FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

DNB Bank ASA
v/Styret
Postboks 1600 Sentrum
0021 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
22/9323			15.02.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i DNB Bank ASA (DNB) 29. og 30. november 2022.

Hensikten med tilsynet var å vurdere styring og kontroll av IT-sikkerheten i DNB, og tilsynet var en oppfølging av tilsyn med samme tema i perioden 2017 – 2019. I tilsynet ble utvalgte prosesser på IT-sikkerhetsområdet for et valgt forretningsområde gjennomgått, for å se på hvordan disse ble håndtert i første- og andrelinjen.

Det valgte forretningsområde var Corporate Banking (CB), og de valgte prosessene var NIST[1]-prosessene "Data Security" (Protect/Beskytte) og "Security Continuous Monitoring" (Detect/Oppdage) som begge inngår i NIST Cyber Security Framework[2]. Med bakgrunn i at forretningsområdet CBs styring og kontroll med IKT-sikkerhet i stor grad er basert på felles infrastruktur og rammeverk som gjelder for andre forretningsområder og datterforetak i DNB, vil vurderingene også kunne ha gyldighet for andre av DNBs forretningsområder og datterselskap.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport av 30. juni 2023 og styrets svar av 19. oktober 2023.

Finanstilsynets merknader etter det stedlige tilsynet framgår nedenfor.

1. Styring og organisering av IKT-virksomheten

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre framgår det av § 8-11 tredje ledd at daglig leder blant annet skal sikre at

[1] **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) at the U.S. Department of Commerce
[2] NIST Cyber Security Framework: https://www.nist.gov/cyberframework

FINANSTILSYNET			
Revierstredet 3			**Saksbehandler**
Postboks 1187 Sentrum		post@finanstilsynet.no	Jarleif Lødøen
0107 Oslo	Telefon 22 93 98 00	www.finanstilsynet.no	Dir. tlf. 22 93 98 00

det finnes forsvarlige styrings- og kontrollsystemer. Kravene til forsvarlig virksomhet er nærmere regulert i § 13-5. Det følger også av § 8-11 tredje ledd at daglig leder er ansvarlig for at det er etablert instrukser for de ansattes arbeidsoppgaver og ansvarsforhold, samt rapporterings- og saksbehandlingsregler. Ifølge IKT-forskriften § 2 skal foretaket utarbeide beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte. Ytterligere utdypninger finnes i den europeiske banktilsynsmyndighetens (EBA)[3] "EBAs retningslinjer for IKT og sikkerhet"[4] punkt 3.2.1.

Dokumentstrukturen som underbygger virksomhetsstyringen i DNB, var på tidspunktet for tilsynet nylig redusert fra fem til fire nivåer. I foreløpig rapport pekte Finanstilsynet på at flere av de mottatte instruksene manglet referanse til overliggende policy og underliggende instrukser, og at enkelte instrukser refererte til nivået som var fjernet.

Fra styrets svar har Finanstilsynet notert seg at samtlige konserninstrukser vil ha referanse til en konsernpolicy som overliggende dokument, og at alle konsernpolicyer vil ha referanse til relevante underliggende konserninstrukser. Metainformasjon om eierskap, forankring og gyldighet blir påsatt styrende dokumenter ved uttrekk til fil eller utskrift. Revisjon av alle konserninstrukser har sikret at innholdet i dem er i tråd med nytt styringshierarki.

Finanstilsynet tar styrets informasjon til etterretning.

2. Validering av IKT-sikkerhetskontroller

IKT-forskriften § 5 stiller krav til at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare. Ytterligere utdypinger om styring og kontroll med IKT-risiko framgår av EBAs retningslinjer for IKT og sikkerhet, punkt 3.2.1.

DNB sitt nye rammeverk for sikkerhetsstyring, Security Governance Framework (SGF), er basert på NIST. Selve sikkerhetskravene er ikke nye for DNB, men er koblet til en ny formell kontekst ved innføringen av SGF. I henhold til foretakets IT Operating Model har rollen IT-ansvarlig et ende-til-ende-ansvar for en IT-komponent uavhengig av om denne er egenutviklet, kjøpt eller om dette utgjør leveranse av IKT-tjenester som er utkontraktert.

