FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

DNB Bank ASA
Ved styret
Postboks 1600 Sentrum
0021 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
24/4612			19.09.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i DNB Bank ASA (DNB eller foretaket) 22. mai 2024 etter å ha varslet om tilsynet 15. april 2024. Nedenfor følger Finanstilsynets tilsynsrapport.

Hensikten med tilsynet var å vurdere DNB Bank ASAs Personmarkedsområdets (PM) gjennomføring av virksomhetsanalyse ved avbrudd (BIA), vurdere PMs kontinuitetsplanlegging, inkludert vurdering av selve kontinuitetsplanen (BCP). Videre å kontrollere om PMs etablerte IKT-løsninger for kontinuitet ivaretar kravene som er satt i BIA, vurdere PMs respons- og gjenopprettingsplaner, vurdere testingen av beredskap og kontinuitet, inkludert involvering av IKT-tjenesteleverandører, samt vurdere PMs kommunikasjons- og eskaleringsplaner i forbindelse med kriser.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 14. juni 2024 og styrets kommentarer til rapporten i brev av 28. august 2024.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Overordnet risikostyring

CRR/CRD IV-forskriften § 35 stiller krav om at styret skal godkjenne og regelmessig vurdere retningslinjer for risikoer foretaket påtar seg og for å identifisere, styre, overvåke og kontrollere risikoene. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finansforetaksloven § 13-5 stiller krav til forsvarlig virksomhet og god forretningsskikk. Foretaket skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke, og rapportere risiko foretaket er eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd.

Finanstilsynet pekte i foreløpig rapport på at med bakgrunn i kapabilitetenes[1] sentrale plass i organiseringen av forretningsprosesser er det viktig at kontrollfunksjonene i andrelinje gjennomfører kontroller av om kapabilitetseier utfører sine oppgaver i samsvar med kravene som

[1] En kapabilitet er en samling av kritiske komponenter slik som prosesser, avtaler, organisasjon, IT-systemer, produkter, data med videre som kan knyttes opp til en felles enhet.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Stig Ulstein
Dir. tlf. 22 93 99 66

stilles til kapabilitetseiere. Videre ble det pekt på viktigheten av at det gjennomføres kontroller på kvalitet og innhold i rapporteringen til kapabilitetseier.

Styret skriver i sitt svar at andrelinjefunksjonene jobber etter en risikobasert tilnærming og gjennomfører uavhengige kontroller etter en dokumentert vurderings- og beslutningsprosess. Videre skriver styret at andrelinje vil inkludere en kontroll knyttet til kapabilitetseiers oppfølging av eget ansvar.

Finanstilsynet tar styrets svar til orientering.

Rapportering av IKT-risiko

Etter finansforetaksloven § 8-6 fjerde ledd skal styret føre tilsyn med den daglige ledelse og foretakets virksomhet for øvrig, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. Styrets rolle knyttet til foretakets system for risikostyring og internkontroll er utdypet i CRR/CRD IV-forskriften § 35. Der presiseres det blant annet at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Finanstilsynets pekte i foreløpig rapport på at når DNB har organisert sine forretningsprosesser med tilhørende infrastruktur inn i kapabiliteter vil det være viktig at kapabilitetseier mottar rapportering basert på kravene stilt i den enkelte virksomhetsmessige konsekvensanalyse (BIA).

Styrets skriver i sitt svar at DNB vil forsterke prosessene som gir kapabilitetseier oversikt over underliggende BIA i kapabilitetens verdikjede slik at kapabilitetseier får nødvendig rapportering og kan følge opp at kravene er forstått og gjenspeilet gjennom verdikjeden.

Finanstilsynet tar styrets svar til orientering.

Finanstilsynet pekte i foreløpig rapport på at det legges til grunn at DNB etablerer rapportering til ledelse og styre som viser omfang og resultat av beredskapstesting, og at styret mottar tilstrekkelig informasjon for å kunne vurdere om DNB ville klart å reetablere kritiske tjenester ved et verstefallsscenario.

Styret skriver i sitt svar at det i dag gjennomføres rapportering til ledelsen og styret på forretningskontinuitet fra Group Security i årlig status på sikkerhetsområdet som inkluderer beredskapstesting, og at det rapporteres risiko og etterlevelse på området via konsernets øvrige linjerapportering. Styret skriver videre at foretaket i tillegg vil styrke den faste rapporteringen til konsernledelse og styre med mer informasjon om status på forretningskontinuitet og resultat fra beredskapstestene.

