FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Sparebank 1 Nordvest
STYRET
Postboks 23
6501 KRISTIANSUND N

| VÅR REFERANSE | DERES REFERANSE | | DATO |
|---|---|---|---|
| 18/9257 | AR379625277 | | 06.11.2020 |

# Tilsynsrapport

Finanstilsynet gjennomførte stedlig IT-tilsyn i Sparebank 1 Nordvest (Banken) 7. november 2018. Tilsynet hadde som formål å vurdere hvordan Banken administrerer, utvikler, drifter, vedlikeholder og sikrer sine IT-systemer og -tjenester, der områder knyttet til IKT-sikkerhet og utkontraktering ble spesielt vektlagt.

Til grunn for merknadene ligger Finanstilsynets foreløpige rapport datert 9. mars 2020 og styrets kommentarer til rapporten av 26. juni 2020.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

## FORHOLD KNYTTET TIL STYRING OG KONTROLL INNEN IKT-OMRÅDET

### Forretningsstrategi og IKT-strategi

Finanstilsynet pekte i foreløpig rapport på at Banken mangler en egen samlet IKT-strategi, der rolle- og ansvarsfordelingen mellom Banken, SpareBank 1 Alliansen (Alliansen), SpareBank 1 Utvikling DA (SB1 Utvikling) og SpareBank 1 SamSpar AS (SamSpar) er omhandlet.

Finanstilsynet har fra styrets svar merket seg at foretaket nå har utviklet en lokal IKT-strategi som ble behandlet av styret 22. juni 2020.

### Forhold knyttet til risikostyring innen IKT-området

I foreløpig rapport stilte Finanstilsynet spørsmål om den etablerte metodikken for risikostyring og omfanget av Bankens risikoanalyse for IKT-området, der Banken i stor grad får sine viktige leveranser gjennom samarbeidet med SamSpar og SB1-Utvikling, er tilstrekkelig i forhold til det risikobildet Banken står overfor.

Finanstilsynet registrerer fra styrets svar at den nyutviklede lokale IKT-strategien har fastsatt et eget rammeverk for risikostyring innen IKT-området. Det fremgår videre av styrets redegjørelse at

**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

Banken fremover i større grad vil formalisere oppfølgingen av utkontraktert virksomhet og at Banken vil følge opp at identifiserte forbedringstiltak hos IKT-leverandørene blir gjennomført.

I foreløpig rapport ba Finanstilsynet Banken om å vurdere om den ville være tjent med å klassifisere avtaler med underleverandører etter viktighet av leveransene i forhold til konsekvenser for Bankens drift.

Finanstilsynet har fra styrets redegjørelse merket seg at SB1 Utvikling i løpet av våren 2020 har endret metodikk for oppfølging av utkontraktert virksomhet på vegne av bankene. Avtaler blir nå klassifisert som strategiske, taktiske, ikke kritiske og hyllevare. Finanstilsynet har merket seg at Banken i gjennomgang av avtaler og leveranser vil benytte en risikobasert tilnærming, der Banken tar utgangspunkt i avtaleeiers[1] oppfølging. Banken vil for den enkelte avtale/leveranse se på etterlevelsen av produkt- og prosessrisiko, IKT-sikkerhet, personvern, betaling og anti-hvitvask for å vurdere om dette følges opp tilfredsstillende.

Finanstilsynet merker seg fra styrets svar at SamSpar primo 2020 vedtok en ny policy for risikostyring og internkontroll, som er gjeldende for IKT-virksomhet som er utkontraktert fra Banken til SamSpar.

Finanstilsynet registrerer at styret i den samlede vurderingen av Bankens risikostyring mener at det benyttes en dekkende metodikk for risikovurderinger knyttet til leveransene Banken har under de ulike avtalene.

Finanstilsynet tar foretakets opplysning til etterretning.

**Dokumentstyring**

I foreløpig rapport ba Finanstilsynet Banken redegjøre for hvordan den sikrer at innholdet i dokumentasjonen av IKT-virksomheten til enhver tid er oppdatert, godkjent og gjort tilgjengelig for Bankens ansatte.

Finanstilsynet har merket seg Bankens redegjørelse for hvordan dokumentasjonen av IKT-virksomheten oppdateres. Blant annet fremgår det at styrende dokumenter skal oppdateres minst årlig med kontroll av at alle dokumentreferanser er oppdatert, og at dokumenter det refereres til er godkjent på riktig ansvarsnivå i Banken.

