FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

DNB Bank ASA
Postboks 1600 Sentrum
0021 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
21/2820			25.09.2022

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i DNB Bank ASA (Banken) 25. og 27. mai 2021. I tillegg gjennomførte Finanstilsynet oppfølgingssamtaler med ansatte i ulike avdelinger og i norske datterselskaper i perioden 30. juni til 20. august 2021. Tilsynet ble gjennomført digitalt.

Tilsynet hadde som formål å vurdere hvordan styring og kontroll med IKT-området blir ivaretatt, med et særskilt fokus på hvordan DNB ivaretar helhetlig planlegging og koordinering av aktiviteter innen IKT-området for konsernet.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige tilsynsrapport datert 25. januar 2022 og styrets kommentarer til foreløpig tilsynsrapport i brev av 6. april 2022.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

1. Styring og kontroll med IKT

IKT-forskriften § 2 Planlegging og organisering har bestemmelser om foretakets organisering og ansvarsforhold for IKT-virksomheten. "EBA Guidelines on ICT and security risk management" (EBA GL on ICT), "3.2 Governance and strategy", og "EBA Guidelines on internal governance" (EBA GL on Governance) utdyper IKT-forskriftens bestemmelser.

1.1. IKT-Styringsmodell

Finanstilsynet har vurdert hvordan DNB styrer og kontrollerer IKT-området, og undersøkt hvordan dette er implementert i forretningsområder (FO) og stabsområder (SO) og datterselskaper.

1.1.1. Oppfølging av nytt rammeverk for IT-leveransemodell, samt styring og kontroll med IT

I foreløpig rapport viste Finanstilsynet til at IKT-området de to siste årene har gjennomgått omfattende endringer med blant annet ny IT-strategi, ny leveransemodell for IT-tjenester (IT operating model - ITOM), omorganisering og innføring av ny styringsmodell for IT-området (IT Governance). Basert på omfanget av endringene var det Finanstilsynets vurdering at IKT-risikobildet endret seg i de ulike FO/SO og datterselskaper, samt i samhandlingen mellom disse, der konsekvensene av endret risiko var til dels ukjente og utilsiktede. Det var videre Finanstilsynet forståelse fra andre- og tredjelinjens rapportering at Banken ikke hadde fullført oppgradering av

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Jarleif Lødøen
Dir. tlf 22 93 98 00

dokumentasjonen ifm. ny IT-leveransemodell og operasjonalisering av ny styringsmodell for IT-området. Det innebærer etter Finanstilsynets vurdering økt risiko i overgangen fra et sett styrende dokumenter til et annet, der ansvarslinjer og roller for å sikre oppfølging og implementering ikke var fastsatt. Det var Finanstilsynets anbefaling at Banken bør ha særskilt oppmerksomhet og oppfølging av IKT-risikoene knyttet til endringene inntil ny styringsmodell er fullt ut implementert, roller og ansvar er avklart på nye samhandlingsarenaer og at styringsmodellen har fått virket noe tid i konsernet.

Av styrets svar framgår det at DNB etter tilsynsmøtet har vedtatt å tydeliggjøre forskjellen mellom styringsmodell for IT-området og leveransemodell for IT-tjenester. DNBs styringsmodell for IT-området er definert med en IT-standard, 10 instrukser og 26 IT-prosesser. Det er disse styrende dokumentene som utgjør grunnlaget for styring og kontroll med IT i DNB. Styret peker på at de overordnede prinsippene i den nye leveransemodellen for IT-tjenester er innarbeidet i styringsmodellen for IT-området og at disse prinsippene gjelder for hele konsernet. Dokumentasjonen av leveransemodellen for IT-tjenester inneholder i tillegg retningslinjer for blant annet organisering av IT-team med beskrivelser av anbefalte roller, ansvar og praksiser. Det framgår videre av styrets svar at deler av styringsmodellen for IT-området fortsatt er under implementering, og at den nye leveransemodellen for IT-tjenester i økende grad blir adoptert utenfor den sentrale IT-enheten, Technology & Services (heretter omtalt som T&S). Finanstilsynet har også merket seg fra styrets svar at de vurderer IT-risikoen i konsernet som redusert etter at ny styringsmodell for IT-området og ny leveransemodell for IT-tjenester ble innført.

