FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Former och metoder för test av it-verksamhetens återställningsplaner

Version: 2021-12-14

FSPOS AG Kunskapsspridning
genom Fokusgrupp Metodstöd

Dokumenthistorik

Utgåva	Datum	Kommentar
1.0	2021-12-14	Första utgåva av Former och metoder för test av it-verksamhetens återställningsplaner.

1 Introduktion

En viktig byggsten för att stärka en organisations operativa motståndskraft är kontinuitetshantering. Förenklat kan kontinuitetshantering beskrivas som den process som säkerställer att organisationen kan driva sin kritiska verksamhet på tolerabel nivå, oavsett vilka störningar som inträffar. 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.

För aktörer i den finansiella sektorn får avbrott i it-tjänster stora konsekvenser för verksamheten, vilket i förlängningen leder till konsekvenser för kunderna. It-verksamheten är därför en viktig stödfunktion, oavsett om den är intern eller outsourcad till tredje part, för att säkerställa robustheten i leveransen mot slutkunden. Kontinuitetshantering för it-verksamheten syftar till att skapa en god återställningsförmåga samt säkerställa en redundans för it-verksamhetens kritiska system/tjänster/resurser. Detta baserat på kravställningar från verksamheten samt på it-verksamhetens egna behov och analyser.

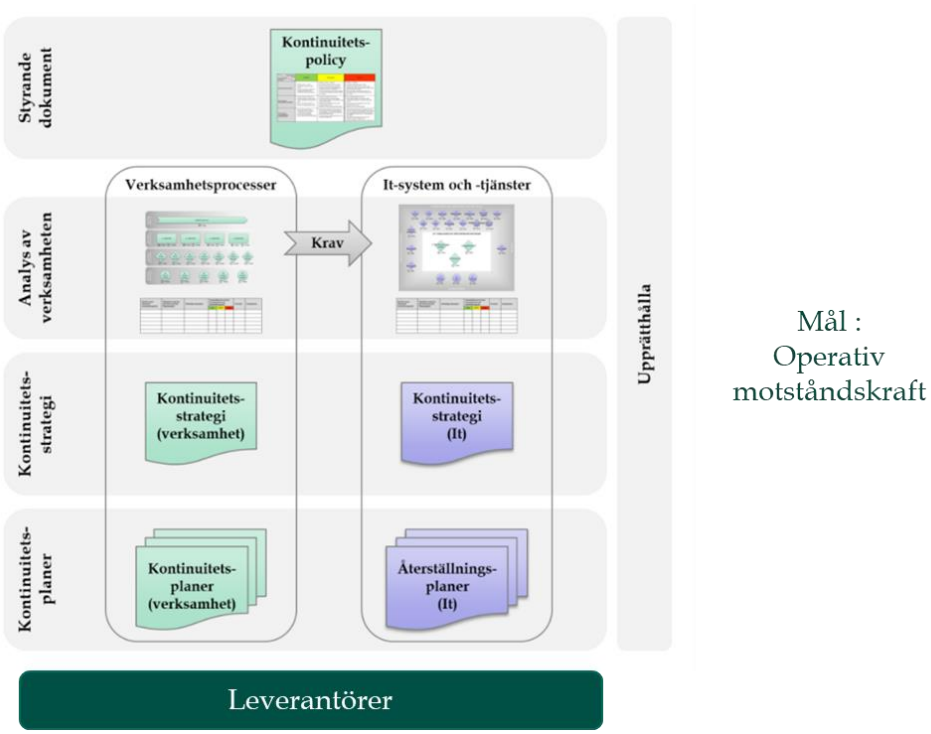
Genom verksamhetens kontinuitetshantering identifieras kritiska processer, samt de aktiviteter och resurser som krävs för att de kritiska processerna ska kunna upprätthållas. It-system och andra it-relaterade resurser utgör ofta kritiska stödresurser till finansiella aktörers kritiska processer. De tidskrav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

Kontinuitetslösningar för it-verksamhetens system/tjänster/resurser beskrivs oftast i återställningsplaner.[1] I återställningsplanerna beskrivs främst konkreta och tydliga kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner för var och en av de identifierade kritiska it-resurserna. Rutiner kan exempelvis handla om hur back-up scheman hanteras vid intrångsförsök, under vilka förutsättning som failover ska genomföras, samt hur detta kommuniceras under och efter återställning.

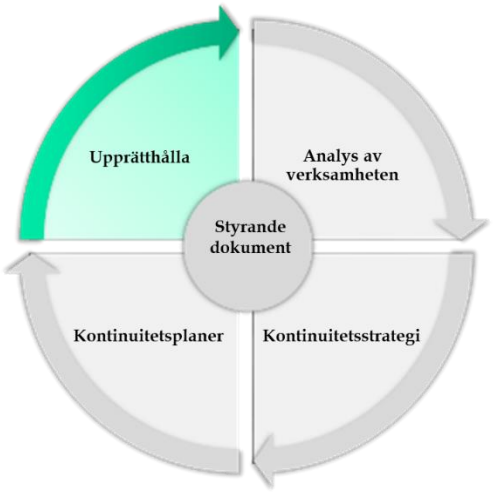
It-verksamhetens återställningsplaner bör, liksom verksamhetens kontinuitetsplaner, testas minst årligen. I syfte att uppnå god kontinuitetsförmåga inom hela organisationen bör även gemensamma tester genomföras för att stärka samordning mellan verksamheten och it. Även leverantörer bör inkluderas vid dessa testtillfällen för att också säkerställa kravefterlevnad i hela leveranskedjan.

---

[1] *Liksom i Appendix F – Kontinuitetshantering för it-verksamheten i FSPOS vägledningen för kontinuitetshantering benämns i detta dokument it-verksamhetens planer för återställningsplaner. Andra vanliga benämningar är disaster recovery-planer eller back up-planer.*



Figur 1: Kopplingen mellan verksamhetens och it-verksamhetens kontinuitetshantering.



Figur 2: Kontinuitetshanteringsprocessen. Test av återställningsplaner är en del av arbetet med att upprätthålla organisationens samlade kontinuitetsförmåga.

Syfte med metodstödet

Detta metodstöd utgör ett komplement till, samt baseras på *FSPOS Vägledning för kontinuitetshantering*, specifikt *Appendix H - Test av kontinuitetsplaner*. Metodstödet följer således samma processteg som presenteras i Appendix H, med skillnaden att detta metodstöd ger fördjupad vägledning specifikt för it-verksamheten, och hur återställningsplaner kan testas, med utgångspunkt i god praxis.

Dokumentets avgränsningar

Detta metodstöd fokuserar på test av it-verksamhetens återställningsplaner. För test av verksamhetens kontinuitetsplaner se *FSPOS Vägledning för kontinuitetshantering*, specifikt *Appendix H - Test av kontinuitetsplaner*.

Metodstödet ska ej ses som ett komplett stöd för test av it-verksamhetens återställningsplaner. I metodstödet beskrivs därför mer generella metoder och arbetssätt för test av återställningsplaner.

Standarder och regelverk

Detta metodstöd följer processen som presenteras i standarderna ISO 22301 om ledningssystem för kontinuitetshantering samt ISO 27031 om återställningshantering för it-verksamhet. Vidare hämtas inspiration från *FSPOS Vägledning för kontinuitetshantering*. Metodstödet utgår från ett antal föreskrifter, lagkrav och allmänna råd gällande test av återställningsplaner. 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 it-verksamhetens återställningsplaner.

Finansinspektionen reglerar test av återställningsplaner genom Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4), Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1) samt Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem (FFFS 2014:5). Enligt föreskrifterna ska berörda[2] aktörer, regelbundet, uppdatera och testa sina återställningsplaner för att effektivisera återgång till normal verksamhet efter ett avbrott eller en större verksamhetsstörning.

[2] *FFFS 2014:1, FFFS 2014:4, FFFS 2014:5 gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, kreditmarknadsföreningar och värdepappersbolag.*

Vidare finns krav i gällande PSD2[3] och EBA:s[4] samt EIOPA:s IKT-riktlinjer[5] som anger att återställningsplaner ska testas för att säkerställa driften av kritiska funktioner, processer, system, transaktioner och beroenden. Även enligt dessa regleringar ska tester genomföras regelbundet, minst årligen.

För försäkrings- och återförsäkringsorganisationer ställer även Solvens II krav på att bolag vidtar rimliga åtgärder för att säkerställa kontinuitet. Detta innebär som minst att organisationen ska upprätta system, resurser och rutiner för kontinuitetshantering, samt att planer utvecklas och testas.[6] För myndigheter 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 övas för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering.[7]

[3] *Payment Services Directive (EU) 2015/2366. EBA Guidelines on security measures for operational and security risks of payment services under PSD2 (EBA/CP/2017/04)*

[4] *EBA Guidelines on ICT and security risk management (2019).*

[5] *EIOPA Guidelines on Information and Communication Technology (ICT) security and governance (2020)*

[6] *European Commission, Solvency II (2009/138/EC), Directive Article 41. 4.*

[7] *Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter om Informationssäkerhet för statliga myndigheter (MSBFS 2020:6).*

2 Centrala begrepp

Begrepp	Förklaring
IKT	Informations- och kommunikationsteknik (ISO 27031).
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 (FSPOS Vägledning för Kontinuitetshantering).
Kontinuitetslösning	Beskrivning av reservrutiner (*hur arbetar vi på alternativa sätt under ett avbrott?*), återställningsrutiner (*hur återställer vi den kritiska resursen efter ett avbrott?*) samt återgångsrutiner (*hur återgår vi till normalläge då den kritiska resursen är tillgänglig igen?*) (FSPOS Vägledning för Kontinuitetshantering)
Kontinuitetsplan	Dokumenterade rutiner som vägleder en organisation att efter avbrott reagera, återställa och återuppta verksamheten i en i förväg definierad omfattning (ISO 22301).
Konsekvensanalys	Process för analys av verksamhet och den effekt som ett avbrott skulle kunna ha för verksamheten (ISO 22301). Även it-verksamheten behöver genomföra en konsekvensanalys för att analysera vilka effekter ett avbrott skulle kunna ha på kritiska it-system/tjänster/resurser samt dess olika beroenden (27301). Konsekvensanalys benämns ibland även beroendekartläggning.

