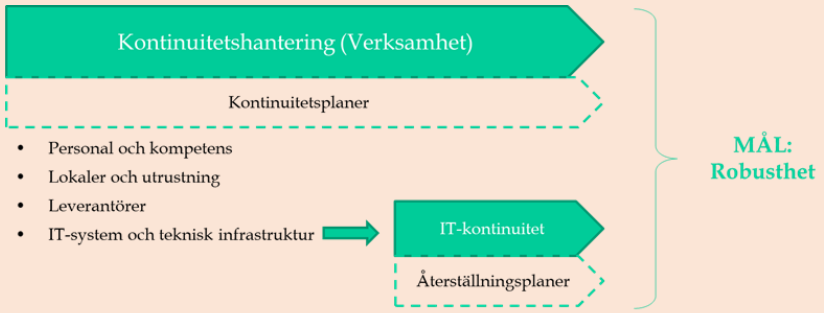
Test av kontinuitetsplaner kan bland annat syfta till att:

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

Test av IT-verksamhetens återställningsplaner

Genom kontinuitetshantering identifieras verksamhetens kritiska processer, samt de aktiviteter och resurser som krävs för att de kritiska processerna ska kunna upprätthållas.

IT-system och andra IT-relaterade resurser utgör ofta kritiska stödresurser till finansiella aktörers kritiska processer. De tidskrav som verksamheten definierat för dessa resurser utgör viktiga ingångsvärden för IT-verksamhetens kontinuitetsarbete. IT-kontinuitetshantering syftar till att skapa robusthet och redundans i IT-verksamhetens kritiska system/tjänster, baserat dels på kravställningar från verksamheten och dels på IT-verksamhetens egna behov och analyser.[14] I *Figur 4* illustreras hur verksamhetens kontinuitetshantering och IT-kontinuitetshantering tillsammans bidrar till organisationens robusthet.



***Figur 4**: Verksamhetens och IT-verksamhetens arbete med kontinuitetshantering bidrar tillsammans till organisationens robusthet.*

Kontinuitetslösningar för IT-verksamheten beskrivs i specifika återställningsplaner för system/tjänster.[15] I återställningsplanerna beskrivs konkreta och tydliga kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner för var och en av de identifierade kritiska IT-resurserna. Lösningarna kan exempelvis handla om back up-hantering, spegling av viktig data samt incidentrapportering och incidenthantering. IT-verksamhetens återställningsplaner för system/tjänster bör, liksom verksamhetens kontinuitetsplaner, testas minst årligen. Exempel på tester för IT-resurser kan vara failover-tester eller återläsningstester.

---

[14] *Se vidare* Appendix F – Kontinuitetshantering för IT-verksamheten.

[15] Liksom i Appendix F – Kontinuitetshantering för IT-verksamheten *benämns i detta appendix IT-verksamhetens återställningsplaner för system/tjänster. Andra vanliga benämningar är disaster recovery-planer eller back up-planer. Notera att återställningsplaner även ska upprättas för verksamhetens kritiska processer enligt FFFS 2014:4. IT-verksamheten kan då även utgöra kritiska verksamhetsprocesser i verksamhetens kontinuitetsplaner. I* FSPOS Vägledning för kontinuitetshantering *beskrivs hur återställningsplaner kan vara en del av verksamhetens kontinuitetsplaner givet att återställnings- och återgångsrutiner beskrivs i dessa.*

K.3. Skapa en teststrategi och testplan

Teststrategi

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

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

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

Prioritering av processer för test

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

I *Tabell 1* utgör processernas maximalt tolerabla avbrottsperioder grunden för prioritering. Att prioritera processer utifrån maximalt tolerabla avbrottsperioder är vanligt. Även andra kriterier, såsom riskbedömning för processernas stödjande resurser eller processernas affärsbetydelse kan ligga till grund för prioritering.