Det er Finanstilsynets vurdering at det er nødvendig med særskilt oppfølging av IKT-risiko inntil ny styringsmodell er fullt ut implementert, roller og ansvar er avklart på nye samhandlingsarenaer og at styringsmodellen har fått virket noe tid i konsernet.

1.1.2. Prioritering

I foreløpig rapport påpekte Finanstilsynet at DNB synes å ha de samme utfordringene, som tidligere påpekt i forbindelse med SREP, når det gjelder å balansere bruken av IKT-ressurser mellom krav til ny funksjonalitet, systemvedlikehold, teknisk gjeld og nødvendige endringer for etterlevelse av regulatoriske krav. Finanstilsynet viste videre til Konsernrevisjonens (tredjelinjen) påpekning om at det er forretningsområder (FO) som ikke benytter fastsatt prosess for behovsstyring (demand management) fullt ut, samt at behovene for IKT-ressurser for utviklingsaktiviteter i tverrgående/horisontale forretningsprosesser, for de tjenester/applikasjoner som går på tvers av IT-teamene, overstiger kapasiteten. Begge disse forholdene har etter Finanstilsynets vurdering betydning for foretakets oversikt over tilgjengelige ressurser for planlegging og prioritering, noe som vil kunne ha konsekvenser for DNBs virksomhet.

Fra styrets svar registrerer Finanstilsynet at Bankens nye prosess for behovsstyring er ment å ivareta prioritering av IKT-utviklingen i forhold til modernisering, etterlevelse, og eventuell ny forretningsutvikling, da Banken styrer bruken av IKT-ressurser basert på tilgjengelig kapasitet uten finansielle rammer for fordelingen mellom utvikling, drift og forvaltning. Ved at IT-teamene har et definert ende-til-ende ansvar for å sikre funksjonalitet i tjenestene, etterlevelse av regulatoriske krav og andre utviklingsbehov for samtlige applikasjoner og/eller infrastruktur som IT-teamet er ansvarlig for, så vil riktig prioritering bli satt utfra tilgjengelig kapasitet.

Finanstilsynet tar foretakets opplysning til etterretning.

2. Styring og kontroll med IKT-risiko

IKT-forskriften § 3 Risikoanalyse stiller krav om at Banken skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemer, og det skal etableres en dokumentert prosess for gjennomføring av risikoanalyser av IT-virksomheten. Prosessen skal definere ansvarsforhold og omfatte oppfølging av tiltak som er iverksatt som følge av gjennomførte risikoanalyser. Banken plikter minimum å gjennomføre årlige risikoanalyser, eller ved endringer som har betydning for IKT-sikkerheten. Slike risikoanalyser skal gjennomføres for å påse at risiko styres innen akseptable grenser. Nærmere utdyping av forskriftens bestemmelser knyttet til håndtering av IKT-risiko framgår av "EBA GL on ICT", "3.3. ICT and security risk management framework" og "EBA GL on Governance, seksjon 19 og 22.

2.1. Oversikt over IKT-risiko

I foreløpig rapport påpekte Finanstilsynet at rapporter fra andre- og tredjelinjen antyder at det samlede IKT-risikobildet for sikkerhetsrisikoer og -kontroller i DNB ikke er enkelt tilgjengelig, da risikostyringen innen IKT forutsetter manuell sammenstilling av data fra to systemer. Finanstilsynet ba om styrets vurdering av utfordringene knyttet til rapporteringen ved bruk av de to systemene og konsekvensene dette innebar for til enhver tid ha et komplett og oppdatert risikobilde for IT-virksomheten i DNB, inkludert de ulike FO/SO og datterselskaper.

Av styrets svar framgår det at dagens to systemer ikke er til hinder for at det rapporteres et helhetlig risikobilde. Finanstilsynet merker seg fra styrets svar at styret mener en mer automatisert sammenstilling av data vil kunne bidra til en mer kontinuerlig oversikt over det totale risikobildet og en mer effektiv rapporteringsprosess.

Finanstilsynet tar foretakets opplysning til etterretning.

2.2. Førstelinjen

2.2.1. Førstelinje - Risikostyring

Et formål med tilsynet var å vurdere i hvilken grad førstelinjen har tilstrekkelig IKT-kompetanse for å identifisere relevante IKT-risikoer innen eget virkeområde. Finanstilsynet oppfatter at DNB har rendyrket de tre forsvarslinjene, der det er tydeliggjort at det er førstelinjen som eier all risiko. Videre er det Finanstilsynets forståelse at førstelinjen selv er ansvarlig for å etablere de miljøene som skal utføre nødvendige risikoanalyser, samt identifisere og teste kontroller i egne prosesser.