Maximalt tolerabla avbrottsperioder (MTPD)	Den maximala tiden som processen/aktiviteten kan vara otillgänglig innan oacceptabla konsekvenser uppstår. På engelska Maximum tolerable period of disruption (MTPD) (ISO 22301).
Mål för återställningstid (RTO)	Tid efter en incident inom vilken det är nödvändigt att en aktivitet eller resurs återställs. På engelska Recovery Time Objective (RTO) (ISO 22301).
Mål för återställningspunkt (RPO)	Punkt till vilken det är nödvändigt att återställa den information/data som används av en aktivitet, för att göra det möjligt för aktiviteten att återgå till normal leveranskapacitet. På engelska Recovery Point Objective (RPO) (ISO 22301).
Återställning	Organisationens IKT-förmåga att återställa kritiska affärsfunktioner på en acceptabel nivå inom fördefinerade tidsperioder efter en störning (ISO 27031).
Återställningsplan	Dokumenterade rutiner som ger vägledning i återställandet av organisationens IKT-förmåga vid ett inträffat avbrott (ISO 27031). Ibland kallas även återställningsplaner för disaster recovery-planer eller back-up planer.

3 Kontinuitetsstrategier för it-verksamheten

Liksom för övriga verksamheten bör kontinuitetsstrategier upprättas för it-verksamheten. Dessa strategier ska syfta till att möjliggöra för de kritiska it-resurserna att möta de tidskrav som definierats efter genomförda konsekvensanalyser. Beroende på verksamhetens storlek och komplexitet skiljer sig valda kontinuitetsstrategier åt. En kostnad-nyttoanalys bör alltid genomföras för att hitta de mest kostnadseffektiva lösningarna. Nedan listas några exempel på kontinuitetsstrategier för it-verksamheten. Läsaren bör dock beakta den ständigt pågående tekniska utvecklingen, och vad detta innebär för nya krav på tekniska lösningar samt kontinuitetsstrategier.

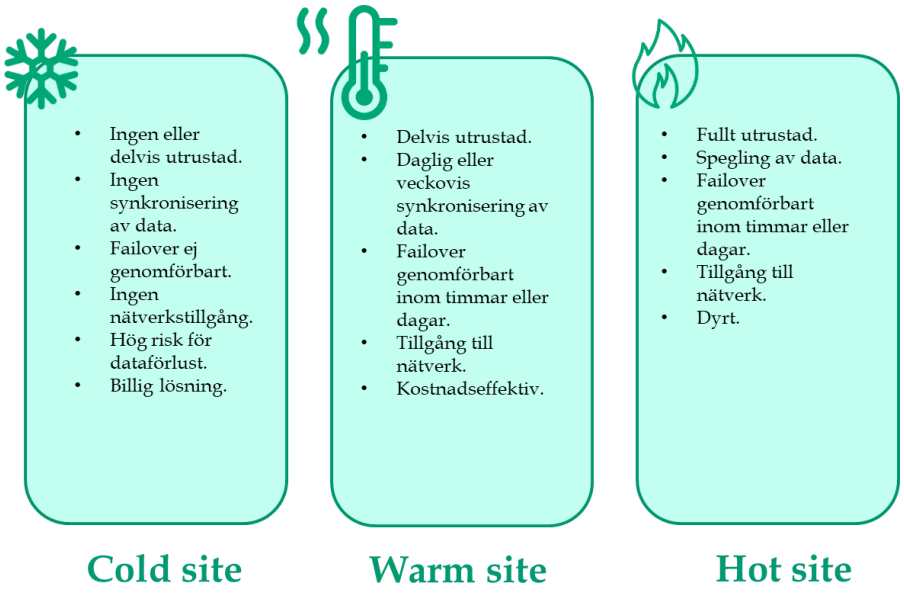
Kontinuitetsstrategier för återställning kan omfatta allt ifrån rutiner för säkerhetskopiering och återställande av data, till att skapa tillgång till standby-lösningar. Detta för att säkerställa att de kritiska it-resurser som identifierats i konsekvensanalysen kan återställas i förhållande till definerade tidskrav.

Genom rutiner för säkerhetskopiering kan data automatiskt kopieras och lagras på en eller flera platser. Omfattningen och regelbundenheten av säkerhetskopieringen kan skilja sig åt beroende på vilken typ av data som ska lagras, samt hur kritisk den specifika datan är för verksamheten vid en eventuell dataförlust. Valet av lösning för datahantering kan då bli avgörande för hur snabbt återställning av data kan ske, det vill säga om data hanteras fysiskt, virtuellt eller via molntjänst.

Genom tillgång till standby-lösningar kan it-verksamheten automatiskt eller manuellt via failover täcka upp för när den primära lösningen inte längre är tillgänglig. Det kan till exempel vara en server, en datahall eller ett nätverk. Dessa lösningar kan skilja sig åt i både omfattning och utrustning, men framför allt avseende hur snabbt de kan tas i bruk vid en eventuell störning eller avbrott.

För att bygga en robust beredskap kan it-verksamheten välja att skapa redundanta datahallar, som hålls frånskilda ordinarie it-system. En så kallad Cold site är en datahall som inte alls eller delvis är utrustad med ordinarie it-system. Ingen synkronisering av data sker vilket gör att möjligheten till automatisk failover saknas. Det kan därför ta mycket lång till att ta denna typ av datahall i bruk, därav passar denna lösning resurser med långa RTO:er och RPO:er. En Warm site är en delvis utrustad datahall, där synkronisering av data sker dagligen eller veckovis. Failover kan då göras inom timmar eller dagar, vilket är lämpligt för resurser som har en RTO eller RPO som motsvarar dessa tidsestimat. En Hot site är den mest komplexa och dyraste lösningen för datahall. Datahallen speglar då i princip den ordinarie it-miljön och kan därför tas i bruk omedelbart efter en störning eller avbrott. Denna lösning är lämplig för resurser med korta eller mycket korta RTO:er eller RPO:er.

Idag finns det leverantörer som erbjuder disaster recovery as a service vilket innebär att organisationer kan ladda upp alla verksamhetskritiska program och all data som skulle behövas vid en eventuell störning eller ett avbrott. Detta är mer omfattande än en vanlig säkerhetskopiering eller back-up lösning då infrastrukturens olika konfigurationer och program behöver sparas och lagras. Vid en allvarlig störning eller avbrott kan organisationen fortsätta som normalt genom att ansluta sig till operatörens tjänstelösning.



Figur 3: Alternativ för datahall.

4 Test av återställningsplaner

Återställningsplaner ska upprättas för de it-resurser som identifierats genom verksamhetens konsekvensanalys, och därefter också genom it-verksamhetens egna konsekvensanalys. För mer information gällande hur kritiska it-resurser identifieras, se *FSPOS Vägledning för kontinuitetshantering, Appendix F – Kontinuitetshantering för it-verksamheten*.

Återställningsplaner innehåller en uppsättning av förfaranden för att möjliggöra återställande av vitala tekniska system och infrastrukturkomponenter efter en allvarlig störning eller ett avbrott. Planerna ska ge effektiv vägledning för it-verksamheten att återställa de kritiska system/tjänster/resurser som verksamheten är beroende av, med utgångspunkt i den kravställning som framkommit från verksamhetens kontinuitetshantering. Tidskraven i återställningsplanerna ska dock både vara baserade på krav som fastställts av den övergripande verksamheten, samt den egna konsekvensanalys som gjorts av it-verksamheten. Återställningsplaner kan vara skrivna för enskilda system eller tjänster, eller vara gemensam för flera system eller tjänster. För verksamheten är det dock alltid viktigt att ha egna upprättade kontinuitetsplaner som ska användas då kritiska system/tjänster/resurser inte är tillgängliga, detta för att kunna upprätthålla processen under tiden som it-verksamhetens återställningsarbetet pågår. I *Figur 4* nedan redogörs ett fiktivt exempel från en återställningsplan för det kritiska systemet *Betalningssystem*. I återställningsplanen beskrivs kontinuitetslösningen i form av en instruktion för hur it-verksamheten kan upprätthålla funktionaliteten under ett avbrott (reservrutin), hur arbetet med att återställa systemet hanteras (återställningsrutin) samt hur återgång till normalläge ska genomföras när systemet åter är tillgängligt (återgångsrutin).

Figur 4: Exempel på kontinuitetslösning.