2.1. Kvaliteten på de IT-ansvarliges attestasjon

Finanstilsynet pekte i foreløpig rapport på at det nye sikkerhetsrammeverket i stor grad baseres på attestasjoner fra IT-ansvarlige og at det hviler et stort ansvar på dem. Modellen baserer seg på at kvaliteten på de IT-ansvarliges attestasjoner er tilfredsstillende, inkludert at den IT-ansvarlige har den nødvendige IT-kompetansen for å ta stilling til kontrollen. I foreløpig rapport var det derfor Finanstilsynets forventning at det til hvert kontrollmål knyttes kontrollspørsmål/sjekklister med krav til dokumentasjon av vurderingene, slik at attestasjonene baseres på de samme

[3] European Banking Authority (EBA)
[4] EBA GL on ICT - EBA/GL/2019/04: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

vurderingskriteriene, og at det i ettertid kan verifiseres at attestasjonen av kontrollmålet er oppfylt. Finanstilsynet stilte videre spørsmål om hvilken frekvens det er på attestasjonene, og hvilke rutiner som gjelder dersom det gjøres endringer i, eller i tilknytning til, den aktuelle IT-komponenten som skal attesteres.

Finanstilsynet har notert seg styrets svar, og understreker ansvaret styret har for å sikre at kvaliteten på de IT-ansvarliges attestasjoner er tilfredsstillende, inkludert at de IT-ansvarlige som foretar attesteringen har den nødvendige IT-kompetansen for å kunne ta stilling til kontrollen. Styret må videre sikre at de IT-ansvarliges attestasjoner baseres på de samme vurderingskriteriene, eksempelvis ved bruk av kontrollspørsmål/sjekklister. For å kunne etterprøve valideringen av kontrollmålene, må de IT-ansvarlige dokumentere sine vurderinger.

2.2. IT-ansvarliges attestasjon ved utkontraktering av IKT-tjenester

Den IT-ansvarlige skal også attestere for kontrollmål der en eller flere tredjepartsleverandører er knyttet til utvikling, forvaltning eller drift av den aktuelle IT-komponenten. I foreløpig rapport var Finanstilsynets forventning at det er samme krav til dokumentasjon for å verifisere attestasjoner, uavhengig av om IT-komponenten er utkontraktert eller ikke, noe som innebærer at det ved utkontraktering må innhentes dokumentasjon fra tredjepartsleverandøren. Som et eksempel på krav til dokumentasjon nevnte Finanstilsynet at det skal finnes dokumenterte rutiner for tilgangsstyring av utkontraktert IKT-virksomhet der det framgår hva som skal kontrolleres, hvem som er ansvarlig for kontrollen, frekvensen for den enkelte kontrollen og resultatet av kontrollen.

Finanstilsynet har notert seg styrets svar, og understreker ansvaret styret har for å sikre at det er fastsatt klare krav til hva som skal kontrolleres, hvilken dokumentasjon som skal innhentes, hvilken IT-ansvarlig som er ansvarlig for kontrollere når flere komponenter har IKT-tjenesteleveranser fra samme IKT-leverandør, frekvensen for de ulike kontrollene og hvordan vurderingen må dokumenteres for å kunne etterprøve valideringen av kontrollmålene.

2.3. Andrelinjens oppfølging av IT-ansvarliges attestasjoner

Finanstilsynet viste i foreløpig rapport til at det gjennom tilsynet framsto som at andrelinjen først og fremst målte gjennomføringsgrad og framdrift på bekreftelsene av kontrollmålene. Finanstilsynet kunne ikke se at kvaliteten på attestasjonene hadde blitt vurdert. Finanstilsynet etterspurte også om det gjøres kontroller for å sikre at samtlige aktuelle IT-komponenter er omfattet av sikkerhetsrammeverket.

Finanstilsynet har fra styrets svar merket seg at andrelinjen ikke gjennomfører fullstendige og systematiske gjennomganger og kontroller av de IT-ansvarliges attestasjoner, men gjør kontroll av utvalgte områder med utgangspunkt i risikovurderinger. Av styrets svar framgår det at etterlevelsesfunksjonen etter tilsynet har gjennomført noen kontroller som inkluderer kontroll av grunnlaget for IT attestasjonene. Videre at risikostyringsfunksjonen har planlagt kontroller for andre halvår 2023 som inkluderer deler av attestasjonene.

