FINANSTILSYNET

DANMARKS NATIONALBANK

Stresstest af operationel robusthed

Rapport

Juli 2026

Indholdsfortegnelse

Stresstest af operationel robusthed

Denne rapport præsenterer resultaterne af en stresstest af operationel robusthed på sektorniveau, som Finanstilsynet og Danmarks Nationalbank i 2025 gennemførte sammen med 11 virksomheder fra den finansielle sektor; Danske Bank, Jyske Bank, Nykredit-koncernen, Sparekassen Kronjylland, SEB, Nordea, JN Data, BEC, Bankdata, Netcompany Banking Services og VP Securities A/S[1].

Testen fokuserede på værdipapirområdet og havde til formål at undersøge, hvordan sektoren samlet kan håndtere ekstreme med plausible IT-hændelser, der påvirker samfundskritiske funktioner. Rapporten beskriver testens metode, scenarie og centrale læringspunkter I bilag 1 beskrives metoden bag testen mere udførligt. Bilaget kan bruges som inspiration i andre sektorer med komplekse afhængigheder og samfundskritiske funktioner, som ønsker at prøve kræfter med redskabet. I bilag 2 angives refleksionsspørgsmål, som andre finansielle virksomheder og sektorer kan lade sig inspirere af til at videreudvikle deres beredskabsplaner, uden nødvendigvis at kaste sig ud i en stor testøvelse.

Perspektiver og læringsmuligheder

Virksomheder, der er en del af Danmarks kritiske infrastruktur, er nødt til at forholde sig til, at operationel robusthed ikke kun handler om egne systemer og beredskabsplaner. De fleste nødplaner bygger på den antagelse, at resten af sektoren fungerer normalt, når en krise opstår. Men hvad sker der, når denne antagelse ikke holder?

Når den samlede sektor påvirkes, bliver det afgørende at have fælles, velforberedte og testede planer for krisehåndtering, genetablering og videreførelse af kritiske funktioner. Den udførte test af operationel robusthed har givet værdifuld indsigt i, hvordan de enkelte virksomheder og sektoren kan styrke deres evne til at håndtere krisen.

En stresstest af denne karakter giver mulighed for at:

- afprøve og udfordre eksisterende beredskabsplaner under realistiske og komplekse scenarier
- afprøve, hvordan samarbejde, kommunikation og beslutningsprocesser fungerer, når ingen enkelt aktør kan løse krisen alene
- skabe fælles forståelse for roller, ansvar og beslutningsveje, så alle parter ved, hvem der skal gøre hvad – og hvornår – under en krise
- identificere styrker og svagheder i informationsdeling og koordinering, og hvor der er behov for at iværksætte tiltag, som sikrer, at både interne og eksterne parter får klare og koordinerede budskaber

[1] Deltagerne i testen var delt ind i to kategorier. De syv kategori 1-deltagere har, udover de fælles læringer, der sammenfattes i denne rapport, også modtaget individuelle rapporter med læringspunkter.

- identificere, hvor der er behov for at videreudvikle fælles standarder og procedurer for forretningsvidereførelse, genetablering og genåbning, som styrker sektorens evne til at opretholde kritiske forretningsprocesser og sikre en effektiv og pålidelig genopretning af driften.

Sammenfattende viser erfaringerne fra stresstesten, at det er nødvendigt løbende at udfordre egne antagelser og praksis for samarbejde. Der skal være styr på egne nødplaner, men man skal også være opmærksom på, at genopretning, videreførelse og krisehåndtering i nogle scenarier kræver fælles, velforberedte og testede planer på tværs af sektoren.