Test av återställningsplaner kan och bör innefatta samtliga av kontinuitetslösningarnas tre delar (reservrutiner, återställningsrutiner, återgångsrutiner). Detta bör göras antingen i separata tester för specifika målgrupper eller i form av gemensamma tester med verksamheten, där utvalda målgrupper från verksamheten deltar. Vidare bör underliggande beroenden, såsom externa leverantörer inkluderas i genomförandet av tester i syfte att säkerställa ändamålsenlighet genom hela beroendekedjan. Innan test genomförs med leverantör är det viktigt att se över avtal med kritiska leverantörer, i syfte att säkerställa rätt kravbild och att gemensamma tester ingår som del i avtalet. Om krav gällande tester inte finns med i nuvarande avtal bör detta ses över för att kunna säkerställa god kontinuitets- och återställningsförmåga hos organisationens kritiska leverantörer.

Leveransmässiga villkor avseende kontinuitetshantering bör även finnas med som skall-krav redan vid upphandlingen och fungera som urvalskriterier för vilka leverantörer som är lämpliga att sluta avtal med. Kraven bör utgå från tidigare analyser (konsekvensanalys och riskanalys) och de krav som ställs på den egna organisationen (se *FSPOS Vägledning för Kontinuitetshantering, Appendix G – Kontinuitetshantering för outsourcad verksamhet* för djupare beskrivning).

Genom tester kan it-verksamheten bland annat säkerställa:

- ✓ att återställningsplanerna är förenliga med verksamhetens konsekvensanalyser,
- ✓ att it-systemet/tjänsten/resursen kan återställas oavsett störning eller avbrott,
- ✓ att återställningsrutiner för it-miljön är tillräckliga för att möta verksamhetens krav på återställning (RTO/RPO),
- ✓ att rutinerna för återgång till normalläge fungerar som avsett,
- ✓ att okända tekniska brister kan identifieras och hanteras,
- ✓ att den egna personalen besitter rätt kompetens,
- ✓ att kritiska leverantörer svarar upp mot avtalad kontinuitets - och återställningsförmåga.

4.1 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 it-resurser. Teststrategin bör svara på vad organisationen vill uppnå och varför, hur organisationen ska nå dit, samt hur utvecklingen ska mätas.

Teststrategin kan med fördel vara en del av it-verksamhetens kontinuitetsstrategi. Upprättande av en kontinuitetsstrategi för it-verksamheten beskrivs ytterligare i *FSPOS Vägledning för kontinuitetshantering, Appendix F – Kontinuitetshantering för it-verksamheten*. En tät dialog mellan it-verksamheten och verksamhet bör upprättas i framtagandet av en teststrategi, detta för att säkerställa att förmågan inom hela organisationen kan verifieras. På så sätt kan även de resurser som tas i anspråk vid test optimeras.

Teststrategin bör även vara förankrad och godkänd av ledningen.

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

Prioritering för test

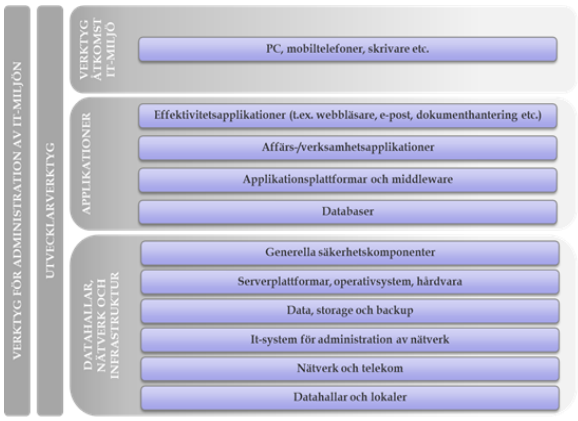
En beskrivning över hur it-verksamheten har prioriterat de kritiska it-resurserna för test kan ingå i teststrategin. Utifrån denna prioritering kan olika krav, exempelvis avseende frekvens eller omfattning för tester av återställningsplaner, definieras. Prioriteringen styrs mycket av hur den egna it-miljön är uppbyggd.

I *Figur 5* visas ett exempel på hur en it-miljö kan beskrivas och visualiseras.[8] För att underlätta valet av vilka system/tjänster/resurser som ska ingå för testning kan ett första steg vara att dela in it-miljön i tre olika kategorier:

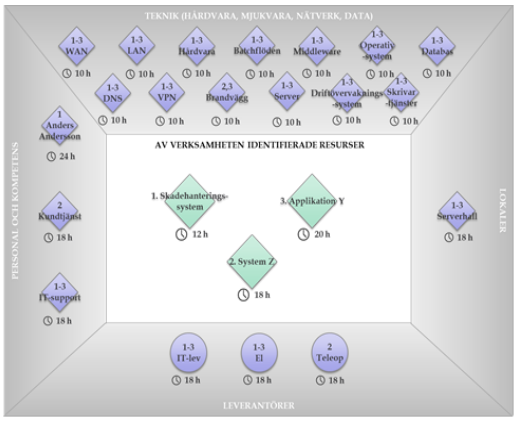
1. **Verktyg för åtkomst till it-miljö** (inkluderar telefoner, PC, skrivare etc).
2. **Applikationer** (inkluderar affärs-/verksamhetsapplikationer, applikationsplattformar och middleware, databaser etc.).
3. **Datahallar, nätverk och infrastruktur** (inkluderar generella säkerhetskomponenter, serverplattformar, operativsystem, hårdvara, nätverk, datahallar etc.).

[8] *The Open Group Architecture Framework (TOGAF 2020).*

För att sedan göra en prioritering bland alla system/tjänster/resurser som ska ingå för test bör valet baseras på it-resursernas kritikalitet och de definierade tidskrav som framkommit i den övergripande verksamhetens konsekvensanalys, samt it-verksamhetens egen konsekvensanalys.



Exempel på indelning av it-miljö.



Sammanställning av tidskrav på identifierade kritiska it-resurser från genomförda konsekvensanalyser.

Figur 5.

Nedan anges ett exempel på hur en prioritering av valda it-resurser för test kan göras. It-resurser delas då in i guld, silver och bronskategorier. Guldkategorin motsvarar de it-resurser som har ett mål för återställningstid under 2 timmar, silverkategorin motsvarar it-resurser med mål för återställningstid mellan 2-24 timmar, och bronskategorin motsvara de it-resurser som har mål för återställningstid på över 24 timmar. Då tester även kan innehålla återställning av data bör prioritering även göras utifrån krav på återställningspunkt. Prioriteringarna bör även baseras på satt kontinuitetsstrategi för it-verksamheten. I exemplet nedan anges olika strategier baserat på hur kritiska de olika resurserna är.

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

Tabell 1: Exempel på modell för prioritering av it-resurser för test.

Exemplet ovan utgår ifrån en prioritering på resursnivå. Då it-resurser oftast ingår som en del av organisationens kritiska affärsfunktioner är det viktigt att prioriteringen inte endast görs utifrån satta tidskrav för den enskilda resursen, utan även tar hänsyn till hela informationsflödet och resursens beroendekedja. Beroenden kan finnas inom och mellan system eller tjänster, internt eller outsourcat. Det är därför viktigt att känna till dessa beroenden innan it-resurser väljs ut för testning. Detta görs enklast genom att utgå ifrån genomförd konsekvensanalys, där it-resursens alla beroenden till andra system, tjänster eller funktioner har identifierats. På så sätt kan även hela beroendekedjan testas.

Förmågeområden

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

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

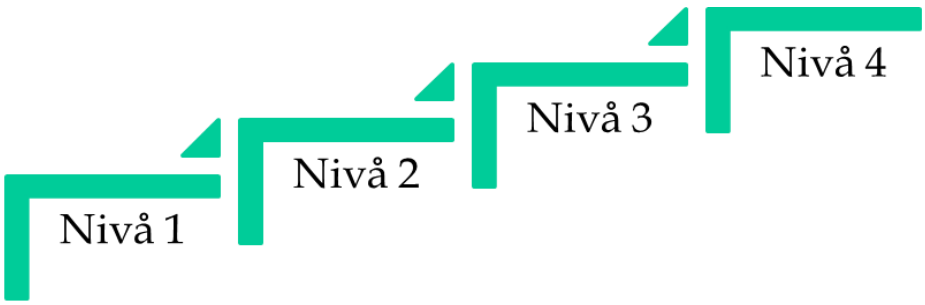
Förmågeområde	Beskrivning
Kommunikation	Avser förmågan att kommunicera och rapportera såväl internt som externt, vid störningar och avbrott.
Medvetenhet	Avser medvetenhet om återställning samt gällande rutiner. Olika krav på medvetenhet bör ställas på individer/grupper. Exempelvis: • Planägare/systemägare: bör ha full insyn i återställningsplanerna. Planägare/systemägare 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 kontinuitetshanteringsarbetet samt gällande rutiner vid störningar eller avbrott.
Kompetens	Avser berörda funktioners förmåga och kompetens att följa och utföra de rutiner som finns beskrivna i återställningsplanerna. Kunskap och kompetens krävs även hos tilltänkta ersättare.
Samverkan	Avser förmågan att samverka, såväl inom organisationen som med externa aktörer (t.ex. leverantörer) i syfte att hantera en störning eller ett avbrott.
Ledning	Avser arbetsätt, samt planernas ändamålsenlighet avseende rutiner för incidentrapportering, initiering, larmning och aktivering av planer. Avser även åtgärder i syfte att åstadkomma inriktning och samordning för återställningsarbetet.
Logistik	Avser olika typer av leverantörslösningars möjlighet att upprätthållas vid störningar eller avbrott.
Fysisk säkerhet	Avser förmågan att återställa fysiska faciliteter eller resurser så som data och serverhallar samt resurser för elförsörjning vid störning eller avbrott.
Teknik	Avser förmågan att återställa; • infrastruktur inklusive servar, lagring, nätverk och övriga komponenter. • system inklusive operativsystem, applikationer, gränsnitt mellan applikationer och batch-rutiner.
Data	Avser förmågan att återställa data, såsom applikationsdata eller annan kritisk data.