Finanstilsynet tar styrets informasjon til etterretning, men understreker styrets ansvar for å sikre at andrelinjen følger opp det nye sikkerhetsrammverket med tilstrekkelige kontroller for å sikre at det ivaretar kvaliteten av kontrollene på en tilfredsstillende måte, inkludert IT-attestasjonene.

3. IKT-sikkerhetsovervåking

IKT-forskriften § 5 stiller krav til at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Ytterligere utdypinger om styring og kontroll med IKT-sikkerhetsrisiko framgår av EBAs retningslinjer for IKT og sikkerhet, der punkt 3.2.3 omfatter tredjeparts utkontraktering, og punkt 3.4.5 omfatter sikkerhetsovervåkning.

I foreløpig rapport stilte Finanstilsynet spørsmål til hvordan det sikres at overvåkingen på systemnivå er dekkende, spesielt for de systemene CB selv har eierskap til. Videre stilte Finanstilsynet spørsmål til hvilke krav og vurderinger CB legger til grunn for å sikre tilstrekkelig logging på system- og nettverksnivå, adekvat oppfølging av loggene og hvordan kravene til loggfunksjonalitet ivaretas i prosessen for endringshåndtering samt hvordan dette følges opp ved utkontraktering. Finanstilsynet stilte også spørsmål til om CB hadde en totaloversikt for systemene de har eierskap til, der det framkommer om sikkerhetsovervåkingen er optimalisert, har identifiserte mangler eller avventer vurdering.

Finanstilsynet har merket seg styrets redegjørelse for sikkerhetsovervåkingen, inkludert hvordan overvåkingen er implementert for CB sine applikasjoner. Finanstilsynet tar styrets informasjon til etterretning.

4. Beredskap og kontinuitet

IKT-forskriften § 11 stiller krav til at foretaket skal ha en dokumentert kriseplan, slik at forretningsmessig kontinuitet kan opprettholdes. Kriseplanen skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Minimumskravene til en slik kriseplan framgår av IKT-forskriften § 11 annet ledd. IKT-forskriften §11 tredje ledd stiller krav til at det skal gjennomføres opplæring, øvelse og testing av at kriseløsningen fungerer som forutsatt. Resultatet av testen skal dokumenteres.

Videre framgår det av EBAs retningslinjer for IKT og sikkerhet, punkt 3.7, at hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i foretakets analyse av konsekvensene ved avbrudd for de kritiske forretningsprosessene som identifiseres. Det framgår også at for å verifisere at det er etablert fungerende planer og løsninger må det foretas regelmessig opplæring, øvelse og testing.

4.1. Tilstrekkelig kapasitet for tilgang til data

Finanstilsynet viste i foreløpig rapport til at infrastruktur i liten grad er forbeholdt CB alene, da CB i stor grad benytter felles plattformer og felles arkitektur i DNB. Finanstilsynet kunne ikke se at vurderinger av kapasitet for å sikre tilgjengelighet til data, inngikk i CBs årlige analyse av konsekvensene ved avbrudd, eller om slike vurderinger inngikk i arbeidet med beredskap og kontinuitet i CB, og eventuelt hvilke tiltak CB hadde iverksatt.

Fra styrets svar framgår det at CB i den årlige analysen av konsekvensene ved avbrudd vurderer produkter og tjenester ut fra et kritikalitetsperspektiv med et særlig fokus på tilgjengelighet til forretningsprosesser. I denne vurderingen inngår tilgjengelighet til data, der CB fastsetter kravene til tilgjengelighet for de kritiske komponentene som understøtter de viktigste prosessene. Basert på

disse analysene vil IT-teamene med ansvar for applikasjonene sikre at CB har tilstrekkelige tekniske løsninger for å ivareta tilgjengelighetskravene

Finanstilsynet tar styrets informasjon til etterretning.