Formål med en stresstest af operationel robusthed på sektor-niveau

Truslerne mod den finansielle sektor udvikler sig hastigt, og de seneste år har især cybertrusler, ransomware og AI skabt et mere komplekst og uforudsigeligt risikobillede. AI kan både bruges til at styrke forsvar og til at udføre mere avancerede angreb, og automatisering gør det muligt for trusselsaktører at ramme flere virksomheder samtidigt og mere effektivt. Samlet set betyder det, at det bliver mere og mere væsentligt ikke bare at kunne forsvare sig mod angreb. Sektoren skal også kunne opretholde og genetablere kritiske forretningsprocesser under og efter en operationel hændelse. Virksomhederne og sektoren skal med andre ord være forberedte og øve sig på at kunne videreføre deres kritiske funktioner under længerevarende nedbrud og på hurtigt at kunne vende tilbage til normal drift på tværs af forskellige nedbrudsscenarier.

Stresstesten af operationel robusthed på sektorniveau er den første af sin slags i EU. Det er således en ny tilgang, hvor en stor del af en finanssektor testes over en længere periode i en kombination af kriseøvelser i realtid og skrivebordsøvelser. Den første cyberstresstest i Danmark i 2023 fokuserede på individuelle virksomheder, mens den seneste test har haft fokus på, hvordan aktørerne samarbejder og håndterer en fælles, langvarig IT-hændelse på tværs af den finansielle sektor.

Den enkelte virksomhed kan teste sin egen parathed, men på grund af den høje grad af forbundethed i den finansielle sektor kan den ikke afdække, hvordan dens mangler eller handlinger påvirker andre, eller hvordan andres mangler eller handlinger påvirker den enkelte virksomhed. Derfor har både myndigheder og virksomheder et fælles incitament og ansvar for at teste og styrke sektorens robusthed, så kritiske funktioner kan opretholdes under alvorlige hændelser. Myndigheder og virksomheder har fælles interesser, når man bruger ressourcer på at teste sektorens robusthed: begge har ønske om, at sektoren som helhed kan opretholde samfundskritiske funktioner under alvorlige operationelle hændelser

En stresstest på sektorniveau er et instrument, der gør samarbejdet operationelt: i det fælles øvelsesrum bliver reelle afhængigheder og brudflader synlige. Testen handler ikke om at finde fejl, men om at skabe fælles læring og udvikling.

Testens scenarie

Scenariet i stresstesten blev udviklet i tæt samarbejde med deltagerne for at udfordre grundlæggende antagelser om tilgængelighed og stabilitet i sektoren.

Værdipapirområdet blev valgt, fordi netop dette område, værdipapirhandel og de underliggende infrastrukturer, udgør et centralt fundament for sektorens forretningsprocesser og funktioner. Her kan en teknisk eller datamæssig forstyrrelse hurtigt få konsekvenser for hele sektoren – ikke kun for de direkte berørte virksomheder, men også for deres kunder, samarbejdspartnere og samfundet som helhed. Under normale omstændigheder er disse afhængigheder ofte usynlige, fordi de fungerer stabilt og effektivt.

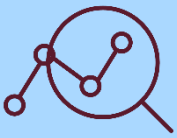
Scenariet i testen involverede et angreb, hvor handelsdata gradvist blev manipuleret over uger, før det blev opdaget. Det betød, at både respons og genetablering blev vanskeligere, fordi manipulationen også kunne have påvirket backups. Scenariet gav derfor mulighed for at undersøge tre centrale områder:

1. Hvordan håndteres forretningsvidereførelse og genetablerings-processer, når selv backups kan være kompromitteret af et langvarigt angreb?
2. Hvordan fungerer samarbejdet om at gendanne fælles og kritiske data, ikke mindst når deltagerne har forskellige metoder til at opretholde deres forretningsprocesser under en krise?
3. Hvordan balancerer og integrerer virksomheder sektorens fælles beredskab med deres egne lokale beredskabsplaner, når begge skal fungere samtidigt under pres?

Scenariet blev designet til at afprøve tværgående samarbejde i praksis og sætte fokus på de forberedelser og det samspil, der er nødvendige for, at sektoren kan håndtere en krise kollektivt.

Testens metode

Testen blev gennemført som en kombination af skriftlige skrivebordsøvelser, live scenariestyring både online og fysisk samt strukturerede spørgeskemaer. Kombinationen af metoder gav mulighed for både dybdegående refleksion og samarbejde i realtid. Metoden er uddybet i bilag 1.