Tidskrav	Avser möjligheten att möta definierade tidskrav, så som Mål för återställningstid (RTO) samt mål för Mål för återställningspunkt (RPO). Tidskrav inkluderar även test av uppfyllande av kravställning i avtal (SLA) med leverantör.

Tabell 2: Exempel på förmågor att inkludera i en teststrategi.

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 6*. 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.[9] Beslut om vilken mognadsnivå organisationen ska befinna sig på bör fattas av ledningen.



Figur 6: Exempel på modell för att mäta nuvarande samt önskad mognadsnivå.

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

Mognadsnivå	Beskrivning
Nivå 1	• It-verksamheten genomför sällan eller aldrig tester. Tester som genomförs görs ostrukturerat, utan tydliga målsättningar eller mätpunkter. • Återställningsplaner saknas helt eller är bristfälliga.

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

Nivå 2	• It-verksamheten genomför tester för utvalda it-system/tjänster/resurser • Använder sig av en begränsad variation av testtyper. • Genomförda tester utvärderas utifrån målsättningar men dokumentationen och uppföljningen är bristfällig. • Har upprättade återställningsplaner men är bristfälliga. Planerna uppdateras ej regelbundet.
Nivå 3	• It-verksamheten har en etablerad testsstrategi. • Genomför tester regelbundet för utvalda it-system/tjänster/resurser. • Använder sig av ett varierat urval av testtyper för att även få in mer avancerade testmoment. • Uppsatta testmål utvärderas utifrån fördefinierade mätpunkter för att identifiera förbättringsområden. Resultatet dokumenteras och följs upp. • Har upprättade detaljerade återställningsplanen för återställning av alla kritiska identifierade it-system/tjänster. Planerna uppdateras regelbundet.
Nivå 4	• It-verksamheten genomför tester i samverkan med övriga verksamheten samt externa aktörer (ex. leverantörer). Teststrategin är långsiktig och beskriver tydligt hur it-verksamheten ska täcka in samtliga av de kritiska it-system/tjänster som ska testas, under ett bestämt tidsintervall. • Visar på hög mognadsgrad genom att dra lärdomar av tidigare tester, samt omsätter lärdomar till konkreta förbättringsåtgärder för att vidareutveckla och upprätthålla sin förmåga. • Behärskar alla former av testtyper och använder också resultatet från tidigare tester som ett ingångsvärde i testplaneringen. • Har upprättade detaljerade återställningsplaner för återställning av alla kritiska identifierade it-system/tjänster/resurser. Planerna uppdateras regelbundet.

Tabell 3: Exempel på definitioner för mognadsnivåer.

Testformer

I teststrategin beskrivs de testtyper som organisationen avser använda. Valet av testtyper bör anpassas till målgruppens och återställningsplanernas mognads- och ambitionsnivå. Ambitionsnivån bör vara att gradvis öka komplexitet och omfattning över tid.

Gällande testform bör beslut fattats kring omfattningen av rena tekniska tester och tester av arbetssätt och procedurer. Detta avgör i sin tur vilka testtyper och testalternativ som kan bli möjliga. För att skapa en robusthet inom it-verksamheten bör både tekniska och mer procedurfokuserade tester genomföras, och helst i kombination.

Diskussionsbaserade testtyper

Diskussionsbaserade testtyper såsom dokumentationsgenomgångar och skrivbordsövningar har som huvudfokus att stärka medvetenhet och kompetens gällande rutiner och arbetssätt i återställningsplanen. Både dokumentationsgenomgångar och skrivbordsövningar bör inkluderas i teststrategin för att täcka alla av organisationens behov. Diskussionsbaserade testtyper passar bra för en organisation med en lägre mognadsnivå samt som ett bra komplement för mer mogna organisationer.

TESTTYP	BESKRIVNING	LÄMPLIGA FÖRMÅGE-OMRÅDEN ATT TESTA
Dokumentations-genomgång	En dokumentationsgenomgång, även kallad walk-through, syftar till att på ett strukturerat sätt identifiera flaskhalsar och andra svagheter i återställningsplanerna. Deltagare granskar och diskuterar steg för steg i varje komponent av återställningsplanen. På så vis kan eventuella brister i rutiner eller kontinuitetslösningar identifieras. Denna testtyp är lämplig vid introduktion av ny plan eller vid uppdateringar. Kan exempelvis göras av planägare/systemägare med stöd av checklista, eller under ledning av facilitator.	Exempelvis kompetens och medvetenhet
Skrivbordsövning	Under skrivbordsövningar diskuterar deltagarna planernas ändamålsenlighet utifrån ett eller flera scenarier som påverkar en eller flera planer samtidigt. Deltagare diskuterar eventuella åtgärder och lösningar i återställningsplanen men genomför inte aktiviteter ”skarpt”. Skrivbordsövningar har framförallt ett lärande syfte, där deltagarna i lugn och ro ges möjligheten att reflektera och diskutera utifrån olika scenarier. Skrivbordsövningar lämpar sig väl för organisationer med en låg mognadsnivå, samt som ett bra komplement för mer mogna organisationer.	Exempelvis kompetens och medvetenhet

	Skrivbordsövningar kan även genomföras för nya eller uppdaterade planer. 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.	

Tabell 4: Exempel på diskussionsbaserade testtyper.

Tekniska testtyper

För att verifiera återställningsplaner bör även mer tekniska testtyper genomföras. Exempel på testtyper som involverar tekniska tester är simulering, funkionstest, parallellt funktionstest samt fullskaligt återställningstest. Nedan ges en beskrivning av dessa testtyper.

TESTTYP	BESKRIVNING	LÄMPLIGA FÖRMÅGE-OMRÅDEN ATT TESTA
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 genom att förmedla inspel som på ett realistiskt sätt ska hjälpa till att testa hur olika resurser fungerar i en realistisk situation. 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, rapporteringsvägar eller verifiering av viss teknisk utrustning.	Exempelvis kommunikation, kompetens, ledning, samverkan, logistik, tidskrav.

Funktionstest	Vid funktionstestning utförs systemåterställning för att konfirmera systemets/tjänstens förmåga. Då testas enskilda komponenter eller system/tjänster i syfte att säkerställa att enheterna kan stödja varandra även under störda förhållanden. Tester av planerna görs då delvis skarpt eller i en för testet uppbyggd kontrollerad testmiljö. Testerna kan även inkluderas externa leverantörer.	Exempelvis kommunikation, kompetens, data, teknik, fysisk säkerhet, logistik, tidskrav.
Parallellt funktionstest	En mer avancerad och tidskrävande variant av funktionstestning är parallell funktionstestning, vilket innebär att funktionstestning av flera komponenter genomförs, samtidigt som ordinarie verksamhet fortgår. Deltagare genomför aktiviteter och test av återställningsplan ”skarpt” samtidigt som ordinarie verksamhet fortgår. Systemåterställning utförs för att konfirmera systemets förmåga att utföra riktiga affärstransaktioner parallellt medan det primära systemet fortsätter med full produktionskapacitet. Parallellt funktionstest är avancerat och tidskrävande men ger möjligheten att kunna testa en återställningsplans precision genom att jämföra testdata och produktionsdata. Paralellt funktionstest är lämpligt när samtliga rutiner i återställningsplanen är väl inövade av samtliga deltagare.	Exempelvis kommunikation, kompetens, ledning, data, teknik, fysisk säkerhet, samverkan, logistik, tidskrav.
Fullskaligt återställningstest	Deltagare genomför aktiviteter ”skarpt”. Test av befintliga kontinuitetslösningar sker i full skala. Fullskaligt återställningstest kan innebära att systemåterställning utförs för att konfirmera systemets förmåga att utföra riktiga affärstransaktioner genom att stänga av det primära systemet. En annan form av fullskaligt återställningstest kan vara återställning av datahall. Fullskaligt återställningstest är det ultimata återställningstestet eftersom en eller flera affärsverksamheter är helt beroende av it-resursens återställningsförmåga. Fullskaligt återställningstest är lämpligt endast efter ett eller flera lyckade parallella funktionstest då det utgör stor risk för affärsverksamheten.	Exempelvis kommunikation, kompetens, ledning, data, teknik, fysisk säkerhet, samverkan, logistik, tidskrav.

Tabell 5: Exempel på tekniska testtyper.

Vidare bör tekniska testtyper kombineras med olika former av testande moment. Nedan presenteras några exempel på vanliga testmoment som kan inkluderas vid tekniska tester.

