FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

SPAREBANK 1 HELGELAND
Postboks 68
8601 MO I RANA

VÅR REFERANSE	DERES REFERANSE		DATO
22/7080			31.03.2023

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Sparebank 1 Helgeland (banken) 7. september 2022. Tilsynet hadde som formål å gjøre en vurdering av hvordan styring og kontroll med IKT-området, herunder utkontraktering, tilgangsstyring, beredskap og risikostyring ivaretas av banken. Tilsynet omfattet gjennomgang av bankens styrende dokumentasjon knyttet til IKT-risiko, styring og kontroll med IKT-området, bruk av kvalitetsstyringsverktøy for internkontroll og samspill innen styring og kontroll med Sparebank 1 Utvikling AS og Sparebank 1 SamSpar AS.

Finanstilsynet har følgende merknader etter det stedlige tilsynet.

Organisering

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre stilles det i § 13-5 andre ledd krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. CRR/CRD IV-forskriften § 38 stiller krav om at banken skal ha en uavhengig risikokontrollfunksjon med tilstrekkelig kompetanse og ressurser, og at risikokontrollfunksjonen skal sikre at alle vesentlige risikoer i banken er identifisert, målt og rapportert av de relevante organisatoriske enhetene. EBAs retningslinjer for IKT og sikkerhet kapittel 3.3.1 gir en utdyping av IKT-forskriftens bestemmelser og finansforetakslovens bestemmelser om forsvarlig organisering og uavhengige kontrollfunksjoner knyttet til risikostyring, etterlevelse og internrevisjon, gjeldende for bankens IKT-virksomhet.

Finanstilsynet pekte i foreløpig rapport på at bankens funksjon sikkerhetssjef, som kravstiller på informasjonssikkerhetsområdet til førstelinjen, selv inngikk i førstelinjen og rapporterte til IT-sjefen i banken. Finanstilsynet vurderte at denne funksjonen burde være uavhengig fra førstelinjen og pekte på at arbeidet i kontrollfunksjonen burde holdes tilstrekkelig adskilt fra daglige IT-driftsprosesser for å sikre uavhengighet.

Finanstilsynet ser av styrets svar at banken vil organisere rollen som sikkerhetssjef i andrelinjen, mens rolle som fagansvarlig sikkerhet legges i førstelinjen.

Finanstilsynet tar styrets svar til etterretning.

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

Overordnet risikostyring

CRR/CRD IV-forskriften stiller krav om at styret skal godkjenne og regelmessig vurdere retningslinjer for å påta banken risikoer, og for å identifisere, styre, overvåke og kontrollere risikoene. IKT-forskriften § 2 første ledd stiller videre krav til at banken skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet pekte i foreløpig rapport på at det i bankens styrende dokumenter for hhv. operasjonell risiko og informasjonssikkerhet framgår en målsetting om en lav risikoprofil, Det framgikk derimot ikke en nærmere omtale eller operasjonalisering av styrets risikotoleranse.

Finanstilsynet ser av styrets svar at banken vil definere risikotoleranse for bankens bruk av IKT og konkret risikoeksponering av virksomhetens samlede IKT-risiko. Dette for å sikre at bankens risikotoleranse for bruk av IKT er tydelig og forankret i styrende dokumenter.

Finanstilsynet tar styrets svar til etterretning.

Metodikk for vurdering av IKT-risiko

IKT-forskriften § 3 første ledd stiller krav om at banken skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT. Videre stilles det i forskriftens § 3 andre ledd krav om at banken skal ha en dokumentert prosess for gjennomføring av risikoanalyser for IKT-virksomheten.

I foreløpig tilsynsrapport pekte Finanstilsynet på at bankens metodikk for vurdering av risiko ikke i tilstrekkelig grad ivaretar identifisering og dokumentasjon av risiko forbundet med bankens bruk av IKT.

Av styrets svar framgår det at banken vil innarbeide en beskrivelse av de ulike graderingene for sannsynlighet og konsekvens relevant for vurdering av IKT-risiko i sine styrende dokumenter.

Finanstilsynet tar styrets svar til etterretning.

Rapportering av IKT-risiko

Etter finansforetaksloven § 8-6 fjerde ledd skal styret føre tilsyn med den daglige ledelse og bankens virksomhet for øvrig, og sørge for at daglig leder regelmessig gir styret informasjon om bankens virksomhet. Styrets rolle knyttet til bankens system for risikostyring og internkontroll er utdypet i CRR/CRD IV-forskriften § 35. Der presiseres det blant annet at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Finanstilsynet pekte i foreløpig tilsynsrapport på at skal styret kunne føre kontroll med daglig ledelse og banken ellers, må styret sikre seg løpende og oppdatert informasjon om all IKT-risiko i banken.

