FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

DNB Bank ASA
Konsernsekretariatet
0021 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
17/3347			27.09.2019

Merknader - endelig rapport

Finanstilsynet gjennomførte stedlig tilsyn i DNB Bank ASA (DNB) 27. april 2018 og 27. november 2018 med tema styring og kontroll av IT-sikkerhetsområdet. Hensikten med tilsynet var å vurdere status på forventninger til informasjonssikkerhetsarbeidet, kommunisert til DNB etter tilsyn med samme tema i 2014 og 2017.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 8. februar 2019 og styrets kommentarer til rapporten i brev av 17. juni 2019.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Forhold knyttet til styring og kontroll av IT-sikkerhetsområdet.

Organisering av sikkerhetsområdet.
Finanstilsynet viste i foreløpig rapport til tidligere uttrykt forventning om tydeliggjøring av bankens organisering av IT-sikkerhetsområdet. Finanstilsynets vurdering i foreløpig rapport er at nåværende organisering på IT-sikkerhetsområdet, med et tydelig skille mellom ansvar for den overordnete strategiske sikkerhetsstyringen og det operative sikkerhetsarbeidet og mellom første- og andre forsvarslinjer, er en hensiktsmessig organisering. Finanstilsynet legger til grunn at denne organiseringen videreføres for å sikre stabilitet på IT-sikkerhetsområdet. Styrets svar på foreløpig rapport bekrefter dette. Finanstilsynet tar styrets svar til etterretning.

Oppmerksomhet om og forankring av IT-sikkerhetsarbeidet.
Finanstilsynet viste i foreløpig rapport til tidligere uttrykt forventning om at arbeidet med informasjonssikkerhetsområdet må få økt oppmerksomhet, bedre forankring og sterkere fremdrift. Finanstilsynets vurdering i foreløpig rapport er at den nåværende organiseringen av IT-sikkerhetsområdet, som innbefatter en større del av banken enn tidligere, kan bidra til at IT-sikkerhetsarbeidet får bredere ledelsesoppmerksomhet og -forankring. Finanstilsynet forutsetter at nødvendige tiltak for økt oppmerksomhet og forankring på området videreføres. Finanstilsynet har fra styrets svar merket seg beskrivelsen av den modellen banken har etablert for å styrke sikkerhetsarbeidet i forretnings- og støtteområdene. Finanstilsynet tar styrets svar til etterretning.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
Telefaks 22 63 02 26

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf 22 93 97 02

Sikkerhetsrammeverket.
Finanstilsynet viste i foreløpig rapport til bankens sikkerhetsrammeverk, og legger til grunn at overordnede prinsipper og krav i sikkerhetspolicy og -standard er rimelig statiske, uavhengige av organisering, roller, ansvar og detaljerte problemstillinger, og at de følges opp og rapporteres på. Det fremgår av styrets svar at banken gjennomgår og oppdaterer styrende dokumenter for sikkerhet minimum årlig. Finanstilsynet tar styrets svar til etterretning.

Finanstilsynet uttrykte i foreløpig rapport forventning om at banken sikrer regelmessig gjennomgang og oppdatering av sikkerhetsinstruksene, og at instruksene forankres internt og hos leverandørene. Finanstilsynet har fra styrets svar merket seg at sikkerhetstiltak videreutvikles og implementeres i driftsorganisasjonen og hos leverandørene i tråd med endringer i risiko. Finanstilsynet forventer at dette omfatter oppdatering av relevante sikkerhetsinstrukser til bruk internt og hos leverandørene.

Forretningssidens involvering i IT-sikkerhetsarbeidet.
Finanstilsynet ba i foreløpig rapport banken redegjøre for status på arbeidet med å involvere forretnings- og støtteområdene i sikkerhetsarbeidet. Styret redegjorde i sitt svar om arbeidet med å involvere forretnings- og støtteområdene mer systematisk i sikkerhetsarbeidet. Finanstilsynet tar styrets redegjørelse til etterretning.

Kopi av dette brevet bes sendt til ekstern og intern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Åshild Johnsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.