FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i DNB Bank ASA
Postboks 1600 Sentrum
0021 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
19/13577			06.09.2021

Tilsynsrapport

Finanstilsynet gjennomførte IT-tilsyn med DNB Bank ASAs (DNBs) filial i London (filialen) 7. og 8. desember 2020. Tema for tilsynet var styring og kontroll med IT-virksomheten i filialen med spesiell vekt på samhandlingen mellom IT i konsernet og IT i filialen, herunder konsernet og filialens evne til å håndtere en alvorlig IT-hendelse og filialens etterlevelse av DNBs sikkerhetsrammeverk.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 15. februar 2021 og styrets kommentarer til rapporten i brev av 28. april 2021.

Organisering.
DNB International er en del av DNB Corporate Banking. DNB International har gjennom IT International ansvar for IT i filialene, herunder filialen i London. Hovedkontoret leverer IT-tjenester til filialen. Dette er avtalefestet i Service Level Agreement (SLA) mellom hovedkontoret og filialen. Hovedkontoret har inngått avtalene med tredjepartsleverandørene, med unntak av noen få avtaler om lokale IT-leveranser til filialen.

IT-virksomhet i filialen.
Filialen i London håndterer IT lokalt i filialen, og i tillegg opererer den [redacted] Centre of Excellence [redacted] CoE). IT International i hovedkontoret har, som for de andre systemene i filialene, ansvar for leveransen av [redacted], men filialen i London, gjennom [redacted] CoE, har et spesielt ansvar for [redacted]. [redacted] CoE utvikler, forvalter og supporterer [redacted] for alle DNBs filialer der [redacted] brukes.

Systemporteføljen i filialen.
Filialen har kun bedriftskunder og tilbyr betalingstjenester, valutatjenester og kredittjenester. [redacted] er kjernesystemet. For øvrig benytter filialen de samme systemløsningene som hovedkontoret. Leveransene til filialen er regulert i en SLA-avtale med hovedkontoret, og hovedkontoret følger opp tredjepartsleverandørene. Det gjelder også for systemet [redacted]

Kort om [redacted]
[redacted] brukes i de fleste av de internasjonale filialene til DNB og er filialenes kjernesystem. [redacted] har funksjonalitet for hovedbok, regnskap, lån / kreditter, klientkontoer, betalinger, valuta m.m. [redacted] har grensesnitt til en rekke av DNBs andre systemer. Til sammen er det tre installasjoner av [redacted]. En i London, en i Singapore og en i New York. Ved å organisere det slik at [redacted] CoE har ansvar for alle tre installasjonene, blir kompetansen samlet. [redacted] er driftsleverandør for [redacted]

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf 22 93 97 02

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Forhold knyttet til styring og kontroll av risiko ved bruk av det proprietære systemet [redacted].
Finanstilsynet viste i foreløpig rapport til at bruk av et kjernesystem som er så gammelt som [redacted] kan medføre økt risiko. Det er fare for at teknologien som ligger til grunn for systemet ikke lenger vil kunne få system-støtte, samt høy avhengighet av nøkkelpersoner med risiko for mangel på kompetanse. Fra tilsynet noterte Finanstilsynet seg tiltak banken har iverksatt for å redusere risikoen ved bruk av [redacted], og ba i foreløpig rapport om oppdatert status på, og plan for, utfasing av funksjonalitet fra [redacted]

Fra styrets svar har Finanstilsynet merket seg at banken ikke prioriterer utskiftning av kjernesystem for internasjonale kontorer i inneværende strategiperiode, men planlegger å redusere bruken av [redacted] over tid, blant annet gjennom å flytte betalingsfunksjonalitet over i andre systemer. Den tekniske plattformen supporteres av [redacted] slik at risikoen ved å operere på denne plattformen ikke er forhøyet. Finanstilsynet har merket seg at banken i januar 2021 godkjente en plan for å rekruttere fem personer til [redacted] CoE for å håndtere potensiell, fremtidig nøkkelperson-risiko og at rekrutteringen er i gang. Finanstilsynet har også merket seg bankens program Corporate Payment Processing programme (CPP) for å forenkle verdikjeden for prosessering av bedriftsbetalinger, noe som vil redusere kompleksiteten og «fotavtrykket» til [redacted] gjennom prosessering av betalingene i andre, mer moderne systemer.

Finanstilsynet ber om status på rekrutteringsprosessen til [redacted] og CPP-programmet for prosessering av internasjonale betalinger pr. 1. desember 2021.