Finanstilsynet understreker at det er Banken som er ansvarlig for at IKT-virksomheten er tilstrekkelig dokumentert, også i de tilfeller der utgangspunktet er dokumentasjon utviklet av fellesskapet, eksempelvis i SB1 Utvikling. Banken må være særskilt oppmerksom på endringer i felles styrende dokumenter som har konsekvenser for Bankens egne rutiner og Bankens egenutviklede dokumentasjon, slik at Banken sikrer at konsekvenser av endringer er forstått på riktig ansvarsnivå i Banken.

[1] Avtaleeier er en medarbeider i SB1 Utvikling som er utpekt som ansvarlig for oppfølging av avtalen

## IKT-anskaffelser

I foreløpig rapport peker Finanstilsynet på at beslutningsprosessen knyttet til IKT-anskaffelser, bl.a. knyttet til hvordan Banken velger leverandør, fremstår som uklar. Finanstilsynet forventet at dette fremkom i Bankens IKT-strategi eller var uttrykt i en egen anskaffelsesstrategi.

Av styrets svar fremgår det at Bankens nye IKT-strategi har et eget kapittel om IKT-anskaffelser, og at innkjøp følger en fast prosess. Finanstilsynet tar foretakets opplysning til etterretning.

## Leverandørstyring

For Banken utgjør utkontraktering med ulike tjenesteleveranser, en helt sentral del av bankdriften. Finanstilsynet ba i foreløpig rapport Banken redegjøre for styring, kontroll og oppfølging av Bankens utkontraktering ift. IKT-forskriftens krav i § 12 om utkontraktering. Det følger av forskriften at foretaket er ansvarlig for å oppfylle alle krav i forskriften, også når hele eller deler av IKT-virksomheten er utkontraktert.

Det fremgår av styrets svar at oppfølging av forhold knyttet til utkontraktering er beskrevet i Bankens nyutviklede IKT-strategi, inklusive beskrivelse av styringsmodell. Kontrollene for etterlevelse av IKT-forskriften og av interne styrende dokumenter er tatt inn i årshjulet for de kontroller som compliancefunksjonen skal utføre. Banken har revidert rutinen for leverandørstyring, og leder for compliance vil delta på de interne månedlige og kvartalsvise møtene for oppfølging av utkontraktering. Leder compliance er tildelt et særskilt ansvar for å påse at kontrollene hos leverandørene utføres i tråd med avtalenes krav.

Det fremgår av styrets svar at styret mener Bankens reviderte metodikk nedfelt i den nyutviklede IKT-strategien, og forslagene til forbedringer av styringsmodellen som er beskrevet over, vil bidra til en tilfredsstillende oppfølging av den utkontrakterte virksomheten.

Siden Bankens utkontraktering, med ulike tjenesteleveranser, utgjør en så sentral del av bankdriften finner Finanstilsynet likevel grunn til å understreke det ansvaret Banken har for å oppfylle IKT-forskriftens bestemmelser også når hele eller deler av IKT-virksomheten er utkontraktert (jf. IKT-forskriftens § 12). Finanstilsynet forventer at Banken operasjonaliserer egne foreslåtte tiltak og at styret følger opp tiltakene knyttet til styring og kontroll med utkontrakteringen.

## Styring og kontroll med IKT-sikkerhet i samarbeidet med SamSpar

Finanstilsynet pekte i foreløpig rapport på at det fremstår uklart hvordan vedtatte policyer, retningslinjer og standarder for IKT-sikkerhet i Banken gjøres gjeldende, følges opp og kontrolleres i samarbeidet med SamSpar.

Av styrets svar fremgår det at arbeidet med IKT-sikkerhet i SamSpar bygger på de felles styrende dokumentene i Alliansen. Finanstilsynet merker seg fra styrets svar at de beskriver SamSpar sin virksomhet som begrenset, og at det ved behov utvikles egne styrende dokumenter i SamSpar. Som eksempel på egne utviklede styrende dokumenter nevnes policy for risikostyring og internkontroll med tilhørende årshjul som ble vedtatt primo 2020.

## Tilgangsstyring

I foreløpig rapport påpekte Finanstilsynet at Bankens rutine for tilgangskontroll ikke fastsetter hva som skal kontrolleres, hvor ofte kontroll skal utføres eller hvem som er ansvarlig for kontrollen.

Det fremgår av styrets svar at Banken har oppdatert rutinen for tilgangsstyring slik at den nå omfatter kontroll av ansatte, vikarer og eksterne parter (brukere som er gitt tilgang til informasjon og utstyr gjennom forhold knyttet til utkontraktering, inklusive SB1 Utvikling og SamSpar). Den oppdaterte rutinen konkretiserer hva som skal kontrolleres, frekvens på kontroller, hvem som er ansvarlige for gjennomføringen og at gjennomførte kontroller skal dokumenteres. Finanstilsynet tar foretakets opplysning til etterretning.