Forskellen på at teste hurtigt og langsomt

Der er væsentlig forskel på en almindelig kriseøvelse og en stresstest af operationel robusthed, og de to typer tests har forskellige fordele og begrænsninger. En almindelig kriseøvelsevarer typisk ca. en dag. Det er en komprimeret øvelse, hvor en gamemaster typisk styrer forløbet, og deltagerne hurtigt skal reagere på nye spor og udfordringer. Det fremprovokerer realistisk stress og giver ressourceeffektiv læring, men begrænser samtidig muligheden for at fordybe sig i beslutningsprocesser, fordi fokus er på at teste organisationens umiddelbare reaktioner.

En stresstest af operationel robusthed fungerer mere som en eksplorativ øvelse over længere tid. Deltagerne får mulighed for at arbejde grundigt med samarbejde, refleksion og beslutningstagning. Det styrker organisationens evne til at håndtere komplekse og langvarige krisesituationer, fordi deltagerne kan afprøve forskellige tilgange i egen organisation, prøve dem af i kriseøvelser i realtid sammen med andre deltagere, og bagefter reflektere over, om man kunne have håndteret det bedre eller anderledes som fællesskab og lære af erfaringerne undervejs. Samtidig kræver testformen en del ressourcer fordelt over en længere periode og kan dermed være vanskelig at gennemføre hyppigt. Valg af testformat vil derfor afhænge af bl.a. formål og ressourceforbrug.

Deltagerne var med til at udvikle og prioritere scenarier i en række workshops, hvor både tekniske og forretningsmæssige eksperter bidrog med erfaringer og løsninger. Under selve testen blev samarbejdet sat på prøve. Deltagerne skulle håndtere datakorrumpering og koordinere kommunikation og beslutninger på tværs af deres organisationer. På den måde blev både lokale og fælles beredskabsplaner testet samtidigt. Sektorens fælles kriseberedskab (FSOR Krisberedskab) blev brugt aktivt. Efter testen delte deltagerne deres erfaringer og læringspunkter i evalueringer og workshops.

Den fælles test og erfaring med, hvor der opstår udfordringer i samarbejdet, og hvor den enkelte virksomhed står mindre stærkt, skaber en stærk motivation for alle parter til at rette op på svagheder og arbejde sammen om løsninger. Stresstesten styrker dermed både den fælles forståelse og evnen til at agere samlet.

Testens centrale læringspunkter

Med testen har finanssektoren for første gang undersøgt, hvordan lokale og fælles beredskaber fungerer sammen under en ekstrem, men plausibel hændelse over længere tid. Nogle af testens læringspunkter er scenariespecifikke, mens andre er mere generelle. Det er væsentligt at understrege, at forståelsen af en tests læringer skal ses i lyset af i, at testens design og tilrettelæggelse påvirker resultater og læringspunkter.

Testens mest centrale læringspunkter, som danner grundlag for det videre arbejde, er sammenfattet herunder:

1. læringspunkt: Effektiv koordinering mellem lokale og fælles beredskaber

Ved en større krise aktiveres både de enkelte virksomheders lokale beredskab og sektorens fælles beredskab, FSOR's kriseberedskab. Testen viste, at det i praksis er en kompleks og ressourcekrævende opgave for både virksomheder og myndigheder at håndtere egne interne processer og eget kriseberedskab samtidigt med aktiv deltagelse i sektorens koordinerende beredskab. Deltagerne oplevede, at det kræver betydelig kapacitet og overblik at undersøge hændelsen, træffe beslutninger lokalt og samtidig bidrage til fælles sektorkoordinering – især under tidspres og med begrænset information.

Det kan være udfordrende at få lokale og sektorbaserede beredskaber til at fungere effektivt sammen. Et læringspunkt, som der arbejdes videre med er, at roller, ansvar og beslutningskompetencer skal være tydeligt forberedt, når både lokale og sektorbaserede processer er i gang samtidig.