Finanstilsynet tar styrets svar til orientering.

Kriseberedskap

I IKT-forskriften § 11 framgår kravene om at foretaket skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Minst årlig skal det gjennomføres opplæring, øvelse og testing av at kriseløsningen fungerer som forutsatt, der

resultat av testen skal dokumenteres. Videre gir EBAs retningslinjer for IKT og sikkerhet[2] anbefalinger om utarbeidelse av kontinuitetsplaner, respons- og gjenopprettingsplaner, testing og kommunikasjonsplaner ved kriser.

Finanstilsynet pekte i foreløpig rapport på at det for noen produktområder ikke er etablert forretningskontinuitetsplaner som er basert på gjennomførte BIA. Finanstilsynet vurderer områdene som viktige og kritiske og mener det derfor er viktig at forretningskontinuitetsplaner for disse områdene blir etablert basert på BIA.

Styrets skriver i sitt svar at foretaket vil etablere forretningskontinuitetsplaner for produktområdene det ble pekt på, og at disse utarbeides i tråd med konsernets rammeverk for forretningskontinuitet.

Finanstilsynet tar styrets svar til orientering.

Finanstilsynets pekte i foreløpig rapport på at kravene som stilles i BIA må kunne ivaretas uavhengig av teknologi og at dersom backup-strategier ikke kan etableres i tråd med kravene i BIA må dette rapporteres inn som risiko og behandles ut ifra kritikalitet.

Styret skriver i sitt svar at kravene som stilles i BIA skal være teknologiuavhengig. Styret skriver videre at foretaket gjennomfører utstrakt beredskapstesting, samt tiltak for å sikre motstandskraft i foretakets løsninger.

Finanstilsynet tar styrets svar til orientering.

Finanstilsynets pekte i foreløpig rapport på at utvelgelsen av forretningsområder og infrastruktur for beredskapstesting bør være basert på kritikalitet og risiko som framgår av BIA. Videre pekte Finanstilsynet på at innholdet i den enkelte evalueringen i BIA er en viktig kilde for utvelgelse av testobjekt for beredskapstesting.

Styret skriver i sitt svar at foretaket deler Finanstilsynets vurderingen om at utvelgelse av forretningsfunksjoner fremover må være basert på kritikalitet og risiko som framgår i BIA. Videre skriver styret at det som en del av foretakets kontinuerlige forbedringsarbeid er gjennomført BIA for alle kritiske og viktige kapabiliteter og forretningsfunksjoner. Disse analysene vil fremover legge grunnlaget for foretakets beredskapsplanlegging, og være kilden i utvelgelse av testobjekter.

Finanstilsynet tar styrets svar til orientering.

Finanstilsynet pekte i foreløpig rapport på at testingen av beredskapsplaner, for foretakets egne og utkontrakterte IKT-tjenester, må inkludere relevante informasjonssikkerhetsscenarioer med verstfallscenarioer, der planverk for gjenoppretting og alternativ drift blir testet. Dette for å sikre at interne instrukser og planer er velfungerende også i scenarioer med langvarig utilgjengelighet av IKT-tjenester.

[2] https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-outsourcing

Styret skriver i sitt svar at foretaket deler Finanstilsynets vurdering og vil i tillegg til den helhetlige beredskapstesting av IKT-tjenestene sørge for at beredskapstestene har flere scenarioer som dekker godt både tilgjengelighet, konfidensialitet og integritet i en kontinuitetssituasjon.

Finanstilsynet tar styrets svar til orientering.

Utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av samme paragraf at avtaler om utkontraktering av IKT-virksomhet og endring av slike avtaler skal behandles av styret. Videre skal styret presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransene.

Finanstilsynets pekte i foreløpig rapport på at for utkontrakterte tjenester må foretaket sikre at kravene for valg av testobjekt for beredskapstester kommuniseres til den enkelte IKT-tjenesteleverandør, inkludert relevante scenarioer, og at tjenesteleverandørs utførelse og rapportering følges opp iht. foretakets tredjepartsoppfølging og virksomhetsstyringsmodell.

Styrets skriver i sitt svar at foretaket vurderer kravstilling til, og oppfølging av, IKT-tjenesteleverandører i forbindelse med beredskapstesting som viktig, og at foretaket vil ytterligere tydeliggjøre dagens krav til og oppfølging av IKT-tjenesteleverandører.

Finanstilsynet tar styrets svar til orientering.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.