## Håndtering av kjente sårbarheter (patching)

I foreløpig rapport påpekte Finanstilsynet at Banken har ansvar for å sikre at kjente sårbarheter håndteres tilfredsstillende selv om tjenester er utkontraktert (jf. IKT-forskriften § 12). Dette gjelder både for intern (eksempelvis SB1-Utvikling og SamSpar) og ekstern utkontraktering. Etter Finanstilsynets oppfatning mangler Banken en samlet oversikt over status for oppdatering av kjente sårbarheter. Dette inkluderer utstyr som inngår i leveransene av de utkontrakterte tjenestene.

Finanstilsynet har merket seg at styrets svar er avgrenset til å omhandle Bankens patching av egne klienter som del av den daglige drift. Finanstilsynet etterlyser rutiner og kontroller for hvordan Banken sikrer at utstyr hos SB1 Utvikling, SamSpar og eventuelt andre leverandører, har adekvat oppdatering mot kjente sårbarheter for det tekniske utstyr som benyttes i forbindelse med de utkontrakterte tjenestene.

**Finanstilsynet ber om Bankens tilbakemelding på hvordan den sikrer at utstyr hos sine leverandører har adekvat oppdatering mot kjente sårbarheter innen 15. desember 2020.**

## Hendelsesrapportering

I henhold til IKT-forskriften § 9 tredje ledd skal hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data uten ugrunnet opphold rapporteres til Finanstilsynet. I foreløpig rapport etterlyste Finanstilsynet Bankens rutine for rapportering av hendelser i henhold til IKT-forskriften og spurte spesifikt om hvordan Banken avgjør om en hendelse er rapporteringspliktig eller ikke, og hvordan Bankens følger opp rapporteringen som SB1 Utvikling og eventuelt SamSpar gjør på vegne av Banken.

Det fremgår av styrets svar at Bankens rutine for hendelsesrapportering er oppdatert slik at rutinen nå beskriver hvordan Banken avgjør om en hendelse er rapporteringspliktig eller ikke. Ved alvorlige eller kritiske hendelser som kun påvirker Banken, melder Banken selv inn i tråd med lokal rutine for registrering og oppfølging av hendelser.

Finanstilsynet registrerer fra styrets svar at varslingspliktige IKT-hendelser som berører flere banker (fellesarenaen) varsles fra SB1 Utvikling til Finanstilsynet på vegne av bankene. Det fremgår videre at samtlige hendelser på fellesarenaen som er meldt Finanstilsynet og Datatilsynet vil bli listet opp i den kvartalsvise compliance-rapporten fra SB1 Utvikling. Banken får således mulighet for å kontrollere fullstendigheten av de hendelser som er meldt.

Det fremgår av styrets svar at Banken arbeider med å få etablert gjennomgang av hendelser som et fast agendapunkt i Bankens faste møter med SamSpar. Finanstilsynet forventer at styret også sikrer at det er etablert tilstrekkelig rapportering, styring og kontroll dersom det skulle inntreffe hendelser for IKT-tjenestene der SamSpar er direkte leverandør.

**Krisehåndtering**

Finanstilsynet ba i foreløpig rapport Banken vurdere å etablere spesifikke re-etableringsplaner for de scenariene Banken vurderer som de største risikoene for Bankens virksomhet.

Det fremgår av styrets svar at Banken har påbegynt arbeidet med å etablere slike re-etableringsplaner.

I foreløpig rapport etterlyste Finanstilsynet en rutine som beskriver hvordan resultater fra test av kontinuitets-/beredskapsløsninger skal rapporteres og presenteres for ledelse og styre.

Det fremgår fra styrets svar at både SB1 Utvikling og SamSpar utfører tester på vegne av bankene. Finanstilsynet har merket seg fra styrets svar at Banken pr. i dag ikke har etablert en egen rutine for oppfølging og rapportering av testresultater fra tester hos tredjeparter, men at dette vil inkluderes i Bankens rutine for leverandørstyring.

Finanstilsynet understreker viktigheten av at styret er informert om testplaner, utførte tester og resultatet av tester, også hos tredjeparter, slik at styret har kontroll med evnen til å håndtere kriser og uforutsette hendelser.

**Finanstilsynet ber om tilbakemelding på status for arbeidet med å utarbeide re-etableringsplaner, og rutine for oppfølging og rapportering av testresultater fra tester hos tredjeparter innen 15. desember 2020.**

Finanstilsynet ber om å motta kopi av protokoll fra styremøtet hvor Finanstilsynets merknader blir behandlet.

Kopi av dette brevet bes sendt til ekstern og intern revisor.
Kopi til:
ingvild@snv.no

For Finanstilsynet

Olav Johannessen
seksjonssjef

Jarleif Lødøen
tilsynsrådgiver

*Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.*