2. læringspunkt: Krisekommunikation i fællesskab

Effektiv intern og ekstern kommunikation er afgørende for at bevare overblikket og tilliden under en krise. Testen gav anledning til refleksioner over, hvordan variationer i virksomhedernes valg af krisehåndtering og kommunikation – et naturligt resultat af forskellige forretningsmodeller – potentielt kan føre til forvirring blandt kunder, offentligheden og medarbejdere. Mediedækning og offentlig debat kan hurtigt forstærke denne effekt, og tillid eller mistillid kan sprede sig på tværs af aktører, også til virksomheder i og uden for sektoren, der ikke selv er direkte ramt. Det er derfor værd at overveje på forhånd, hvordan forskellige tiltag påvirker kommunikationen, og om og hvornår det er muligt og hensigtsmæssigt at sigte mod at koordinere udmeldinger til kunder og offentlighed for at undgå unødvendig eskalering.

3. læringspunkt: Samarbejde om videreførelse, genopretning og prioritering under kriser

Når en større hændelse rammer mange aktører samtidigt, bliver videreførelse og genopretning af kritiske funktioner en kompleks og fælles opgave. I en sektor, hvor mange virksomheder er forbundet gennem centrale infrastrukturer og er afhængige af fælles data, er det sjældent muligt for én aktør alene at genskabe normal drift eller få overblik. Genetablering bliver i stedet et puslespil, hvor hver deltager har en del af løsningen, og hvor samarbejde og koordinering er nødvendig for at danne et samlet billede.

Løsningen afhænger derfor af, at virksomhederne samler deres viden og data for at få et fælles grundlag for genåbning af markedet. Denne proces kræver teknisk indsigt, tillid og enighed om, hvordan information valideres og sammenholdes på tværs. Testen gav indsigt i, hvordan disse tilgange og prioriteringer materialiserer sig, og hvordan processen defineres af, at hver virksomhed har egne forretningsbehov, tekniske løsninger og vurderinger af, hvornår virksomhedens del af infrastrukturen er klar. Det kan betyde, at genopretningen sker trinvis, og at der opstår behov for yderligere dialog og løbende afstemning om næste trin i genetablerings-fasen.

4. Læringspunkt: Genåbning af normale forretningsprocesser – balancen mellem sikkerhed og tempo

Genåbning og overgangen til normal drift efter en større hændelse stiller sektoren overfor komplekse afvejninger. I samarbejdet om at genåbne kritiske forretningsprocesser skal sektoren balancere ønsket om hurtig genåbning for at mindske negative konsekvenser og behovet for at sikre, at data og systemer er pålidelige. Virksomhederne i testen var forskelligt eksponeret i scenariet, og det var derfor ikke entydigt i udgangspunktet, hvornår og hvordan driften skulle genoptages.

En længerevarende nedlukning af kritiske servicer kan have vidtrækkende konsekvenser – ikke kun for de direkte berørte virksomheder, men også for samfundsøkonomien og tilliden til sektoren. Det er derfor afgørende, at virksomhederne træffer beslutninger om genåbning på et oplyst grundlag, hvor både risici og samfundsmæssige hensyn indgår. Et centralt læringspunkt i testen var, at når sektoren har drøftet og afprøvet principper og processer for genåbning på forhånd, er den bedre rustet til at træffe hurtige og velbegrundede beslutninger, der balancerer teknisk sikkerhed med samfundsmæssige behov.

Fremadrettede initiativer

Stresstesten af operationel robusthed har givet indblik i, hvordan sektoren reagerer, når flere aktører rammes samtidigt af en alvorlig, men plausibel hændelse. Testen har tydeliggjort, at robusthed både handler om tekniske løsninger og individuelle beredskabsplaner til forretningsvidereførelse og teknisk genopretning, og også i høj grad om evnen til at samarbejde, dele information, sikre videreførelse af kritiske funktioner i fællesskab og træffe svære beslutninger under pres.