TESTMOMENT VID TEKNISKA TESTER	BESKRIVNING
Dataåterställning	Testmoment för att testa återställning av filer eller databas från säkerhetskopia efter skada.
Återställning av system eller applikation	Testmoment för att testa återställning av en eller flera applikationer och tjänster som skapar ett system.
Failover	Testmoment för att testa en redundant eller standby-lösning som, automatiskt eller manuellt, används för att täcka upp för när den primära lösningen inte längre är tillgänglig. Det kan till exempel vara en server, en datahall eller ett nätverk.
Återställning av nätverk	Testmoment för att verifiera redundanta trafikflöden.
End-2-End test	Testmoment för test av exempelvis ett applikationsflöde eller uppbyggandet av ny infrastruktur, från början till slut. Syftet med End-to -End-testning är att validera it-resursens alla delar samt dess olika komponenter.
Fysiska säkerhetstester	Testmoment för test i datahallar, exempelvis brand- och översvämningssystem, utrymningsrutin samt elförsörjning.

Tabell 6: Exempel på testmoment vid tekniska tester.

Testmiljöer

Ett test kan genomföras både i en för testet isolerad testmiljö eller direkt i produktionsmiljön. Valet av testmiljö kan skilja sig åt beroende på hur organisationens it-miljö är uppbyggd. För att verkligen verifiera kontinuitetslösningarna i återställningsplanen kan tester i isolerade testmiljöer kombineras med tester i produktionsmiljö.

Valet av testmiljö bör dock alltid baseras på organisationens riskaptit och mognad. För att säkerställa att testet inte utsätter verksamheten för onödiga risker, som kan leda till allvarliga störningar, bör valet av testmiljö noggrant planeras.

Miljön som används för testet bör vara anpassat för ändamålet, både tekniskt och funktionellt. Detta för att säkerställa relevanta och realistiska testresultat. Det bör även vara väl genomtänkt och bestämt i förväg vilka testtyper och testmoment som kan genomföras i vilken testmiljö.

Innan valet av testmiljö görs bör det även finnas en förståelse kring testmiljön och dess begränsningar vid genomförandet av olika testmoment. Tester som genomförs i isolerade testmiljöer kan försvåra testmoment där integrationen mellan olika system ska testas. Vid användingen av testdata vid genomförandet kan detta försvåra verifieringen av rutiner för säkerhetskopiering. I annat fall där produktionsdata används vid test bör en riskanalys genomföras, samt att hanteringen av data sker i linje med gällande regelverk. I och med dataskyddsförordningen (GDPR) har det skett en ökad reglering gällande användandet av produktionsdata vid test. Även om informationen anonymiseras och tvättas finns alltid risken att känslig data kan läcka ut. Valet av testmiljö samt data bör därför alltid baseras på organisationens riskbeslut. Läs mer om riskbeslut i nästa avsnitt, *Riskanalys och riskbeslut*.

Riskanalys och riskbeslut

För att organisationen ska göra välgrundade val kopplat till de risker som finns vid testning kan en riskanalys ingå som en del av teststrategin. Riskanalysen kan genomföras enligt ett den internationella standarden för riskhantering[10]; etablera kontext (riskacceptans), identifiera risker, bedöma sannolikhet och konsekvens för respektive risk, utvärdera riskerna och ta fram åtgärdsplaner för de risker som inte kan accepteras.

Genomförd riskanalys bör ge en djupare förståelse för de risker som kan kopplas till olika val i samband med test. Mot bakgrund av genomförd riskanalys kan sedan ett medvetet riskbeslut fattas. Analysen kan exempelvis ligga till grund för beslut avseende

- ✓ åtgärder för hantering av identifierade risker samt sårbarheter i nuvarande it-miljö och kontinuitetslösningar,
- ✓ önskad mognadsnivå för test,
- ✓ valet av testtyper vid genomförande av test,
- ✓ valet av testmiljöer vid genomförande av test eller
- ✓ valet av data vid genomförande av test.

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

Ansvar och roller vid test av återställningsplaner

Vid test av återställningsplaner bör någon ha det övergripande ansvaret för att organisationens kritiska it-resurser kan möta ställda krav på tillgänglighet och funktion. Det övergripande ansvaret inkluderar också att se till att tester av återställningsplaner genomförs regelbundet, samt att tillräckligt resurser tillförs testning. Ansvaret inkluderar även att följa upp och kommunicera de risker och riskbeslut som fattats gällande test. Kommunikation av risker görs främst för att säkerställa en god koordinering mellan riskbeslut så att besluten också är baserade på de övergripande riskbesluten som fattats inom verksamheten. Kommunikation av risker och riskbeslut blir även viktiga ingångsvärden för beslut om avgränsningar i genomförandet av tester.

Vid test av återställningsplaner bör det även finnas någon som ansvarar för hur verksamheten på bästa sätt involveras i test, både före, under och efter själva genomförandet. Även då inga gemensamma tester planeras bör verksamheten ändå känna till, samt bli informerad om att tester av, för dem viktiga system/tjänster/resurser, genomgår testning.

Innan test av återställningsplaner genomförs bör det finnas ett tydligt utpekat ansvar för vem som ansvarar för utveckling, implementering samt uppdatering av planerna.

Samarbete och dialog med leverantörer kan också vara centralt då det är viktigt att genomföra gemensamma tester. I avtalsskrivningar mellan leverantörer och beställarorganisationen kan - och bör - förtydliganden göras gällande ansvar och roller vid kontinuitetshanteringen, och då särskilt vad som förväntas av leverantören vid genomförande av test (se *FSPOS Vägledning för Kontinuitetshantering, Appendix G – Kontinuitetshantering för outsourcad verksamhet* för djupare beskrivning).

Exempel på roller som kan tänkas inneha ovanstående ansvar är it - ansvariga, processägare, systemägare, planägare med flera.

Testplan

Som komplement till den strategiska och långsiktiga teststrategin bör en specifik testplan tas fram. En testplan bör visa hur respektive identifierad kritisk it-resurs löpande ska testas. I testplanen dokumenteras förslagsvis testformat (testtyp, testmoment samt testmiljö), vilka kärnområden som den specifika it-resursen stödjer, beroenden kopplat till resursen, aktuella planer som ska testas, förmågeområden, prioritering och målgrupp. Testplanen bör inkludera olika testtyper och testmoment. Omfattning och frekvens av tester bör kopplas till hur kritisk resursen är, eller utifrån annan prioritering som angetts i fastställd teststrategi.

MALLAR FÖR GENOMFÖRANDE
- TESTPLAN -

	Kvartal	System / tjänst /resurs	Kärnprocess(er)	Beroenden	Testade plan(er)	Testtyp	Testmoment	Testmiljö	Förmågeområden	Prioritering	Målgrupp	Ansvarig	Kommentar
År 1	Q1	ERP-system	Ekonomi Försäljning	Central infrastruktur, interna integrationer	Återställnings-plan ERP-system	Paralellt funktionstest Funktionstest	Dataåterställ-ning	Isolerad testmiljö	Data Kommunikation Tidskrav	Avgörande betydelse	Systemägare, planägare, processägare, resurser för återställning, användare från verksamheten.	Systemägare	Återställning av databas
	Q2												
	Q3												
	Q4												
År 2	Q1												
	Q2												
	Q3												
	Q4												
År 3	Q1												
	Q2												
	Q3												
	Q4												

4.2 *Planering, genomförande och utvärdering av test*

Som beskrivs i inledningen utgår detta metodstöd från *Appendix H – Test av kontinuitetsplaner*. Därav har samma sex steg för testplanering kommit att användas även för test av it-verksamhetens återställningsplaner. Se *Figur 7* för samtliga steg i testplaneringen.

Figur 7: De sex stegen i testplaneringen.

Steg 1: Förankra test

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 it-verksamhetens tester, samt för en effektiv rapportering och implementation av åtgärder.

Innan planeringen påbörjas bör testplanen vara förankrad 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 de olika testen 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 testen samt förväntat resultat.
- ✓ Testens målgrupp samt antalet deltagare.
- ✓ Tidpunkt för testen.
- ✓ Budget samt andra nödvändiga resurser för såväl planering, genomförande och utvärdering av testen.

Steg 2: Sätta ramarna för test

Att sätta ramarna för ett test 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. Detta arbete bör även utgå från organisationens mognads - och ambitionsnivå.

Formulera testets syfte och mål

Utifrån de förmågeområden som varje specifikt test 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.

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

Konkretisering av målen genom mätpunkter

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

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

I *Tabell 7* nedan ges ett antal exempel på mätpunkter utifrån de förmågeområden som presenterades i avsnittet *Skapa en teststrategi och testplan*.

FÖRMÅGA	EXEMPEL PÅ MÄTPUNKTER
Kommunikation	• Kontaktlistor i återställningsplanen är uppdaterade. • Drabbade av störningen eller avbrottet hålls informerade (internt/externt). • Alternativa kommunikationsvägar för incidentrapportering vid störningar i ordinarie system fungerar.
Medvetenhet	• Planägare/systemägare har uppdaterat sin(a) plan(er) på regelbunden basis. • Personal i organisationen är medveten om de rutiner som gäller vid avbrott i system X.
Kompetens	• Planägare/systemägare har mandat och kompetens att fatta de beslut som krävs för att aktivera planen. • Berörda resurser, ordinarie presonal samt ersättare, har kompetens nog att genomföra kontinuitetslösningarna enligt plan.
Samverkan	• Samverkan med interna aktörer fungerar enligt rutiner beskrivna i planen. • Samverkan med externa aktörer fungerar enligt rutiner beskrivna i planen.
Ledning	• Rutin för larmning och eskalering fungerar som avsett. • Verktyg och system för incidentrapportering är funktionella. • Återställningsplanerna ger stöttning i att samordna och inrikta återställningsarbetet.
Logistik	• Reservarbetsplatser fungerar som avsett. • Externa leverantörer kan uppfylla sin del av kontinuitetslösningen.