Av styrets svar framgår det at banken vil etablere tiltak som skal sikre en bredere rapportering av IKT-risiko.

Finanstilsynet tar styrets svar til etterretning.

Datakvalitet

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

Styring og kontroll med data utgjør prosessen med å administrere integritet, tilgang, tilgjengelighet, brukervennlighet, og sikkerhet for dataene i bankens datasystemer basert på interne datastandarder og retningslinjer. Dataintegritetsrisiko utgjør risikoen for at data behandlet og lagret av IT-systemer ikke er fullstendige, nøyaktige eller konsistente. Effektiv styring og kontroll med data skal sikre konsistente og pålitelige data, og sikre at data ikke blir misbrukt.

Med bakgrunn i økende bruk av automatisering og behov for økt kontroll og innsikt i tilgjengelige data pekte Finanstilsynet i foreløpig rapport på at banken ikke har et overordnet rammeverk for arbeid med datakvalitet. Risikoen for feil som følge av dårlig datakvalitet kan ha potensielt ha store konsekvenser.

Av styrets kommentarer framgår det at banken har etablert tiltak som vil ivareta Finanstilsynets påpekninger.

Finanstilsynet tar styrets svar til etterretning.

Forretningsmessig konsekvensanalyse

Banken har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. "EBA Guidelines on ICT and security risk management" (EBA/GL/2019/04) (sist nevnte her etter kalt EBAs retningslinjer for IKT og sikkerhet) gir en utdyping av IKT-forskriftens bestemmelse for hvordan banken skal sikre forretningsmessig kontinuitet basert på forretningsmessig konsekvensanalyser (BIA[1]). Videre gir den anbefalinger om utarbeidelse av kontinuitetsplaner, respons- og gjenopprettingsplaner, testing og kommunikasjonsplaner ved kriser.

Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i forretningsmessige konsekvensanalyser for bankens kritiske forretningsprosesser. Forretningsmessig konsekvensanalyse skal bidra til å sikre at bankens beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet. Planene skal basere seg på bankens prioriteringer for gjenoppretting av forretningskritiske tjenester og prosesser. Prioriteringene for gjenoppretning skal basere seg på resultatene fra analysen hvor det også skal framgår hva som er akseptabel nedetid for det enkelte IKT-system. Beredskapsplanene, som viser bankens prioriteringer for gjenoppretting, bør formidles til relevante leverandører. For å verifisere at det er etablert fungerende planer og løsninger må det foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig rapport på at det ikke er gjennomført en forretningsmessig konsekvensanalyse og det er derfor Finanstilsynet vurdering at banken har mangler i sin etterlevelse av kravene i IKT-forskriften § 11 vedrørende driftsavbrudd og kriseberedskap.

[1] BIA – Business Impact Analysis

Av styrets kommentarer til foreløpig rapport framgår det at banken har gjennomført tiltak som vil sikre at forretningsmessige konsekvensanalyser blir utarbeidet og at dette vil inngå i arbeidet med å utarbeide kontinuitet- og beredskapsløsninger som ivaretar bankens krav til reetablering.

Finanstilsynet tar styrets svar til etterretning.

Leverandørstyring

I henhold til IKT-forskriften § 2 Planlegging og organisering skal *"Foretaket ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12"*. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre 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 foretaket skal sikre leveransene"*.

Banken har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det framgår av bestemmelsen at banken må sikre at organisasjonen, i egen regi eller gjennom formalisert samarbeid med andre foretak enn IKT-leverandøren, har tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalene.

Finanstilsynet pekte i foreløpig rapport på at banken har mangler i sin etterlevelse av kravene i IKT-forskriften hva gjelder oppfølging av risikostyring, kvalitet og SLA av den utkontrakterte IKT-virksomheten.

Finanstilsynet pekte videre på at selv om flere av de utkontrakterte IKT-tjenestene er fellestjenester for alliansene banken inngår i, og også banknæringen samlet sett, har likevel den enkelte bank et selvstendig oppfølgingsansvar for sitt kjøp og bruk av tjenestene.

Av styrets kommentar framgår det at banken har etablert et rammeverk for leverandøroppfølging som vil kunne sikre god oppfølging av utkontrakterte IKT-tjenester.

Finanstilsynet tar styrets svar til etterretning.