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

***Tabell 1**: Exempel på modell för prioritering av processer för test.*

Förmågeområden

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

I *Tabell 2* ges exempel på förmågeområden som kan vara aktuella att inkludera i en teststrategi. Områdena är till viss del överlappande men även kompletterande. Att ha definerade förmågeområden i teststrategin underlättar också framtagandet av mätpunkter för varje enskilt test.

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

Tabell 2: *Exempel på förmågeområden att testa över tid.*

Mognadsnivåer

Teststrategin bör också förklara hur organisationen stegvis ska stärka sin förmåga över tid. För att mäta organisationens mognadsnivå kan en modell likt mognadstrappan användas, se *Figur 5*. Mognadstrappan, eller annan modell, kan hjälpa till att identifiera eventuella brister i nuvarande teststrategi. Modellen kan även visa på nuvarande mognadsnivå samt utgöra ett bra underlag för beslut om önskad mognadsnivå.[16] Beslut om vilken mognadsnivå organisationen ska befinna sig på bör fattas av ledningen.

***Figur 5**: Exempel på modell för att mäta nuvarande samt önskad mognadsnivå.*

I *Tabell 3* ges exempel på hur beskrivningar för varje mognadsnivå (1-4) kan definieras.

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

[16] *ISO 22325:2016 - Krishantering - Vägledning för förmågeutvärdering.*

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

Tabell 3: *Exempel på definitioner för mognadsnivåer.*

Testtyper

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

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

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

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

Dokumentationsgenomgång

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

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

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

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

Skrivbordsövning

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

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

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

Simulering

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

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

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

Funktionstest

Funktionstestning syftar till att testa organisationens funktionella enheter, antingen som enskild funktion eller som en del av den kritiska processen. Funktionstester genomförs i syfte att säkerställa att flera organisatoriska enheter fungerar tillsammans under störda förhållanden. Dessa enheter kan tillhöra olika kritiska processer och kan dessutom vara geografiskt skilda. Tester av planerna görs då delvis skarpt eller i en för testet uppbyggd kontrollerad testmiljö med hjälp av verkliga resurser. Ibland inkluderas även externa leverantörer. Ett funktionstest är utformat för att kunna mäta alla stegen som utförs under testet. Därför bör tydliga mätpunkter definieras för att kunna mäta hur verksamheten klarar varje steg av testet.

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

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

Fullskaletest

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

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

Testplan

Som komplement till den strategiska och långsiktiga teststrategin bör en specifik testplan tas fram. En testplan bör visa hur respektive identifierad kritisk process löpande ska testas. I testplanen dokumenteras förslagsvis testformat, förmågeområden, prioritering och målgrupp (se mall för testplan).

Testplanen bör inkludera olika testtyper. Omfattning och frekvens av tester bör kopplas till hur kritisk processen är, eller utifrån annan prioritering som angetts i fastställd teststrategi. Genom att kontinuitetslösningar för de mest kritiska processerna testas mer frekvent och omfattande än de mindre kritiska, kan på så sätt resurser optimeras. Under hur lång tidsperiod testplanen ska sträcka sig beror till stor del på organisationen och dess ambitionsnivå, men vanligt är att cykeln löper över en 2 - 4 årsperiod. Testplanen bör vara förankrad och godkänd av ledningen. Planen bör också revideras varje år eller vid behov.

Tips: Utgå från fastställd teststrategi för att sätta en realistisk testplan.

MALLAR FÖR GENOMFÖRANDE
- TESTPLAN -

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

K.4. Planering, genomförande och utvärdering av test

Som beskrivs i inledningen utgår Appendix K från FSPOS vägledning *6 steg till bättre övningar.*[17] I detta kapitel har stegen för planering, genomförande och utvärdering anpassats till test. Se *Figur 6* för samtliga steg i testplaneringen.

***Figur 6**: De sex stegen i testplaneringen.*

Steg 1: Förankra testet

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

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

I förankringsarbetet kan följande information vara värdefull att förmedla:

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

Steg 2: Sätt ramarna för testet

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

---

[17] *FSPOS vägledning 6 steg till bättre övningar (2018). I detta appendix benämns steg **1 Förankra** (istället för Argumentera för övningen).*

Definition av syfte och mål

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

Syftet ska besvara frågan - Varför ska vi genomföra ett test?