Fysisk säkerhet	• Det finns en förmåga att återställa primär datahall vid störning eller avbrott med stöd av kontinuitetslösningar beskrivna i planen. • Brand- och översvämningsystem i datahall är funktionella. • Det finns kunskap och förmåga att vid avbrott eller störning säkerställa elförsörjning till datahall med stöd av kontinuitetslösningar beskrivna i planen. • Det finns en kunskap och förmåga att följa upprättad utrymningsrutin.
Teknik	• Det finns en förmåga att återställa server X vid störning med stöd av kontinuitetslösningar beskrivna i planen. • Det finns en förmåga att återställa applikation X vid störning med stöd av kontinuitetslösningar beskrivna i planen. • Det finns en förmåga att återställa nätverk X vid störning med stöd av kontinuitetslösningar beskrivna i planen.
Data	• Det finns förmåga att återställa korrupt eller kontaminerad data i applikation X genom stöd av kontinuitetslösningar beskrivna i planen.
Tidskrav	• Mål för återställningstid för it-resurs X kan mötas med stöd av kontinuitetslösningar beskrivna i planen. • Mål för återställningspunkt för it-resurs X kan mötas med stöd av kontinuitetslösningar beskrivna i planen. • Avtalade tidskrav för it-leverantör X gällande hantering av systemåterställning kan mötas.

Tabell 7: Exempel på mätpunkter.

Utse relevant målgrupp och deltagare

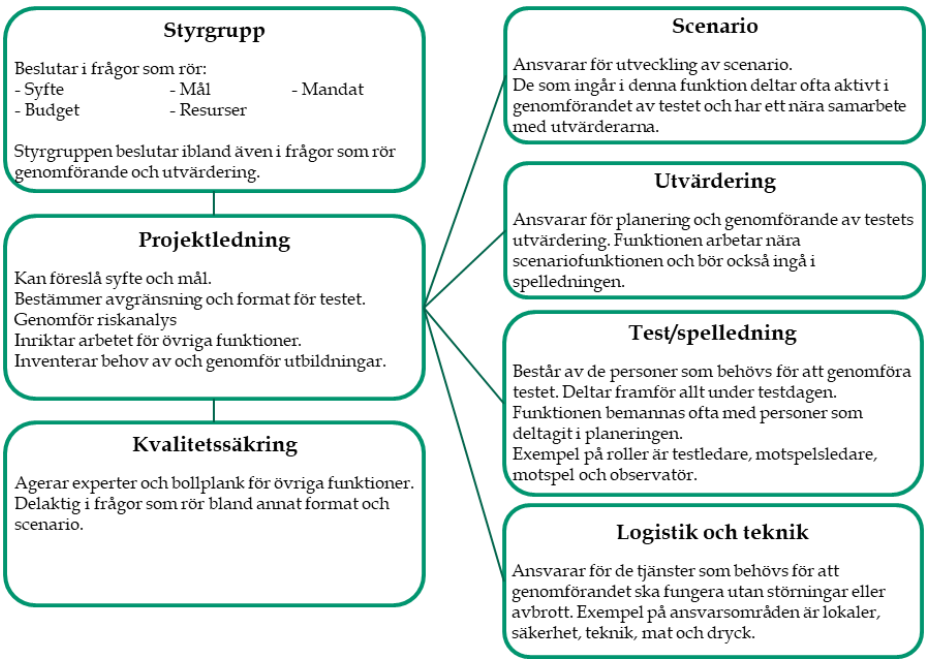
Ett viktigt moment innan ett test genomförs är att utse relevant målgrupp. Målgruppen för det specifika testet bör vara angivet i testplanen. För mindre komplexa testyper, såsom dokumentationsgenomgång eller skrivbordsövning, kan en snävare målgrupp utses. För simuleringar, funktions- eller fullskaletester, där flera system och även ibland hela processer involveras behöver ett större antal målgrupper ingå. Dessa målgrupper kan utgöras av såväl processägare, systemägare och planägare som personal för återställning, slutanvändare och övrig personal inom verksamheten, samt 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.

Skapa en 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 test/spelledning) är en styrgrupp, scenarioansvarig, utvärderingsansvarig samt stödresurser för teknik, logistik och administration. Se *Figur 8* nedan för exempel på testorganisation.



Figur 8: Exempel på testorganisation.

De roller som kan behövas under själva genomförandet av testet beskrivs i *Figur 9* nedan. Dessa utgör testets test- eller spelledning. Vid tester som inkluderar flera delar av organisationen, eller för organisationen kritiska leverantörer, kan lokala testledare samt utvärderare behöva utses.

Figur 9: Roller i test/spelledningen.

Riskhantering och riskanalys

Innan ett test genomförs bör en noggrann och strukturerad riskanalys genomföras, speciellt om det rör sig om ett större och mer avancerat test. Detta för att identifiera vilka risker som det specifika testet kan medföra. Denna riskanalys bör ta utgångspunkt från genomförd riskanalys och fattade riskbeslut i teststrategin.

För att kunna göra en heltäckande riskanalys bör även personer från andra delar av organisationen ingå i analysen. Detta för att få en bättre förståelse för hur testet kan påverka olika delar av verksamheten. Att få in andras synpunkter ger en bredare insikt kring de risker som kan inträffa under testet. Tillsammans avgörs då sannolikheten för att risker inträffar samt konsekvenserna av identifierade risker och dess inverkan. Utifrån resultatet av riskanalysen prioriteras de riskerna som ej kan accepteras utifrån satta risknivåer. Dessa risker tas då vidare för behandling och åtgärd. Även tidigare tester kan utgöra viktiga utgångspunkter för riskanalysen.

Steg 3: Planera inför test

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 tekniska inslag.

Ett test som ska vara så realistiskt och verklighetstroget som möjligt kommer kräva betydligt fler resurser och en omfattande planering.

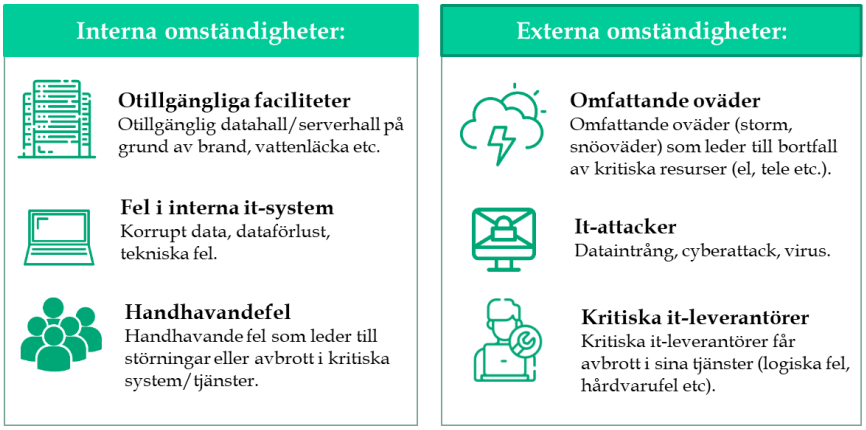
Testtyper bör väljas bland annat med hänsyn till organisationens mognad, ambitionsnivå, resurstillgång, kunskap, storlek, genomförd riskanalys, komplexitet samt nisch inom den finansiella sektorn. Valda förmågeområden bör även beaktas i valet av testtyp.

Det är viktigt att organisationen utvecklar sin erfarenhet inom test innan avancerade testtyper och testmoment genomförs. En testtyp eller ett testmoment som är för svårt i förhållande till organisationens mognadsnivå kan leda till svårtolkade eller bristfälliga resultat eller i värsta fall leda till allvarlig påverkan på verksamheten.

Val av scenario

Baserat på syfte och mål, valda förmågeområden, testtyp, testmoment samt den/de planer eller system/tjänster/resurser som ska testas utvecklas ett relevant scenario. Vid gemensamma tester med ordinarie verksamhet bör scenariot inkludera flera kärnprocesser som gör testet relevant för olika nivåer. Scenariot bör också utgå ifrån organisationens egna identifierade kritiska beroenden. Ett exempel på beroende kan vara en organisations leverantörskedjor. Olika typer av riskanalyser som är genomförda (exempelvis inom kontinuitetshantering, risk- och sårbarhetsanalyser eller hantering av operativa risker) 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. Inträffade händelser eller incidenter inom den egna verksamheten kan också fungera som inspiration vid scenarioutveckling.

Även om valet av scenario är viktigt bör scenariot i sig inte utgöra testets huvudsyfte. Fokus för testet bör istället läggas på it-verksamhetens förmåga att upprätthålla och/eller återställa kritiska it-resurser. Scenarier kan behandla både interna och externa omständigheter. De kan beröra allt ifrån kritiska it-leverantörer som får avbrott i sina tjänster, eller fel i interna it-system (exempelvis korrupt data, dataförlust eller tekniska fel).