Finanstilsynets uttrykte i foreløpig rapport en forventning om at førstelinjen i DNBs ulike FO/SO og datterselskaper har tilstrekkelig og nødvendig IKT-kompetanse for å identifisere og vurdere konsekvensene av relevante IKT-risikoer, og ba på denne bakgrunn om styrets vurdering.

Av styrets svar framgår det at utviklingen i risikomodenhet i konsernets IT-team har vært positiv, der representanter for IT- og forretningseiere i FO/SO og datterselskaper deltar i IT-teamenes risikovurderinger. Det er styrets vurdering at disse representantene har de beste forutsetningene for å vurdere IKT-risiko, herunder både sannsynlighet for at risikoen inntreffer og konsekvens dersom risikoen inntreffer. Det framgår videre fra styrets svar at DNB driver kontinuerlig informasjons- og opplæringsvirksomhet for å sikre at det finnes tilstrekkelig kompetanse om IKT-risiko i førstelinjen.

Finanstilsynet tar styrets svar til etterretning.

2.2.2. Førstelinje – Etterlevelse

Et formål med tilsynet var å vurdere i hvilken grad førstelinjen har ansvar og oppmerksomhet knyttet til det å sikre etterlevelse av relevante regulatoriske krav innen IKT-området. I foreløpig rapport påpekte Finanstilsynet at graden av ansvar som førstelinjen påtar seg for etterlevelse synes å variere mellom de ulike FO/SO og datterselskap. Det er også uklart for Finanstilsynet i hvilken grad førstelinjen selv har et definert ansvar for å ha kontroll med, og å følge med på, endringer/utvikling i regelverk innen IKT-området for eget virkeområde. Finanstilsynet ba derfor i foreløpig rapport om styrets kommentar til rolledelingen mellom første- og andrelinje.

Av styrets svar framgår det at DNBs virksomhetsstyringsdokument "Etterlevelse Konsernpolicy" presiserer at alle ledere og ansatte har et kontinuerlig/løpende ansvar for etterlevelse av eksternt og internt regelverk innenfor sine arbeidsområder, samt at alle tre forsvarslinjer skal kontrollere og rapportere på etterlevelse. Det framgår videre av styrets svar at Group Compliance i Norge har ansvar for regelverksovervåking innen anti-hvitvasking, anti-korrupsjon og sanksjoner, mens DNB-advokatene har ansvar for regelverksovervåking og regelverkstolkning innen teknologi og informasjonssikkerhet. Videre framgår det av virksomhetsstyrings-dokumentasjonen at ansvaret for regelverksovervåking og fortolkning er presisert og fordelt. Av styrets svar framgår det også at utpekte konsernfunksjoner er ansvarlige for å avdekke og formidle informasjon om viktige regelverkshendelser til berørte forretnings- og støtteområder, samt at divisjonsdirektøren med ansvar for Risk og Quality i det enkelte FO/SO har et eksplisitt ansvar for å motta og følge opp informasjon om regelverkshendelser.

Finanstilsynet tar styrets svar til etterretning.

2.3. Kontrollfunksjonen CISO

EBAs retningslinjer "EBA GL on ICT" gir en utdyping av IKT-forskriftens bestemmelser. Videre gir retningslinjene også utdyping av Finansforetakslovens bestemmelser om forsvarlig organisering og uavhengige kontrollfunksjoner knyttet til risikostyring, etterlevelse og internrevisjon som også gjelder for Bankens IKT-virksomhet. Det følger av retningslinjenes kapittel 3.3.1 en anbefaling om å tildele ansvaret for å lede og overvåke IKT- og sikkerhetsrisiko til en uavhengig objektiv sikkerhetsfunksjon som har direkte rapportering til ledelsen, der foretaket også skal sikre at kontrollfunksjonens virksomhet utføres tilstrekkelig adskilt fra annen IKT-virksomhet.

Finanstilsynet har vurdert DNB sin organisering av sikkerhetsarbeidet i forhold til anbefalingene i retningslinjene. Finanstilsynets vurdering var at rollen Chief Information Security Officer (CISO) sin funksjon og organisasjonsmessige innplassering ikke synes å følge EBA sine retningslinjer for etablering av en uavhengig sikkerhetsfunksjon med direkte rapportering til Bankens ledelse. Finanstilsynet ba i foreløpig rapport om styrets vurdering av dette forhold.

