FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

SPAREBANKEN SOGN OG FJORDANE
v/Styret
Langebruvegen 12
6800 FØRDE

VÅR REFERANSE	DERES REFERANSE		DATO
21/11746	AR503457422		27.10.2022

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Sparebanken Sogn og Fjordane (banken) 8. desember 2021 og 18. februar 2022. Tilsynet hadde som formål å gjøre en vurdering av hvordan banken sikrer administrasjon, drift, vedlikehold og sikkerhet for bankens IKT-virksomhet. På bakgrunn av et rapportert sikkerhetsbrudd hos IKT-tjenesteleverandør av bankens kjernesystem ble det valgt å utvide omfanget av IKT-tilsynet til også å omfatte gjennomgang av denne hendelsen.

Til grunn for merknadene ligger Finanstilsynets foreløpige rapport datert 30. juni 2022 og styrets svar på rapporten i brev av 25. august 2022.

Finanstilsynet har følgende merknader etter det stedlige tilsynet.

Organisering
Finanstilsynet pekte i foreløpig rapport på at kontrollfunksjonen for IKT-sikkerhet skal være uavhengig fra førstelinjen. Dette for å sikre at ressurs- og kompetansebehov ikke skal kunne overstyres av tradisjonell IKT-prioriteringer og at viktige forhold som kontrollfunksjonen ønsker rapportert til ledelsen ikke skal kunne endres.

Det framgår av styrets svar at banken har endret organisering av kontrollfunksjonen og tilført en ekstra ressurs til oppgaven. Kontrollfunksjonen for IKT-sikkerhet er plassert i andrelinje med direkte rapporteringslinje til administrerende direktør. Det er utarbeidet rollebeskrivelse og stillingsinstruks for kontrollfunksjonen.

Finanstilsynet tar styrets opplysning til etterretning.

Konsekvensanalyse (Business Impact Analysis, BIA)
Finanstilsynet pekte i foreløpig rapport på at banken bør utarbeide konsekvensanalyser i samarbeid med forretningssiden, der resultatet av konsekvensanalysen gir oversikt over bankens systemportefølje og angir kritikaliteten systemene har for bankens virksomhet. Videre bør det framgå av analysen hva som er akseptabel nedetid for det enkelte IKT-system. Resultatet av analysen bør formidles til relevante leverandører. Det legges videre til grunn at rutine for utarbeidelse av forretningsmessige konsekvensanalyser etableres og inngår i bankens ordinære drift.

Det framgår av styrets svar at banken i løpet av høsten og vinteren 2022/2023 skal implementere et Governance, Risk and Compliance-system (GRC-system) og også utarbeide et fullstendig

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Stig Ulstein
Dir. tlf 22 93 99 66

Information Security Management System (ISMS). Banken ser på dette som viktig for å strukturere og dokumentere forretningsmessige konsekvensanalyser med tilhørende krav til akseptabel nedetid, samt oppfølging av dialogen med leverandører rundt disse kravene. Videre framgår det at arbeidet med å utarbeide forretningsmessige konsekvensanalyser vil starte først etter at GRC-systemet er implementert.

Finanstilsynet understreker viktigheten av at banken utarbeider forretningsmessige konsekvens-analyser, der resultatet av konsekvensanalysen gir oversikt over bankens systemporteføljе og angir kritikaliteten systemene har for bankens kritiske forretningsprosesser, og at gjennomføring av forretningsmessige konsekvensanalyser inngår i bankens ordinære drift, uavhengig av implementering av GRC-system. Finanstilsynet forventer at banken snarlig utarbeider slike konsekvensanalyser, i tråd med kravene i IKT-forskriften § 11 og EBAs "Guidelines on ICT and security risk management" (EBA/GL/2019/04). Finanstilsynet ber om å få en skriftlig redegjørelse og bekreftelse fra styret om at banken har iverksatt tiltak for gjennomføring av forretningsmessige konsekvensanalyser i tråd med regelverket innen 15. januar 2023.

Leverandørstyring

Finanstilsynet pekte i foreløpig rapport på at oppfølging av utkontrakterte IKT-fellestjenester, som inngår i FOI Rammeavtale i regi av Bits, er av stor viktighet for banken. Banken må ha prosedyrer for oppfølging av disse tjenestene. Selv om de utkontrakterte IKT-tjenestene er fellestjenester har likevel den enkelte bank et selvstendig oppfølgingsansvar for sitt kjøp og bruk av tjenestene, jf. IKT-forskriften § 12. Prosedyrene skal sikre at partenes forpliktelser, for eksempel nødvendig kapasitet, sikkerhet, overvåkning, kompetanse og krav til kontinuitet er etablert, og at alle tekniske og organisatoriske grenseflater mot avtalepartene er dokumentert.