Figur 10: 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 och testmoment påverkar utvärderingsfunktionens metoder för hur observationer och bedömningar kan genomföras. Den vanligaste metoden för utvärdering är att genomföra observationer med utgångspunkt från testets definierade mål och mätpunkter. Ett framtaget testprotokoll underlättar dokumentationen under genomförandet av testet. Denna typ av testprotokoll är särskilt användbart vid mer avancerade testtyper såsom simuleringar, funktions- eller fullskaletester. För validering av testets uppfyllande upprättas acceptanskriterier som ska stödja i bedömningen av uppsatta mål och mätpunkter (se mall för testprotokoll).

Grön = Godkänd - Testfall kördes och bedömdes vara acceptabla.

Gul = Godkänd med kommentar - Testfall kördes och bedömdes vara acceptabla till viss del, men med anmärkning.

Röd = Underkänd - Testfall misslyckades eller kunde ej genomföras. Resultatet av genomfört testfall reflekterar inte den befintliga designen av lösning/rutiner som finns beskrivet i återställningsplanen.

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

MALLAR FÖR GENOMFÖRANDE
- TESTPROTOKOLL -

Datum: XX-XX-XX **Scenario:** [Korrupt data] **Plan:** [Återställningsplan – ERP-system]									
Förmågeområden: [Tidskrav, Data]									
Mål/mätpunkter	**Kritisk it-resurs**	**Testmoment**	**RTO**	**RPO**	**Aktuell RTO /RPO vid genomfört test**	**Återställd volym/ kvalitet (%)**	**Status:** Godkänd ○ Godkänd med kommentar ○ Underkänd ○	**Kommentar** Vilket stöd utgör återställlningsplanen? Är stödet från återställningsplanen tillräckligt? Vad behöver utvecklas? Identifierade risker?	**Åtgärder**
Mål: Förmåga att återställa den/de system/tjänster eller resurser som testas.	**ERP-systemet**	Dataåterställning					○ ○ ○		
Mätpunkt 1: Innehar förmåga att återställa korrupt eller kontaminerad data i ERP-systemet i enligt med uppsatta tidskrav i återställningsplan utan dataförlust.	ERP-systemet	Dataåterställning					○ ○ ○		

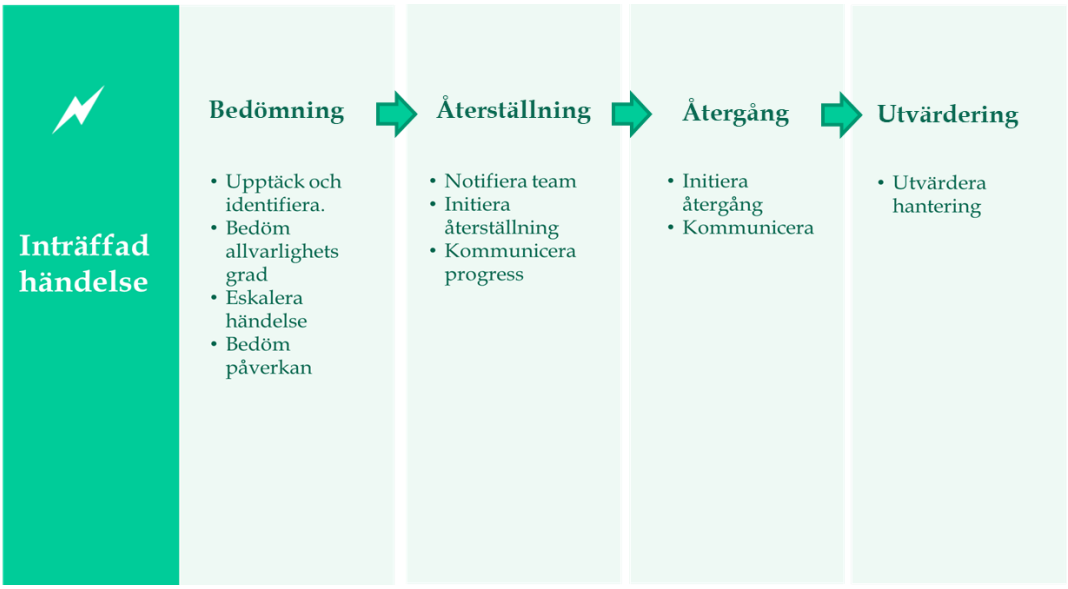
Steg 4: Genomföra test

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

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

För mer tekniska testtyper så som simuleringar, funktions- eller fullskaletester behöver dock scenariot oftast presenteras på ett mer realistiskt sätt, d.v.s. att testet genomförs som vid en verklig händelse.

Tester av återställningsplaner kan med fördel genomföras genom att följa faserna för återställningshantering av en inträffad händelse. Nedan exeplifieras detta genom; *bedömning, återställning, återgång och utvärdering*.



Figur 10: Tester av återställningsplaner kan mycket väl struktureras och utgå ifrån de fyra faserna för återställningshantering; bedömning, återställning, återgång, utvärdering.

Bedömning syftar på den fas där händelsen upptäcks och identifieras. Det bör under testet finnas en möjlighet att testa om det finns en tydlig och strukturerad process på plats för att i ett tidigt skede upptäcka och bedöma en inträffad händelse, detta för att händelsen inte ska få för stor påverkan på de kritiska it-resurserna. När bedömningen är genomförd ska det finnas rutiner på plats för att notifiera och larma den grupp som ansvarar för återställningsarbetet, detta så att rätt kontinuitetslösningar som beskrivs i återställningsplanen kan användas som stöd i återställandet av den eller de aktuella kritiska it-resurserna som avbrottet gäller. Att testa notifiering och larmning kan vara ett bra sätt att se om rutinerna som beskrivs i återställningsplanerna är funktionella.

Gruppen för återställning bör under själva återställningsarbetet också kontinuerligt kommunicera progress. När den kritiska it-resursen är tillgänglig igen ska det också finnas rutiner på plats som beskriver återgång till normalläge, samt hur detta kommuniceras till berörd verksamhet. Som ett sista steg i testet bör det också finnas möjlighet att utvärdera hanteringen av händelsen för att på så sätt dra lärdomar av resultatet.[11]

Nedan följer några exempel på genomförande av tester. Exemplen följer de fyra faserna för återställningshantering som tidigare beskrivits i avsnittet, det vill säga; *bedömning, återställning, återgång och utvärdering*.

Scenario 1: Mjukvarufel	
Testtyp: Simulering **Testmoment:** Återställning av system eller applikation	**Valda förmågor att testa:** Teknik, Data, Kommunikation **Testade planer:** Återställningsplan CRM-system
Bedömning Efter 6 timmar av driftsättande av ny version av kundplatform rapporterar kunder problem och det visar sig att CRM-systemet innehåller en allvarligare bugg som passerat test och verifiering utan att detekteras. Graden av allvarlighet gör att systemet måste återställas till tidigare version. Kunder, systemägare och ledning informeras. Systemet beräknas vara nere 4 timmar under arbetstid. **Återställning** Defekta system tas offline, samtidigt som ansvariga för återställning påbörjar återläsning av den senaste kvalitetsgranskade säkerhetskopian. Systemets alla mjukvarudelar är återlästa efter 2 timmar varpå start och test av återlästa versionen påbörjas och är slutförda efter ytterligare 45 minuter. **Återgång** Plattformen öppnas för extern access. Alla intressenter meddelas om att systemet är tillbaka med föregående version.	

[11] *ISO/IEC 27031:2011, Guidelines for information and communication technology readiness for business continuity (2011).*

Kunder notifieras om händelsen och planering för ny uppgradering påbörjas.

Utvärdering/Resultat

- *Teknik:* Under testet identiferades vissa tekniska brister i nuvarande lösning för återställning. Nya effektivare lösningar för återställning bör utredas vidare.
- *Data:* Data kunde återställas utan dataförlust. Inga avvikelser att rapportera.
- *Kommunikation:* Kunder, systemägare och ledning informerades och hölls uppdaterade under testet. Inga avvikelser att rapportera

Scenario 2: Korrupt / förvanskad data	
Testtyp: Funktionstest **Testmoment:** Dataåterställning	**Valda förmågor att testa:** Data, Teknik, Kompetens, Ledning **Testade planer:** Återställningsplan Handelssystem

Bedömning

Vid en avräkning i plattformen för genomförande av handel visar det sig att data försvunnit vid en tidpunkt två veckor tidigare i systemet. Detta genom ett misstag av en användare. Historisk data måste återställas snarast, dock inte under dagtid. Produktionsstopp måste minimeras. Systemägare notifieras och anvariga för återställning aktiveras för att återläsa databas samt transaktionsloggar för att unvika dataförlust av nyare data.

Återställning

Databasen återläses till sista tidpunkt som innehåller den borttagna datan, varpå inläsning av transaktionsloggar genomförs i väntan på tidpunkt för accepterat driftstopp.

Vid driftstopp inläses återstående transaktionloggar så att datan blir komplett. Återställning av data slutförs och kommuniceras.

Återgång

Överkoppling till återställd databas genomförs.

System för produktion startas igen och data verifieras innan systemet öppnas för användare nästkommande arbetsdag.

Utvärdering/Resultat

- *Ledning:* Rutiner för initiering av hantering och samordning av återställningsarbetet fungerarde väl under testet. Inga avvikelser att rapportera.
- *Data och kompetens*: Återställning av data fungerade utan incidenter, dock identifierades att endast ett fåtal individer inom organisationen har kompetens nog för att genomföra sådana operationer.
- *Teknik*: För att minska riskerna för handhavandefel i kritiska system rekommenderas åtgärder för att minimera möjligheterna att kunna radera data av misstag.