Av styrets svar framgår det at CISO er lagt til førstelinjen, med ansvar for å lede Group Security. Det framgår også av svaret at CISO har, i henhold til DNBs konsernpolicy for sikkerhet, en egen rapportering direkte til konsernsjef og styre. Group Security er i dag en divisjon under konsernenheten Technology & Services (T&S), som ledes av Chief Information Officer (CIO). Videre framgår det av styrets svar at Group Security er premissgiver på sikkerhetsområdet, gir råd i komplekse sikkerhetsspørsmål og utøver flere konsernfelles sikkerhetsoppgaver. Styret peker også i sitt svar på at Banken har gjennomført en ny finansregulatorisk vurdering av kravene til organisering av sikkerhetsfunksjoner, der Finanstilsynet fra styrets svar har merket seg at styret mener Bankens organiseringen sikrer en objektiv og uavhengig kontroll av sikkerhetsområdet, i tråd med EBA ICT Guidelines.

Finanstilsynet tar styrets redegjørelse til etterretning.

3. Vurdering av utvalgte risikoområder

3.1. Utkontraktering av IKT-tjenester

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

3.1.1. Intern utkontraktering

Banken har ansvar for å følge opp utkontraktert virksomhet, jf. IKT-forskriftens § 12, der det framgår at styret og ledelsen må sikre at organisasjonen besitter tilstrekkelig kompetanse for å kunne vurdere utkontrakteringsforholdet. IKT-forskriftens bestemmelser om utkontraktering gjelder uavhengig av om det er konsernekstern eller -intern utkontraktering, jf. Finanstilsynets rundskriv 7/2021 om utkontraktering og om intern utkontraktering i "EBA Guidelines on outsourcing arrangements".

Finanstilsynet har vurdert hvordan intern utkontraktering blir håndtert i DNB. I foreløpig rapport var Finanstilsynets vurdering at håndteringen av konserninterne IKT-utkontrakteringsforhold i varierende grad synes å innfri nevnte krav, og at styret må påse at Banken iverksetter tiltak for å sikre etterlevelsen i Banken og de datterselskaper der Banken opptrer som oppdragstaker.

Finanstilsynet har fra styrets svar merket seg at det er igangsatt tiltak, blant annet nytt register for konserninterne avtaler, forbedret mal for avtaler, bedre systemstøtte og tettere oppfølging mot utkontrakteringsregelverket, for å sikre en bedre kontroll med konsernintern utkontraktering i tråd med kravene i IKT-forskriften.

Finanstilsynet ber om å bli orientert når arbeidet med register for konserninterne avtaler er ferdigstilt.

3.1.2. Utkontraktering av IKT-virksomhet – tredjeparts risikostyring

Banken har iverksatt en ny rutine, Third Party Risk Management (TPRM), med IT-systemstøtte for å følge opp all utkontraktering, inkludert IKT-virksomhet. Målsetningen er å sikre en helhetlig vurdering, overvåking, oppfølging og rapportering av konsernets risiko knyttet til utkontraktering.

I foreløpig rapport påpekte Finanstilsynet at rapporter fra andre- og tredjelinjen viste at IT-området lå bak planen for å fullføre en gjennomgang av all IKT-utkontraktering i løpet av 2021. Videre var det Finanstilsynets forståelse at antallet utkontrakteringsforhold som T&S var ansvarlige for var uklart, og at kriteriene for vurdering av risiko og relevante lovkrav i utkontrakteringsforhold, som var inkludert i IT-løsningen, ikke synes å være dekkende. I foreløpig rapport ba derfor Finanstilsynet om styrets vurdering av hvilke konsekvenser som forsinkelsen, det uavklarte antall utkontrakteringer og de påpekte manglene i IT-løsningen har for oversikt og håndtering av IKT-risiko.