Det framgår av styrets svar at banken har etablerte prosedyrer knyttet til sentrale leverandører og at arbeidet med leverandørstyring skal prioriteres og styrkes ytterligere.

Finanstilsynet tar styrets opplysning til etterretning.

Systemsikkerhet

Finanstilsynet pekte i foreløpig rapport på at bankens utstyrsoversikt (configuration management database, CMDB) er ufullstendig. Ved styring og kontroll av systemsikkerhet for utkontraktert virksomhet må banken sikre at IKT-tjenesteleverandørene innfrir sikkerhetskravene som banken har besluttet i egen sikkerhetspolicy. Dette inkluderer blant annet sårbarhetsstyring med krav til oppdateringer, håndtering av HW/SW (maskin- og programvare) som ikke lenger vedlikeholdes eller oppdateres av IKT-tjenesteleverandør og livssyklushåndtering med krav til anskaffelser/ avhending av utstyr.

Det framgår av styrets svar at banken vil arbeide videre med CMDB og at dette arbeidet vil gjøres i sammenheng med etablering av nytt GRC-system (Governance, Risk & Compliance). Det framgår videre at dette er et område banken vil prioritere.

Finanstilsynet tar styrets opplysning til etterretning.

Sikkerhetshendelse

Service Desk-prosess

Finanstilsynet pekte i foreløpig rapport på at det ikke er etablert en hensiktsmessig Service Desk-prosess hos IKT-tjenesteleverandør som sikrer en komplett oversikt over bankens henvendelser angående driftsoppdrag. Tjenstlige behov de ansatte hos IKT-tjenesteleverandør har for å utføre driftsoppgaver for banken på bakgrunn av henvendelsene blir ikke tilstrekkelig dokumentert. Det

gjør det ikke mulig å sammenstille antall henvendelser mottatt fra banken opp mot antall oppslag utført mot bankens IKT-driftsmiljø.

Det framgår av styrets svar at banken vil ta opp *"denne konkrete problemstillinga"* med IKT-tjenesteleverandør, samt kreve å få oversikt over alle som har tilgang til bankens produksjonsmiljø. Banken vil videre vurdere hvilke krav som kan og skal stilles til tilgangskontroll for å sikre seg mot uautoriserte oppslag.

Finanstilsynet fastholder at det med dagens løsning og praksis ikke er mulig for hverken banken eller IKT-tjenesteleverandør å ha kontroll med om ansatte hos leverandør bruker sine tilganger til uautoriserte oppslag i bankens kundedata. Finanstilsynet anser manglene knyttet til Service Desk-prosessen hos IKT-tjenesteleverandør som alvorlige og forventer at banken snarlig iverksetter nødvendige tiltak for å sikre at IKT-tjenesteleverandøren, og også banken, har komplett oversikt over alle henvendelser angående driftsoppdrag og at formålet med oppslagene leverandøren gjør mot bankens kunder dokumenteres på en slik måte at uautoriserte oppslag i bankens kundedata kan avdekkes. Finanstilsynet ber om å få en skriftlig redegjørelse og bekreftelse fra styret om at banken har iverksatt tiltak som gjør at banken kan avdekke uautoriserte oppslag innen 15. januar 2023.

Tilgangsstyring – utkontraktert IKT-virksomhet
Finanstilsynet pekte i foreløpig rapport på at sikkerhetshendelsen viser at etablert rutine for tilgangsstyring og oppfølging hos IKT-tjenesteleverandør ikke er tilstrekkelig, da det gir muligheter for å misbruke tilgangen til ikke-tjenstlige oppslag som vanskelig lar seg avdekke. Finanstilsynet stilte også spørsmål ved bankens styring og kontroll med tilgangsrettigheter ved utkontraktert virksomhet og om denne har vært tilstrekkelig.

Det framgår av styrets svar at banken *"vil prioritere å styrke oppfølginga av"* IKT-tjenesteleverandør *"i etablerte fora"* samt vurdere dagens rutiner og kontrollaktiviteter. Det framgår videre av styrets svar at banken har ferdigstilt overordnet retningslinje for utkontraktering.

Finanstilsynet fastholder at etablert rutine for tilgangsstyring og oppfølging hos IKT-tjenesteleverandør, samt banken oppfølging av denne, ikke er tilstrekkelig. Finanstilsynet anser manglene knyttet bankens styring og kontroll med tilgangsrettigheter ved utkontraktert virksomhet som alvorlige og forventer at banken, sammen med IKT-tjenesteleverandør, snarlig iverksetter tiltak og etablerer løsninger og kontrollrutiner for tilgangsstyring som sikrer at tilganger i størst mulig grad tildeles for det enkelte oppdrag utfra tjenstlige behov. Finanstilsynet ber om å få en skriftlig redegjørelse og bekreftelse fra styret om at banken har iverksatt tiltak som sikrer at tilganger, utfra tjenstlige behov, i størst mulig grad tildeles for det enkelte oppdrag innen 15. januar 2023.