På baggrund af testen er der igangsat tre nye initiativer:

- Udvikling af en fælles playbook med praktiske retningslinjer i et scenarie med nedbrud på værdipapirområdet.
- Styrkelse af koordineret ekstern krisekommunikation på tværs af sektor og myndigheder.
- Styrkelse af det kollektive beredskab på tværs af relevante scenarier.

Disse tiltag skal sikre, at sektoren står endnu stærkere, hvis en større hændelse indtræffer.

Formålet med initiativerne er således at supplere og understøtte den operationelle robusthed og beredskabsansvar hos de enkelte systemaktører på sektorniveau – ikke at erstatte det.

Metoden og potentialet for læring rækker ud over den finansielle sektor og kan inspirere andre sektorer med komplekse afhængigheder mellem kritiske funktioner. Ved løbende at udfordre egne antagelser og afprøve beredskabet i praksis, også på et sektorniveau, kan organisationer styrke deres evne til at videreføre kritiske funktioner under nedbrud og komme hurtigt tilbage efter alvorlige hændelser.

Bilag 1: Hvis du vil arbejde videre med nogle af de identificerede temaer i din egen organisation

Dette afsnit er skrevet til dig, der arbejder i en virksomhed i finanssektoren eller en anden kritisk sektor, og som ønsker at vide, hvordan du kan bruge indsigterne fra stresstesten i din egen organisation. Afsnittet indeholder konkrete refleksionsspørgsmål, som kan bruges til at videreudvikle jeres eksisterende beredskabsplaner og samarbejdspraksisser, både internt og i samspil med andre aktører i sektoren.

Spørgsmålene bygger på erfaringer fra stresstest af operationel robusthed på sektorniveau i finanssektoren og peger på områder, hvor det er særligt vigtigt at tænke ud over egen organisation. De kan bruges som afsæt for dialog i bestyrelsen, krisestaben, mellem IT og forretning og i samarbejdet med leverandører.

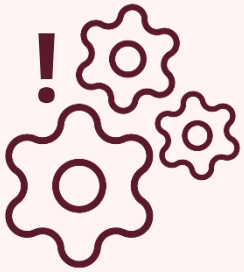
Afsnittet er tænkt som et praktisk værktøj til at:

- teste og videreudvikle jeres beredskabsplaner
- styrke samarbejde og kommunikation på tværs af organisationer
- identificere og håndtere gensidige afhængigheder
- forberede jer på komplekse krisescenarier, som påvirker hele sektoren.

1.

Antagelser i jeres nødplaner

Jeres nødplaner bygger på antagelser om omverdenen: At leverandøren er tilgængelig, at modparten kan modtage, og at infrastrukturen fungerer. Antagelserne er fornuftige for at skabe konkrete og handlingsorienterede planer, men er I opmærksomme på, hvilke risici antagelserne medfører, og i hvilke scenarier de bliver udfordret?



1. Hvilke af jeres nødplaner forudsætter, at andre aktører, f.eks. leverandører, modparter og infrastruktur, fungerer normalt? Er disse forudsætninger dokumenteret?

2. Har I vurderet hvad I gør, hvis kritiske leverandører eller samarbejdspartnere også er ramt, og om jeres virksomhed i stand til at indsætte alternative løsninger eller procedurer for samarbejde under pres?

3. Har I testet, hvad der sker, hvis antagelser i de identificerede planer ikke holder?

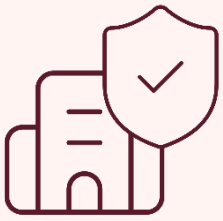
2. Kommunikation og koordination

Når flere aktører er påvirket af den samme hændelse, bliver kommunikation en fælles opgave. Hvad én organisation melder ud, påvirker alle andre, og det kan være vanskeligt at koordinere, hvem der siger hvad hvornår.

1. Har jeres kommunikationsplan taget højde for, at andre berørte aktører kan melde ud før jer, og at I derefter tvinges til at reagere på deres udmelding?
2. Ved jeres kommunikationsafdeling, hvem de skal koordinere med, hvis en hændelse rammer på tværs af sektoren? Har I aftalt en proces for det?
3. Kender I de eksisterende mekanismer for koordinering i sektoren, f.eks. krisberedskaber og myndighedskanaler, og er de integreret i jeres egen kommunikationsplan?