Systemsikkerhet

IKT-forskriften § 5 Sikkerhet stiller krav om at banken skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for bankens 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 utdypinger finnes i EBAs retningslinjer for IKT og sikkerhet.

IKT-forskriften § 13 stiller krav til at det er etablert en *"oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten"*. EBAs retningslinjer har lignende anbefalinger, der det framgår at banken bør ha en oppdatert utstyrsoversikt over IKT-systemer, nettverksenheter, databaser etc. Utstyrsoversikten bør inneholde tilstrekkelige konfigurasjonsdata

og angi avhengigheter mellom utstyr/komponenter, samt at det bør være registrert tilstrekkelig informasjon for å kunne identifisere eiendelen, dens plassering, eiendelens sikkerhetsklassifisering og eier.

Finanstilsynet pekte i foreløpig rapport på at bankens utstyrsoversikt hadde mangelfull registrering av utstyr, manglende dokumentasjon- av sammenhenger mellom utstyr/tjenester og eierskap. Det ble videre pekt på at ved styring og kontroll av systemsikkerhet for utkontraktert virksomhet må banken sikre at også tjenesteleverandørene innfrir sikkerhetskravene i bankens besluttede sikkerhetspolicy.

Av styrets kommentar framgår det at banken har tilgang til detaljert dokumentasjon av utstyrsoversiktene hos bankens IKT-tjenesteleverandører. Det framgår videre av styrets svar at banken vil etablere tiltak som skal sikre en fullstendig oversikt over bankens eget tekniske utstyr.

Finanstilsynet tar styrets svar til etterretning.

Ikke-tjenstlige oppslag på kundedata

Finanstilsynet mottok meldinger om at bankens IKT-tjenesteleverandør hadde varslet om at to av leverandørens ansatte hadde gjort ikke-tjenstlige oppslag på en rekke norske bankers kunder. Hendelsen var omfattende, og det ble ved nærmere undersøkelser avdekket oppslag på bankkunder fra to ansatte hos tjenesteleverandøren. Sparebank 1 Helgeland var ikke direkte berørt av hendelsen siden ingen av deres kunder ble gjort oppslag på.

Av styrets svar kommer det fram hvilke tiltak banken planlegger å etablere, samt allerede etablerte tiltak, for å styrke kontroll og håndtering av oppfølging av oppslag på kundedata.

Finanstilsynet tar styrets svar til etterretning.

Service Desk-prosess

I EBAs retningslinjer for IKT og sikkerhet anbefales det at "*Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur*".

Det ble i foreløpig rapport var det Finanstilsynets vurdering at det ikke er etablert en hensiktsmessig Service Desk-prosess hos IKT-tjenesteleverandør som sikrer en komplett oversikt over bankens henvendelser angående driftsoppdrag.

Av styrets svar kommer det fram at banken sammen med IKT-tjenesteleverandør vil søke å etablere løsninger som vil sikre dokumentasjon på at oppslag på bankens kundedata er basert på tjenstlig behov.

Finanstilsynet tar styrets svar til etterretning

Tilgangsstyring – utkontraktert IKT-virksomhet

IKT-forskriften § 5 Sikkerhet stiller krav om at banken skal ha "*prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk"*. Videre skal "*prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene*". Ytterligere utdypinger finnes i EBAs retningslinjer for IKT og sikkerhet.

Finanstilsynet ble under tilsynet informert om at dersom en ansatt hos IKT-tjenesteleverandør innehar en rolle hvor det er nødvendig å ha tilganger til bankens IKT-driftsmiljø anses dette som et tjenstlig behov for å kunne utføre sitt arbeid. Ved et slikt definert tjenstlig behov vil den ansatte bli satt opp med permanente tilganger til bankens IKT-driftsmiljø uten tidsbegrensning, eller andre typer begrensninger for når tilgangene kan benyttes.

Finanstilsynet vurderte i foreløpig rapport at dersom ansatte hos IKT-tjenesteleverandør har et tjenstlig behov for å ha tilgang til bankens IKT-driftsmiljø, inkludert applikasjoner og data, bør løsningene for tilgangsstyring og kontrollrutiner i størst mulig grad være utformet slik at tilganger tildeles og kontrolleres for det enkelte oppdrag.

Av tar styrets svar fremgår det at banken sammen med IKT-tjenesteleverandør har iverksatt tiltak for i størst mulig grad å kunne tildele tilgangsrettigheter tidsbegrenset og/eller for det enkelte oppdrag.

Finanstilsynet tar styrets svar til etterretning.

Kopi av rapporten bes sendt intern og ekstern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.