Logging av brukeraktivitet
Finanstilsynet pekte i foreløpig rapport på at informasjonen som banken mottar fra IKT-tjenesteleverandør i form av logger over brukeraktivitet hos leverandøren ikke er tilstrekkelig for å avdekke ikke-tjenstlige oppslag i kundedata. Finanstilsynet mente også at banken ikke i tilstrekkelig grad har stilt krav til informasjon som gjør det mulig å sammenstilles data på en måte som vil kunne avdekke ikke-tjenstlige oppslag på kundedata.

Det framgår av styrets svar at banken vil kreve at det finnes datagrunnlag for å kunne *"utføre ein meir omfattande og regelmessig kontroll av bruk og tilgang til kundedata*". Videre framgår det av styrets svar at hvordan slik kontroll skal gjøres må utredes nærmere, at rutiner for håndtering av avvik og hendelser vil bli oppdatert og at det vil bli vurdert behov for ny løsning for systemstøtte.

Finanstilsynet fastholder at informasjonen som banken mottar fra IKT-tjenesteleverandør i form av logger ikke synes å være tilstrekkelig for å avdekke ikke-tjenstlig oppslag i bankkunders data og at

banken ikke i tilstrekkelig grad har stilt krav til informasjon fra IKT-tjenesteleverandør. Finanstilsynet anser bankens mangler i kontrollarbeidet med å avdekke om det foretas ikke-tjenstlige oppslag i bankens kundedata som alvorlig. Finanstilsynet forventer derfor at banken snarlig krever tilstrekkelig informasjon som gjør det mulig å sammenstilles data på en måte som kan avdekke ikke-tjenstlige oppslag i kundedata, både hos IKT-tjenesteleverandør og hos banken. Videre forventer Finanstilsynet at banken etablerer en funksjon for å avdekke eventuelle ikke-tjenstlige oppslag på kundedata. Finanstilsynet ber om å få en skriftlig redegjørelse og bekreftelse fra styret om at banken har iverksatt tiltak for å få tilgang til tilstrekkelige data for å kunne avdekke ikke-tjenstlige oppslag og etablert en funksjon for dette innen 15. januar 2023.

Tap av data

Finanstilsynet pekte i foreløpig rapport på at det følger av IKT-forskriften at banken skal ha prosedyrer for å sikre beskyttelse av informasjon av betydning for foretakets virksomhet mot blant annet skader, misbruk og hærverk. Basert på gjennomgang av IKT-tjenesteleverandørs tekniske løsninger for å hindre tap av data ble det stilt spørsmål ved i hvilken grad løsningene er tilstrekkelige og hensiktsmessige i forhold til de regulatoriske krav som stilles til banken. Finanstilsynet pekte videre på at de tekniske løsningene for å hindre tap av data må tilpasses risikoen for at dataene kan gå tapt, og eventuelt komme på avveie, og den konsekvens dette vil kunne ha for banken.

Det framgår av styrets svar at banken vil prioritere å styrke oppfølgingen av IKT-tjenesteleverandør, også med tanke på risiko for tap av data. Videre framgår det av svaret at *"vurderingar rundt kritikalitet og korleis sikre integriteten til relevante data, og vurderinga av konsekvensar av dette, vil vere ein del av ISMS og BIA".*

Finanstilsynet understreker viktigheten av at banken følger opp IKT-tjenesteleverandørs tekniske løsninger for å forhindre tap av data og forventer at banken snarlig etablerer en oppfølging for å sikre at disse samsvarer med bankens fastsatte beskyttelseskrav for data, jf. IKT-forskriften § 5. Finanstilsynet ber om å få en skriftlig redegjørelse og bekreftelse fra styret om at banken har iverksatt tiltak for å følge opp IKT-tjenesteleverandørs løsninger for å forhindre tap av data innen 15. januar 2023.

Finanstilsynet legger videre til grunn at banken vil vurdere beskyttelseskrav for relevante data i forbindelse med utarbeidelse av blant annet forretningsmessige konsekvensanalyser (BIA).

Finanstilsynet ber om å få oversendt protokollen fra styremøtet hvor tilsynsrapporten blir behandlet.

Finanstilsynet ber også om at kopi av dette brevet sendes til bankens valgte revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.