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

Målet ska besvara frågan – Vad ska testet leda till?

Konkretisering av målen genom mätpunkter

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

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

Exempel på mätpunkter

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

Kommunikation

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

Kompetens

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

Ledning

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

Logistik

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

Medvetenhet

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

Resurser

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

Samverkan

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

Tidskrav

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

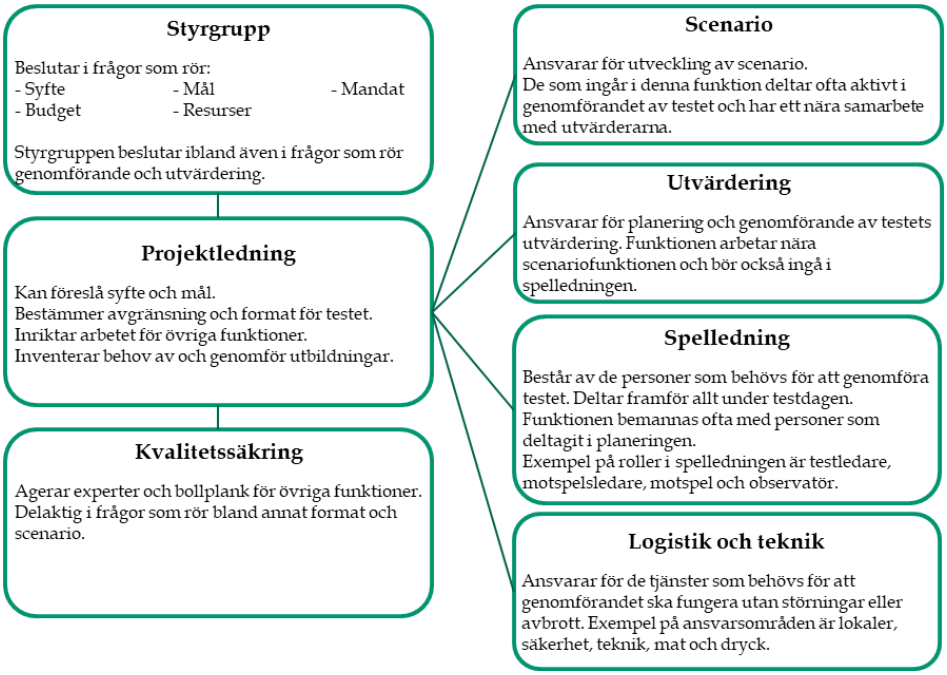
Utse relevant målgrupp

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

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

Utse testorganisation

Beroende på testets storlek och ambitionsnivå behöver en större eller mindre testorganisation utses. För mindre, enklare tester räcker det oftast med att testledaren ansvarar för alla steg i testet. För större, mer komplexa tester såsom simuleringar, funktions- eller fullskaletester behöver en utökad testorganisation utses för planering, genomförande och utvärdering. Exempel på roller som kan behöva ingå i en sådan testorganisation utöver testledare (del av spelledning) är en styrgrupp, scenarioansvarig, utvärderingsansvarig samt stödresurser för teknik, logistik och administration. Se Figur 7 nedan för exempel på testorganisation.



***Figur 7**: Exempel på testorganisation.*

De roller som kan behövas under själva genomförandet av testet beskrivs i *Figur 8* nedan. Dessa utgör testets spelledning.

***Figur 8**: Roller i spelledningen.*

Steg 3: Planera testet

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

Val av testtyp

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

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

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

Val av scenario

Baserat på syfte och mål, valda förmågeområden, testtyp samt den/de planer eller processer/resurser som ska testas utvecklas ett relevant scenario. Om möjligt bör scenariot inkludera information som gör testet relevant för olika nivåer, d.v.s. att kontinuitetslösningar på processnivå, aktivitetsnivå och resursnivå kan verifieras. Scenariot bör också utgå ifrån organisationens egna identifierade kritiska beroenden. Ett exempel på beroende kan vara en organisations leverantörskedjor. Riskanalyser är också lämpliga att använda som inspiration vid scenarioutveckling. Det är dock viktigt att inte låsa sig fast vid redan identifierade risker. Hänsyn bör även tas till vad som sker i vår omvärld, med nya trender och hot.