Forhold knyttet til styring og kontroll av leverandøroppfølging for filialen.
Filialens systemløsninger er basert på bruk av de samme leverandørene som hovedkontoret, herunder [redacted] som drifter [redacted] Hovedkontoret har inngått avtalene med tredjepartsleverandørene, inkludert rutinene for oppfølging av dem. Finanstilsynet stilte i foreløpig rapport spørsmål til om filialen har tilstrekkelig oversikt over og er tilstrekkelig involvert i utvikling, test, implementering og drift av systemene og tjenestene som filialen er avhengig av, og ba om styrets vurdering av om avtalene mellom hovedkontoret og filialen sikrer filialen tilstrekkelig kontroll med leveransene fra tredjepartsleverandørene.

Av styrets svar fremgår det at styret vurderer det som at implementeringen av en revidert IT-serviceavtale og etableringen i 2020 av månedlig servicerapportering med påfølgende oppfølgingsmøter, sikrer filialen tilstrekkelig oversikt over og involvering i utvikling, test, implementering og drift av systemene og tjenestene i filialen. Videre fremgår det av styrets svar at avtalene mellom hovedkontoret og filialen gir filialen tilfredsstillende kontroll over leveransene fra tredjepartsleverandørene.

Forhold knyttet til styring og kontroll med oppdatering mot sårbarheter.
Finanstilsynet pekte i foreløpig rapport på at oppdateringer mot sårbarheter og kvaliteten på rutiner for dette, samt oppfølgingen av aktuelle tredjepartsleverandørers etterlevelse av bankens krav til sårbarhetsoppdateringer, synes å ha vært dårligere for filialen enn for hovedkontoret.

Gjennom informasjon på tilsynsmøtet og styrets svar på foreløpig rapport, har Finanstilsynet merket seg tiltak iverksatt i 2020 for å øke kvaliteten på sårbarhetsoppdateringer for filialen.

Finanstilsynet ber styret sikre kontinuerlig oppmerksomhet på området.

Forhold knyttet til styring og kontroll med tilganger.

Privilegerte tilganger til [redacted]
Finanstilsynet ble på tilsynsmøtet informert om at filialen i 2020 planla å overlate majoriteten av privilegerte tilganger til [redacted] til medarbeidere hos driftsleverandøren og beholde færre selv. Finanstilsynet ba i foreløpig rapport filialen redegjøre for bakgrunnen og risikovurderingen som lå til grunn for dette.

Fra styrets svar har Finanstilsynet merket seg at filialen p.t. administrerer privilegerte tilganger selv, men at banken sammen med leverandøren er i en analysefase hvor risiko blir vurdert og krav dokumentert for å få til en slik endring, og at en endelig beslutning vil fattes etter dette er gjennomført. Finanstilsynet har videre merket seg at det samsvarer med bankens hovedavtale med leverandøren, at privilegerte tilganger administreres på samme måte for de ulike plattformene leverandøren drifter for banken.

Finanstilsynet stilte i foreløpig rapport spørsmål om privilegerte tilganger til [redacted] hos leverandøren og hos filialen selv, er gitt i henhold til kravene i bankens instruks 'Requirements for Identity and Access Management' kapittel Privileged Access.

Finanstilsynet har fra styrets svar merket seg at det er igangsatt en gjennomgang av om tilgangsstyringen for [redacted] tilfredsstiller alle kravene i nevnte instruks.

Rollebaserte tilganger.
Finanstilsynet viste i foreløpig rapport til at bankens instruks 'Requirements for Identity and Access Management' kapittel Privileged Access beskriver rollebasert tilgangsstyring, og det samme gjør filialens 'Information Security Framework'. Finanstilsynet ba filialen redegjøre for status på bruk av rollebaserte tilganger.

Fra styrets svar har Finanstilsynet merket seg at banken har identifisert et behov for å styrke bankens tilgangsstyring gjennom bruk av rollebaserte tilganger, og at det er startet et prosjekt der filialen er pilot.

Forhold knyttet til styring og kontroll med logging og overvåking av aktivitet i [redacted]
Gjennom tilsynet oppfattet Finanstilsynet det som at pålogging til [redacted] logges, men at øvrig aktivitet i [redacted] ikke logges og at logger ikke overvåkes spesielt. Finanstilsynet stilte i foreløpig rapport spørsmål ved om manglende aktivitetslogging og logg-oppfølging av [redacted] er i tråd med bankens egne instrukser på området.

Fra styrets svar har Finanstilsynet merket seg at all privilegert tilgang og arbeid gjennomført i [redacted] blir logget og journalført, herunder påloggінger fra tredjepartsleverandører. Alle påloggінger fra privilegerte brukere blir aktivt overvåket gjennom at brukeren må beskrive hvorfor pålogging skjer med privilegert tilgang.

Finanstilsynet forventer at banken aktivt følger opp loggingen av privilegerte brukere.

Kopi av tilsynsrapporten bes sendt intern og ekstern revisor.

For Finanstilsynet

Olav Johannessen
Seksjonssjef

Åshild Johnsen
Senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.