Fra styrets svar har Finanstilsynet merket seg at styret oppfatter vurderingene som gjøres i forbindelse med TPRM-gjennomgangen som kompletterende til det øvrige arbeidet innen IT-sikkerhet, IT-risiko og IKT-utkontraktering. Det framgår videre fra styrets svar at *"Brorparten av alle tredjepartsforhold innen IT har blitt registrert og vurdert i løpet av andre halvår 2021"* og at eierskap og ansvar har blitt avklart for de utkontrakteringsforhold som er gjennomgått. Videre framgår det fra styrets svar at IT-løsningen har et økt antall kriterier som vurderes, og at det ikke er meningen at IT-løsningen skal dekke alle forhold knyttet til tredjepartsvurderinger. Det framgår også at IT-løsningen er gjenstand for kontinuerlig videreutvikling og forbedring, i tråd med både eksterne og interne krav og behov.

Finanstilsynet har fra styrets svar også merket seg at Banken i interne utkontrakteringsforhold med datterselskaper (der DNB Bank er oppdragstaker) benytter andre risikovurderingsmekanismer (GRAP – Group Risk Assessment Process) enn TPRM.

3.2. Prosjektstyring

IKT-forskriften § 2, § 6 og § 9 har bestemmelser knyttet til utvikling, anskaffelser og avviks- og endringshåndtering. Nærmere utdyping av forskriftens bestemmelser følger av kapittel 3.5 og 3.6 i "EBA GL on ICT".

I foreløpig rapport var det Finanstilsynet vurdering at DNB ville være tjent med å etablere en konsernprosess for gjennomføring av IT-prosjekter som omfatter horisontale forretningsmessige verdikjeder, der problemstillinger for prosjekter som går på tvers av Tech-familiene også ivaretas.

Finanstilsynet merker seg fra styrets svar at DNB har en prosjektstyringsmodell med strategisk porteføljestyring, der Nøkkelteam IT beslutter hvilke IT-porteføljer Banken skal ha. Det framkommer også av svaret at "det er IT-porteføljene som foretar prioritering, oppfølging og rapportering", mens det er linjen gjennom de ulike IT-teamene som gjennomfører og implementerer i tråd med prosess for behovsstyring. Prosjektlederne er hovedsakelig organisert i forretningsnær IT for å ivareta verdikjeder. Finanstilsynet merker seg også fra styrets svar at Banken har som mål om å endre IT-porteføljene til i større grad å reflektere produkt- og verdikjededimensjonen, i stedet for det enkelte FO/SO, noe som utfordrer linjeansvaret slik det er etablert i dag, og som vil kreve noe tid og modning.

3.3. IKT-tilgjengelighet og kontinuitetsledelse (inklusive drift og beredskap)

Banken har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. Nærmere utdyping av forskriftens bestemmelser finner man i "EBA GL on ICT" kapittel 3.7.

I tilsynet har Finanstilsynet vurdert IKT-tilgjengelighet og kontinuitet. Finanstilsynet tilkjennega sin forventning om at hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres på grunnlag av forretningsmessige konsekvensanalyser (BIA) for Bankens kritiske forretningsprosesser. Videre forventer Finanstilsynet at det gjennomføres regelmessig opplæring og øvelse, og at testing av løsninger og planer verifiserer at tilgjengelighet og kontinuitet innfrir kravene i analysen av de kritiske forretningsprosessene.

Fra styrets svar har Finanstilsynet merket seg at FO/SO utarbeider kontinuitetsplaner som dekker *"det fysiske, personell- og IT-messige"*, samt at det gjennomføres øvelser på operativt og strategisk nivå for ulike scenarier som kan inntreffe. Videre framgår det av svaret at det pågår arbeid med å forbedre prosesser og tydeliggjøre roller og ansvar knyttet til forretningsmessig kontinuitet. I dette

arbeidet inngår også forbedring av planer og etablering av tiltak som skal sikre forretningsmessig kontinuitet, inkludert gjenoppretting av IKT-løsninger for de mest kritiske forretningsprosessene.

Med bakgrunn i at deler av planlagt testing av beredskap og kontinuitet ikke ble gjennomført grunnet ressursmangel hos avgivende leverandør i forbindelse med leverandørbytte, påpekte Finanstilsynet i foreløpig rapport at DNB må sørge for at exit-bestemmelsene i avtalene med IKT-leverandører ivaretar dette.

Finanstilsynet tar styrets svar om at det er etablert virksomhetsstyringsinstrukser vedrørende terminering av utkontrakteringsavtaler, exit-bestemmelser, til etterretning.

3.4. Dataintegritet/styring og kontroll med data

IKT-forskriften § 4 stiller krav til at det fastsettes kvalitetsmål for de enkelte deler av IKT-virksomheten knyttet opp mot Bankens øvrige mål. Banken skal videre ha dokumenterte prosedyrer for oppfølging av fastsatte kvalitetsmål.