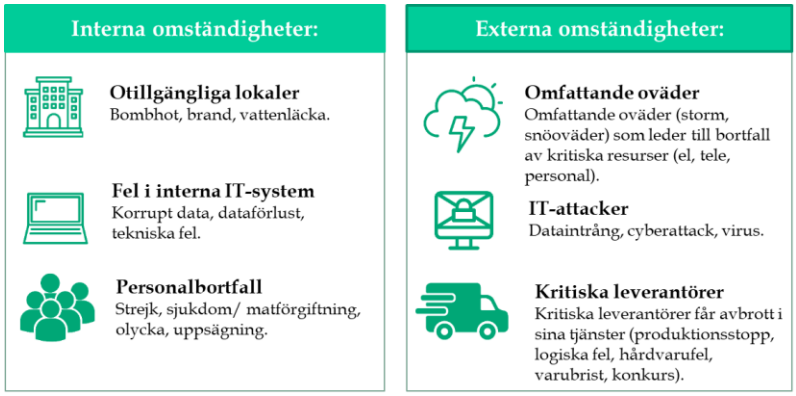
Givet att kontinuitetshantering syftar till att upprätthålla en tolerabel nivå för kritiska processer oavsett vilka störningar som inträffar, bör scenariot i sig inte utgöra testets huvudsyfte. Fokus för testet bör istället läggas på organisationens förmåga att upprätthålla den/de testade kritiska processerna.

Scenarier kan behandla både interna och externa omständigheter. De kan beröra allt ifrån omfattande oväder som stegvis leder till bortfall av kritiska resurser, till kritiska leverantörer som får avbrott i sina tjänster, eller fel i interna IT-system (exempelvis korrupt data, dataförlust eller tekniska fel). För fler exempel på övergripande scenarier se *Figur 9*.

EXEMPEL PÅ SCENARIO OCH FRÅGESTÄLLNINGAR

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

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



***Figur 9**: Förslag på scenarier på en övergripande nivå.*

Planera för utvärdering

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

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

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

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

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

Förslag på testprotokoll

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

Steg 4: Genomföra testet

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

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

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

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

Steg 5: Utvärdera testet

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

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

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

Utvärderingsdiskussionen bör också inkludera en tydlig koppling till uppsatta mål och mätpunkter för att tydliggöra uppfyllandegraden av testets mål. Baserat på testledarens och observatörernas observationer, samt resultatet från utvärderingsdiskussionen sammanställs resultatet från testet i en testrapport. Rapporten bör innehålla förslag på konkreta åtgärder på kort, medellång och lång sikt för att förbättra de testade planerna (inkl. ansvarig och deadline för att implementera åtgärderna). Se *Tabell 5* för exempel på en enkel åtgärdslista.

Åtgärdsförslag	Ansvarig	Deadline	Kommentar

***Tabell 5**: Åtgärdslista. Exempel på åtgärdslista att inkludera i rapport.*

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

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

Steg 6: Implementera och följa upp åtgärder

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

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

K.5. Rapportering till ledning och styrelse

Rapportering av resultatet från genomförda tester av kontinuitetsplaner ska enligt Finansinspektionens föreskrifter ske minst årligen till ledning och styrelse.[18] Rapporteringen bör utgå ifrån fastställd teststrategi samt hållas på en sådan nivå att rekommendationer och åtgärdsförslag inte går att feltolka, samtidigt som rapporten till ledning och styrelse anpassas efter målgruppen. Till exempel bör rapporten inte innehålla alltför många tekniska termer och begrepp.

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

En rapport till ledning och styrelse bör innehålla följande:

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

[18] *FFFS 2014:4 Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker.*