3. Sektorsamarbejde og aktivering af beredskab

Jeres beredskab er løbende testet og forbedret gennem interne øvelser med realistiske scenarier og skrivebordsøvelser. Men det er en anden opgave at indgå i et større sektorberedskab i samarbejde med andre virksomheder, der hver især har deres egen måde at opbygge et beredskab på og egne hensyn.



1. Ved jeres krisestab, hvornår og hvordan sektorens fælles beredskab aktiveres, og hvad der forventes af jer, f.eks. bemandingsmæssigt?
2. Har I testet, hvordan jeres lokale beredskab fungerer i konteksten af sektorhændelser?
3. Har I overvejet, hvordan jeres sektor som helhed håndterer en hændelse, der rammer fælles infrastruktur? Og om der er en plan for det, der rækker ud over den enkelte organisations nødplan?

4.

Anerkendelse og planlægning af gensidige afhængigheder

De fleste organisationer tænker primært på krisehåndtering fra deres eget perspektiv: Hvad gør vi, når vi er ramt? I en sektorhændelse er I dog potentielt ikke de eneste, der er ramt. Andre er afhængige af jer, ligesom I er afhængige af andre. Jeres beslutninger påvirker andres muligheder – og omvendt.

1. Har I vurderet, hvornår en operationel hændelse i jeres organisation kan påvirke andre aktører, og omvendt, hvornår en hændelse hos andre kan påvirke jer?

2. Har I overvejet, hvordan jeres egne krisetiltag, f.eks. nedlukning af adgang, prioritering af bestemte kunder og begrænsning af ydelser, påvirker andre aktørers mulighed for at videreføre og genetablere deres forretning? Og har I overvejet, at andre aktørers tilsvarende krisetiltag kan påvirke jer på samme måde?

3. Har I en aftale om prioritering, hvis I er afhængige af en leverandør, som også betjener mange andre i sektoren? Og har I overvejet, at resten af sektoren sandsynligvis har samme behov?

Bilag 2: Metode for stresstest af operationel robusthed på sektorniveau

Indledning

Dette bilag beskriver den metode, som blev brugt til at gennemføre stresstest af operationel robusthed på sektorniveau i den danske finansielle sektor. Metoden er udviklet med inspiration fra internationale erfaringer, bl.a. fra Bank of England og ECB, og er tilpasset danske forhold. Fremgangsmåden kan bruges som inspiration i andre sektorer med komplekse afhængigheder og samfundskritiske funktioner.

Grundprincipper

- **Samarbejde:** Testen bygger på aktiv involvering af alle deltagere, både i design, gennemførelse og evaluering.
- **Realistiske scenarier:** Scenarierne er teknisk detaljerede og tilpasset sektorens faktiske risici og afhængigheder.
- **Miks af metoder:** Kombination af skrivebordsøvelser, kriseøvelser i realtid og strukturerede spørgeskemaer.
- **Læring:** Fokus på at identificere styrker, svagheder og udviklingsmuligheder, ikke på at finde fejl.

Overordnet proces

1. Forberedelse og design

- **Initiale møder:** Indledende dialog med nøgleaktører for at identificere relevante risici og mulige scenarier
- **Arbejdende grupper:** Oprettelse af tekniske og forretningsmæssige arbejdsgrupper med deltagere fra alle relevante virksomheder
- **Scenarieudvikling:** Samarbejde om at prioritere og raffinere scenarier baseret på sektorens risikobillede
- **Evt. datasæt:** Udvikling af datasæt til simulering af tekniske hændelser (f.eks. datakorrumpering).

2. Teststruktur og faser

Selve stresstesten blev gennemført i tre faser:

Fase 1: Forberedelse og scenarieopbygning

- Skrivebordsøvelser: Individuel forberedelse og opbygning af scenariet
- Distribution af testmateriale og konsultation internt i deltagende organisationer.