I tilsynet har Finanstilsynet vurdert hvordan Banken har organisert arbeidet med datakvalitet, og hvordan Banken styrer og kontrollerer data.

Det er Finanstilsynets vurdering at arbeidet med å etablere et velfungerende opplegg for styring og kontroll med data i DNB er tidkrevende, og at det er utfordrende å få tilstrekkelig oppmerksomhet og prioritet for dette arbeidet. Det er videre Finanstilsynets forståelse, fra gjennomgangen i tilsynsmøtene, at konsernets tverrgående forretningsprosesser utgjør komplekse verdikjeder av systemer, der det er utfordrende å identifisere og plassere ansvaret for datakvalitet til en dataeier.

I foreløpig rapport pekte Finanstilsynet på at risikoen for feil som følge av dårlig datakvalitet er et konsernanliggende som potensielt kan ha store negative konsekvenser. Uten en klar plassering av ansvaret for, og kvaliteten på, data var det Finanstilsynets vurdering at dette ville ha konsekvenser for hvordan dårlig datakvalitet rapporteres, følges opp og utbedres.

Finanstilsynet har fra styrets svar merket seg at styrking av arbeidet med data og datakvalitet har høy prioritet i Banken. Det er i løpet av 2021 igangsatt konsernfelles moderniseringsinitiativer der bedret datakvalitet er vektlagt. Videre har konsernledelsen i Banken valgt databehandling som et av områdene med særskilt oppmerksomhet i internkontrollattestasjonen for 2022. Finanstilsynet merker seg videre fra styrets svar at Banken i 2021 har formalisert en konsernstandard for data og et rammeverk for styring og kontroll med data (data governance), og med dette tatt viktige steg for etablering av en styringsmodell for data, dataeierskap og datakvalitet. Videre merker Finanstilsynet seg at DNB i andre halvår 2021 igangsatte et arbeid i den sentrale dataorganisasjonen med sikte på å tydeliggjøre ansvar for datakvalitet i verdikjedene. Av styrets svar framgår det også at Banken i 2022 har etablert en tverrfaglig arbeidsgruppe som jevnlig rapporterer status og framdrift til styrende organer. Finanstilsynet merker seg også fra svaret at Banken har sett et behov for å øke kapasitet og kompetanse på området og at det er igangsatt tiltak for å styrke fagområdet styring og kontroll med data.

Finanstilsynet ber om å bli orientert om status og framdrift på arbeidet pr. 31. desember 2022.

3.5. IT-sikkerhet

IKT-forskriften § 5 stiller krav om at Banken 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. Nærmere utdyping av forskriftens bestemmelser finner man i "EBA GL on ICT" kapittel 3.4 "Information security".

3.5.1. Styring og kontroll med IKT-sikkerhet

Finanstilsynet har vurdert hvordan forbedringstiltak på IKT-sikkerhetsområdet identifiseres og gjennomføres.

DNB har de senere år gjennomført en årlig ekstern IT-modenhetsvurdering (IT maturity assessment), som er en analyse av om DNB følger beste praksis når der gjelder metoder og prosesser for styring av IKT-området. Banken benytter denne analysen til å identifisere tiltak som skal sikre at Banken når samme modenhet på IKT-området som sammenlignbare finansforetak, og bidra til at Banken har kontroll med de største cybersikkerhetsrisikoene. Tiltakene for forbedring av sikkerheten inngår i et veikart (Cyber Security Roadmap), som oppdateres med nye tiltak med utgangspunkt i det gjeldende trusselbildet for sikkerhetsrisiko.

I foreløpig rapport viste Finanstilsynet til Konsernrevisjonens rapport for første halvår 2021 der det framkommer at sikkerhetsstyring med distribuert sikkerhetsansvar og bruk av Security Champion som inngår i den nye leveransemodellen for IT-tjenester ikke fungerer tilfredsstillende.