Scenario 3: Hårdvarufel	
Testtyp: Parallellt funktionstest. **Testmoment:** Återställning av nätverk, Failover. Återställning av brandvägg.	**Valda förmågor att testa:** Samverkan, Logistik, Ledning, Teknik, Tidskrav **Testade planer:** Återställningsplan Kärnnätverk (Core network) samt Återställningsplan Brandvägg

Bedömning

Övervakningsystem larmar till jour om att en av två controllermoduler fallerat i central core switch. Ingen omedelbar påverkan är rapporterad men det finns fortsatt en hög risk så länge controllern inte har återställts. Fallerar controller nummer två kan stora delar av organisationens it-system bli otillgängliga.

Eskalering sker till driftchef som beslutar om att sätta ansvarig för nätverket i 24/7 standby tills controllermodulen är utbytt.

Samtidigt inkommer rapporter och automatlarm om att klienter tappar anslutningar mot olika system i banken. Larm bekräftar att paket tappas när det ska passera branväggen som skiljer produktion och klientnät. Vid undersökning visar det sig att ett nytt system som driftsattes så sent som i förra veckan har ett utökat trafikmönster mot föregående version, vilket har orsakat att säkerhetsfunktioner i brandväggen inte hinner scanna all trafik, och då tappat paket.

Återställning

Ny controllermodul behöver beställas då detta inte finns lagerhållet av den egna organisationen. Leverantören har ett SLA på att leverera reservdelar inom 8 timmar.

Efter att reservdelar levererats från leverantör kan controllermodulen bytas ut, och en automatisk återställning kan göras av den andra controllern i switchen.

Återställning görs samtidigt som ordinarie verksamhet fortgår.

Tillfällig workaround genomförs för att hantera brandväggsproblemen, detta genom att sänka nivån på säkerhetsscanningen. För att återgå till normal drift undersöks samtidigt möjligheterna att öka kapaciteten i scanningen.

Återgång

Kommunkation till inblandade intressenter såsom påverkade systemägare har genomförts.

Nätverksteamet inte längre i 24/7 standby.

Utvärdering/Resultat

- *Ledning*: Rutiner för initiering av hantering i återställningsplan fungerarde väl under testet. Inga avvikelser att rapportera.
- *Teknik*: Automatisk failover av controller har fungerat enligt plan. Inga avvikelser att rapportera. Brandvägg saknar lösningar för att effektivt hantera överbelastning av trafik. Ny lösning för att bättre hantera och återställa brandvägg vid överbelastning bör utredas vidare.
- *Samverkan*: Samverkan mellan inblandade team och leverantör har fungera väl. Inga avvikelser att rapportera.
- *Tidskrav och logistik*: Verifiering av leverantörs SLA visar att dom inte kan möta kravet på leverans av ny reservdel inom 8 timmar då dessa av kostnadskäl lagerförs centralt i Europa och måste flygas in. Eskalering och omförhandling med leverantör bör genomföras omgående.

Steg 5: Utvärdera och återkoppla test

Utvädering

Vid avslutningen av varje test bör en utvärderingsdiskussion genomföras. Syftet med utvärderingsdiskussionen är att ge deltagarna möjlighet 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.

Även testsledning och utsedda observatörer bör deltaga aktivt under utvärderingsdiskussionen för att lyfta eventuella problem eller brister som uppmärksammats under testet.

Genomförda tester resulterar ofta i behov av att revidera gällande återställningsplaner. Det är också troligt att nya risker uppdagas gällande den tekniska lösningen som kräver omdesign av antingen enskilda it-system eller hela återställningsmiljön om riskerna inte kan accepteras. Dessa framkomna brister i framtagna kontinuitetslösningar kan då utgöra underlag för nya investeringsbeslut.

Utvärderingsdiskussionen bör främst utgå ifrån testets uppsatta syfte och mål. Nedan ges exempel på övergripande frågeställningar som kan behöva besvaras under utvärderingsdiskussionen:

- ✓ Vilket stöd utgjorde återställningsplanen?
- ✓ Var stödet från planen tillräckligt?
- ✓ På vilket sätt behöver återställningsplanen utvecklas?
- ✓ Kunde definierade tidskrav i planen mötas, eller behöver tidskraven korrigeras efter genomfört test?
- ✓ Kunde data återställas korrekt i förhållande till volym och kvalitet?
- ✓ Kunde samtliga planerade aktiviteter utföras under genomförandet av testet?
- ✓ Framkom brister i framtagna kontinuitetslösningar under testet som kan utgöra underlag för investeringsbeslut?
- ✓ Vilka risker identifierades under testet?

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 8* nedan för exempel på en enkel åtgärdslista.

Åtgärdsförslag	Ansvarig	Deadline	Kommentar

Tabell 8: Exempel på åtgärdslista att inkludera i rapport.

Rekommendationerna i testrapporten bör med fördel struktureras 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.

Återkoppling

Testrapportens resultat och slutsatser bör återkopplas till samtliga deltagare samt övriga intressenter så snart som möjligt efter avslutat test. Då resultatet av genomförda tester kan innebära stora investeringsbeslut, både kostnadsmässigt och tidsmässigt, behöver beslut fattas på strategisk nivå. De personer som beslutar om ambition, strategi och budget måste därför känna till vad som framkommit av testet och vilka investeringar som kan behöva genomföras för att hantera eventuella nya upptäckta risker. Rapportens resultat bör även integreras i ordinarie riskprocess för att undvika separat hantering utanför ordinarie riskmiljö.

Steg 6: Implementera och följa upp test

Utvärderingsresultat samt rekommendationer i testrapporten bör ligga till grund för en handlingsplan för granskning, uppdateringar och förbättringar av it-verksamhetens kontinuitetsstrategier, teststrategi samt återställningsplaner. Handlingsplanen bestämmer hur rekommendationerna i testrapporten kommer att implementeras och tillämpas inom organisationen. Planen bör innehålla specifika förbättringsåtgärder för verksamhetens återställningsplaner, en satt tidsram för när varje identifierad åtgärd såsom implementeringen av nya strategier eller kontinuitetslösningar ska vara genomförda, samt en statusindikator som visar på statusen för respektive åtgärd. Säkerställ också att handlingsplanen beslutas i rätt organisationsled, med rätt mandat för att kunna hantera till exempel investeringsbehov. Ansvaret för genomförandet av åtgärder bör även fördelas inom organisationen.

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 uppföljningsmöten, med det beslutande organisationsleden, för att hållas levande och uppdaterade. Dessa handlingsplaner bör även integreras i ordinarie riskprocess för att undvika separat hantering utanför ordinarie riskmiljö.

4.3 *Rapportering*

Rapportering av resultatet från genomförda tester av kontinuitetsplaner ska enligt Finansinspektionens föreskrifter samt EBA:s och EIOPA:s IKT-riktlinjer ske minst årligen till ledning och styrelse. 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 återställa kritiska it-resurser. It-verksamheten bör därför ha en rutin för hur ofta rapportering ska ske till ledning och styrelse.

För att få en heltäckande bild av it-verksamhetens återställningsförmåga bör även krav ställas på kritiska it-leverantörer att inkomma med rapportering gällande genomförda tester, testresultat inklusive upprättade åtgärdsplaner.

Rapporteringen kan innehåll följande delar:

- ✓ Kort beskrivning av syfte, mål och mätpunkter för genomförda tester.
- ✓ Status på återställningsplaner samt andel planer som är testade.
- ✓ Övergripande beskrivning av testade scenarier samt förklaring till valda scenarier kopplat till organisationens riskanalys.
- ✓ Beskrivning av vilka teststyper och testmoment som genomförts.
- ✓ Förklaring till prioritering av kritiska it-resurser, samt varför vissa it-resurser 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 återställa kritiska it-resurser vid avbrott eller störning.
- ✓ 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.
- ✓ Genomförd riskanalys.

5 Referenser

- European Commission, Solvency II (2009/138/EC).
- European Banking Authority. EBA Guidelines on ICT and security risk management, EBA/GL/2019/04.
- European Banking Authority. EBA Guidelines on security measures for operational and security risks of payment services under PSD2 (EBA/CP/2017/04).
- Finansinspektionen (2014), Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1).
- Finansinspektionen (2014), Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4)
- Finansinspektionen (2014), Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem (FFFS 2014:5)
- FSPOS Vägledning för kontinuitetshantering (2021).
- ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements (2019).
- ISO/IEC 27031:2011, Guidelines for information and communication technology readiness for business continuity (2011).
- ISO 31000 - Risk management – Principles and guidelines (2018).
- Myndigheten för samhällsskydd och beredskaps (MSB:S) föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
- Payment services (PSD 2) - Directive (EU) 2015/2366.
- SS-EN ISO 22301:2019 - Säkerhet och resiliens - Ledningssystem för kontinuitetshantering - Krav (2019).
- SS-ISO 22325:2016 - Krishantering - Vägledning för förmågeutvärdering (2016).
- The European Insurance and Occupational Pensions Authority (EIOPA) Guidelines on Information and Communication Technology (ICT) security and governance (EIOPA-BoS 19/526) (2020).
- The Open Group Architecture Framework (TOGAF 2020).