Fase 2: Krisehåndtering og samarbejde

- Live-elementer: Fokus på kritiske tidspunkter, hvor tværgående samarbejde er nødvendigt.

- Sektorens kriseberedskab: Sektorens fælles kriseberedskab (FSOR Kriseberedskab) anvendes til kommunikation, rapportering og test-injektioner.
- Løbende kontakt: Deltagerne skal koordinere mellem live-sessioner og lokale krisestyrings-setup.

Fase 3: Recovery og genåbning

- Skrivebordsøvelser: Refleksion og dokumentation af recovery-processen
- Live recovery-workshop: Koordination af genopretning og genåbning af kritiske funktioner
- Evaluering: Workshop om erfaringer og læringspunkter.

3. Metodeelementer

A. Skrivebordselementer

- Semistrukturerede spørgeskemaer til dokumentation af beslutninger, processer og konse-kvenser
- Datasæt-øvelser som forberedelse til live-elementer.
- Individuelle og kollektive refleksioner.

B. Live-elementer

- Scenariestyring i realtid (online og fysisk)
- Fokus på samarbejde, kommunikation, koordinering og beslutningstagning under pres
- Test af både lokale og fælles beredskabsplaner.

C. Interaktiv scenariejustering

- Løbende tilpasning af scenariet baseret på deltagernes input og reaktioner
- Opdatering af tidslinje og progression for at sikre relevans og realisme.

4. Ressourceallokering

- Involvering af forretnings-, IT-, juridiske og kommunikationsfunktioner for et helhedsoriente-ret perspektiv
- Dedikerede ressourcer til både interne og sektorbaserede krisestyringsaktiviteter
- Særligt fokus på dataanalyse, forretningsvidereførelse, recovery og vurdering af konsekven-ser.

5. Impact assessment og second-order effects

- Beskrivelse og, hvor muligt, kvantificering af konsekvenser fra hændelsens start til genopret-ning af normal drift
- Vurdering af både direkte og indirekte (second-order) effekter, f.eks. på kunder, modparter og sektoren som helhed
- Strukturering af spørgeskemaer med fokus på antagelser, usikkerheder og professionel vur-dering.

6. Evaluering og læring

- Individuelle rapporter med læringspunkter til deltagende virksomheder
- Fælles evaluering og workshops for at dele erfaringer og identificere sektorinitiativer
- Opfølgning på sektorens læring i relevante fora.

Fremgangsmåde: Sådan kan en stresstest på sektorniveau forløbe

1. **Identificér relevante aktører og risici**
    1. Indled dialog med nøgleaktører.
    2. Kortlæg kritiske afhængigheder og mulige scenarier.
2. **Etabler samarbejdsstruktur**
    3. Opret tekniske og forretningsmæssige arbejdsgrupper.
    4. Planlæg designworkshops og konsultationer.
3. **Udvikl og tilpas scenarier**
    5. Prioritér og raffinér scenarier i samarbejde med deltagerne.
    6. Udarbejd tekniske datasæt til simulering.
4. **Planlæg testens faser**
    7. Forbered skrivebordsøvelser og live-elementer.
    8. Fordel ressourcer og roller internt og på sektorniveau.
5. **Gennemfør testen**
    9. Start med skrivebordsøvelser og individuel forberedelse.
    10. Afhold live-elementer med fokus på samarbejde og beslutningstagning.
    11. Justér scenariet løbende baseret på deltagernes input.
6. **Dokumentér og vurder konsekvenser**
    12. Brug spørgeskemaer til at indsamle data om beslutninger, processer og effekter.
    13. Vurder både direkte og indirekte konsekvenser, f.eks. muligheden for at videreføre det mest kritiske.
7. **Afhold recovery-workshop og evaluering**
    14. Koordiner genopretning og genåbning af kritiske funktioner.
    15. Del erfaringer og læringspunkter i fælles workshops.
8. **Følg op på læring og initiativer**
    16. Udarbejd individuelle og sektorbaserede rapporter.
    17. Identificér og igangsæt relevante initiativer for at styrke robustheden.