Finanstilsynet registrerer fra styrets svar at den nye leveransemodellen for IT-tjenester forutsetter et distribuert sikkerhetsansvar, der rollen Security Champion i IT-enhetene ivaretar dette ansvaret. Det framgår av svaret at Group Security så langt har gjennomført sikkerhetsopplæring for totalt 62 Security Champions, et antall som vil øke utover i 2022. Banken oppgir at opplæringsprogrammet for Security Champions har vært viktig for å øke modenheten innen bevisstgjøring- og opplæringsområdet. Videre registrerer Finanstilsynet av styrets svar at arbeidet med å øke modenheten og redusere risikoen innenfor IKT-sikkerhetsområdet er et langsiktig og kontinuerlig arbeid som har høy prioritet i organisasjonen.

Finanstilsynet tar styrets vurdering om at gjennomførte tiltak de siste årene har medført en betydelig forbedring i den interne bevisstgjøringen og kunnskapen innenfor IKT-sikkerhet, til etterretning.

Finanstilsynet registrerer videre fra styrets svar at DNB i IT-modenhetsvurderingen for 2021 er vurdert til å ha tilsvarende modenhetsnivå innen cybersikkerhetsområdet som andre ledende internasjonale banker.

I foreløpig rapport påpekte Finanstilsynets også at det var fare for mangelfull implementering i gjennomføringen av tiltak for å styrke IKT-sikkerheten, da det framstod som uklart hvilke kriterier som legges til grunn for å konkludere om et tiltak er lukket, og om det gjennomførte tiltak faktisk reduserer sikkerhetsrisiko.

Fra styrets svar har Finanstilsynet merket seg at Konsernrevisjonen vil gjennomføre en egen revisjon av veikartet for forbedring av sikkerhet i første kvartal 2022, der rapporten vil bli behandlet av konsernledelsen og styret.

Det er Finanstilsynets forventning at Konsernrevisjonens revisjon vil ivareta vurdering av kriteriene for å lukke tiltak, og at tiltak i veikartet faktisk har redusert den risiko som er identifisert. Finanstilsynet ber om å få oversendt revisjonsrapporten når denne foreligger.

3.5.2. Tilgangsstyring for privilegerte brukere i foretaket og hos leverandører

IKT-forskriften § 5 stiller blant annet krav om at Banken skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon som er av betydning for foretakets virksomhet mot uautorisert adgang og endring. Videre at det skal finnes retningslinjer for tildeling, endring, sletting og kontroll

med autorisasjon for tilgang til IT-systemene. Utdyping av forskriftens bestemmelser finnes i "EBA GL on ICT", kapittel 3.4.2, der det blant annet framgår at medarbeidere ikke skal ha rettigheter og tilganger utover det som er nødvendig for at daglige oppgaver kan utføres. Det samme gjelder for leverandører og andre personer som har behov for tilgang direkte inn systemene.

Finanstilsynet har vurdert arbeidet med å forenkle og effektivisere styringen av tilganger i systemer i Banken. I tilsynsmøtene framkom det informasjon om at Banken arbeider med å forenkle og effektivisere styringen av tilganger ved å utvikle rollebaserte sikkerhetsmekanismer i systemene. Det ble opplyst at det gjenstår betydelig arbeide for ferdigstilling, der det ble antydet at 80% av arbeidet gjenstod ved utgangen av 2021. I foreløpig rapport var det Finanstilsynets vurdering at gjenstående tid er lang før DNB får forbedret systemstøtten for oppfølgingen av tilgangsstyringen basert på rollemodellering, og at nødvendige kompenserende kontroller for oppfølging av risiko for feil tildelte brukerrettigheter må vies særskilt oppmerksomhet.

Av styrets svar framgår det "*at rollemodellering er et av flere tiltak for å effektivisere og forenkle arbeid tilknyttet identitets- og tilgangsstyringsområdet. Formålet er å forenkle tilganger som gis på et organisatorisk nivå når en ansatt starter eller flytter internt i DNB. Arbeidet er en kontinuerlig prosess og utføres i parallell med andre utviklings- og forvaltningsoppgaver. Rollemodellering er en av mange mekanismer for å styrke automatisering og selvbetjening innenfor identitets- og tilgangsstyringsområdet, sammen med andre aktiviteter som for eksempel innføring av policybasert tilgangsstyring. Kontroller for oppfølging av risiko for feil tildelte brukerrettigheter gis høy oppmerksomhet fra alle forsvarslinjer, med gjennomføring av kontroller av nærmeste leder, tett oppfølging og rapportering fra Group Security på periodisk re-sertifisering og kontrollaktiviteter både hos 2.linje, 3.linje og eksternrevisor."* Videre framgår det av styrets svar *"at tilgangsstyring får en stadig viktigere rolle i DNBs dybdeforsvar, og videreutvikling av tilgangsstyring i takt med det digitale skiftet er nødvendig. Det er ingen åpne kontroll- og revisjonsfunn på tilgangsstyringsområdet".*

Finanstilsynet tar styrets svar til etterretning.