4.2. Kvalitet på Configuration Management Database (CMDB)

Finanstilsynet viste i foreløpig rapport til sin forståelse av at korrekt registrering i CMDB er avgjørende for styringen av forretningsmessig kontinuitet og beredskap. Finanstilsynet pekte på at CB må sikre at samtlige sentrale og kritiske forretningsprosesser vurderes, og at alle avhengigheter blir kartlagt. Finanstilsynet stilte spørsmål ved om CB har tilstrekkelig kontroll med om systemer/tjenester registreres i CMDB på det detaljeringsnivået som er nødvendig for å ha tilstrekkelig kontroll i arbeidet med beredskap og kontinuitet.

Av styrets svar har Finanstilsynet notert seg at målrettet arbeid de senere årene har gitt betydelig forbedring i kvaliteten på data i CMDB. Når applikasjoner registreres i CMDB, kreves det blant annet utfylling av informasjon om forretningskritikalitet, rolleinnehavere (forretningseier/IT-ansvarlig), arkitektur-egenskaper, hvilken type data applikasjonen prosesserer og detaljer om tekniske relasjoner. DNB vil gjennom arbeidet med fornyelse av forretningskontinuitet ha ytterligere fokus på å sikre at innholdet i CMDB i enda større grad knyttes direkte mot verdikjeder og forretningsprosesser for å videre styrke arbeidet med kontinuitet og beredskap.

Finanstilsynet tar styrets informasjon til etterretning.

4.3. Beredskapstesting av ikke-kritiske applikasjoner

I foreløpig rapport viste Finanstilsynet til at det var gjort kjent med hvordan DNB gjennomfører disaster recovery-testing av kritiske tjenester, men at det ikke var kjent med hvordan beredskapstesting av ikke -kritiske tjenester foregår. Finanstilsynet pekte på at det var uklart hvilke konsekvenser de ikke-kritiske tjenestene kan utgjøre for DNBs forretningsmessige kontinuitet og etterspurte foretakets vurdering av i hvilken grad testing av ikke-kritiske tjenester burde gjennomføres.

Av styrets svar framgår det at det ved klassifisering av kritikaliteten til applikasjonene gjøres det en vurdering av hvor viktig tilgjengeligheten er for forretningsprosessene de understøtter, basert på potensielt økonomisk tap, etterlevelsesrisiko, omdømmetap, tap av kundetilfredshet og produktivitetstap. Dersom en applikasjon blir kategorisert som ‘ikke-kritisk’, vil den ha en begrenset innvirkning på forretningsmessig kontinuitet, og det konserninterne kravet om disaster recovery-testing av konsernkritiske tjenester vil være tilstrekkelig for å sikre forretningsmessig kontinuitet. Videre har Finanstilsynet fra styrets svar merket seg at det er opp til CB å sørge for at tjenestene basert på systemer som ikke er definert som kritiske, leveres med den oppetid og redundans som er vurdert hensiktsmessig.

For Finanstilsynet framstår det som lite sannsynlig at ikke-kritiske systemer har ensartet kritikalitet. Finanstilsynet understreker styrets ansvar for å sikre at det gjennomføres tilstrekkelig beredskapstesting av systemene som kategoriseres som ikke-kritiske.

4.4. Kundenes behov når tilgjengelighetskrav skal fastsettes

Finanstilsynet stilte i foreløpig rapport spørsmål ved hvordan CB kartlegger behovene til kundene når tilgjengelighetskrav skal fastsettes, gitt at en del av CB i sine løsninger er prisgitt de tilgjengelighetskrav som er fastsatt av andre internt i DNB, eksempelvis betalingsløsningene.

Fra styrets svar har Finanstilsynet merket seg at CB gjennomfører forretningsmessig konsekvensanalyser på produkter og tjenester med en konsekvensvurdering av hvilken innvirkning bortfall vil ha både for DNB og kundene. For verdikjeder som strekker seg over flere forretningsområder, så blir området med høyest kritikalitet hensyntatt ved fastsettelse av tilgjengelighetskrav.

Finanstilsynet tar styrets informasjon til etterretning.

***

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet. Kopi av tilsynsrapporten bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen

Seksjonssjef

Jarleif Lødøen

Tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.