3.5.3. Sårbarhetsskanning

IKT-forskriften §13 stiller krav til at det er etablert "en samlet oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten". Utdyping av forskriftens bestemmelser finnes i "EBA GL on ICT", kapittel 3.5, der det framgår at utstyrsoversikten bør inneholde tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter. Videre bør det være registrert tilstrekkelig informasjon for å kunne identifisere eiendelen, dens plassering, eiendelens sikkerhetsklassifisering og eier.

I foreløpig rapport vurderte Finanstilsynet DNB sin utstyrsoversikt (CMDB) som ufullstendig med mangelfull registrering av utstyr, manglende dokumentasjon av sammenhenger mellom utstyr/tjenester, og at eier av utstyr for enkelte eiendeler manglet eller var feil. Finanstilsynets anbefaling var at DNB burde iverksette tiltak for å sikre kompletthet i CMDB, og sikre at utstyrsoversikten til enhver tid er oppdatert.

Videre var Finanstilsynets vurdering at det var en forhøyet sikkerhetsrisiko som følge av utestående arbeid i sårbarhetshåndteringen, noe som må oppfattes som mulig sikkerhetshull i DNB sitt etablerte cyberforsvar. Det var videre Finanstilsynet forventning at DNB sikrer at Banken har tilstrekkelig kapasitet til å ha løpende kontroll med sårbarheter i eksisterende IKT-systemer og IKT-utstyr, og at de identifiserte sårbarhetene blir klassifisert og utbedret i tråd med IKT-systemenes og IKT-utstyrets sikkerhetsmessige og forretningsmessige kritikalitet.

Finanstilsynet registrerer fra styrets svar at arbeidet med å utbedre sårbarheter er forbedret. Blant annet nevnes det at oversikten over IKT-systemer (CMDB) er forbedret, at det er etablert en mer effektiv prosess for håndtering og oppfølging av sårbarheter, at rapportene fra sårbarhetsanalysene er forbedret for å øke forståelsen av hvordan sårbarheter påvirker risikobildet og at området med sårbarhetshåndtering har fått økt fokus og rapporteres til konsernledelse og konsernsjef. Finanstilsynet har fra styrets svar merket seg at Banken benytter data fra nettverksutstyr som ekstra datakilde i skanneverktøy slik at man identifiserer og skanner for sårbarheter på enheter i nettverket som eventuelt ikke er registrert i CMDB. Finanstilsynet har fra styrets svar notert seg at det alltid vil eksistere et antall sårbarheter, der muligheten for å utnytte sårbarheten reduseres gjennom øvrig teknisk dybdeforsvar og kompenserende kontroller. Det framgår videre av styrets svar at Banken har hatt svært få hendelser med vellykket utnyttelse av sårbarheter.

Finanstilsynet tar styrets svar til etterretning.

3.5.4. Hindre tap av data

Finanstilsynet har vurdert i hvilken grad de ulike FO/SO og datterselskaper har vurdert risikoen for datatap og konsekvensene av dette med utgangspunkt i Bankens løsninger for å avdekke og hindre datatap.

I foreløpig rapport pekte Finanstilsynet på at det var uklart i hvilken grad de ulike FO/SO og datterselskaper vurderer egen risiko for datatap og konsekvensene av dette, og om de ulike FO/SO og datterselskaper har vurdert om de etablerte løsningene i Banken beskytter mot tap av data og ivaretar deres krav til datasikkerhet.

Av styrets svar framgår det at Banken ønsker å forbedre risikovurderinger knyttet til forretningsmessig konsekvens av datatap i de ulike FO/SO og datterselskaper. Finanstilsynet har fra styrets svar merket seg at Banken for 2022 har *"besluttet at risikokategorien "informasjonssikkerhet" skal få særskilt fokus i risiko- og kontrollvurderingene i samtlige områder, og Group Risk Management vil etterse at risiko for datatap inkluderes i disse vurderingene".*

Finanstilsynet ber om å motta dokumentasjon på at dette er gjennomført.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Jarleif Lødøen
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.