FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Sparebank 1 SMN
Postboks 4796 Torgarden
7467 TRONDHEIM

VÅR REFERANSE	DERES REFERANSE		DATO
23/6326			15.04.2024

Tilsynsrapport - Sparebank 1 SMN

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Sparebank 1 SMN (SMN) 29. og 30. august 2023. Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Tilsynet ble avgrenset til elektronisk forsvar og tilhørende emner innen IKT-sikkerhet, og styring og kontroll med IKT-virksomheten. Videre ønsket Finanstilsynet å gjøre en vurdering av foretakets beredskapsarbeid relevant for IKT-området, herunder vurdere beredskapen i foretaket og for utkontrakterte IKT-tjenester, samt overholdelse av regulatoriske krav på IKT-området.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 29. november 2023 og styrets kommentarer til rapporten i brev av 9. februar 2024.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

1. Overordnet styring og kontroll

1.1. Organisering

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre i lovens § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. CRR/CRD IV-forskriften stiller krav i § 38 om at foretaket skal ha en uavhengig risikokontroll-funksjon med tilstrekkelig kompetanse og ressurser, og at risikokontrollfunksjonen skal sikre at alle vesentlige risikoer i foretaket er identifisert, målt og rapportert av de relevante organisatoriske enhetene. Forskriften stiller videre krav i § 39 at foretaket skal ha en uavhengig kontrollfunksjon for kontroll av etterlevelse, samt ha retningslinjer og prosedyrer for å avdekke risiko for at foretaket ikke oppfyller sine forpliktelser etter lov og forskrift.

Det er Finanstilsynets vurdering at for å ha god styring og kontroll på egen IKT-virksomhet, også den som er utkontraktert, bør foretaket gjennomføre egne kontroller både når det gjelder risiko og etterlevelse. Finanstilsynet mener videre at det er viktig med tilstrekkelig IKT-kompetanse og nok ressurser i de tre forsvarslinjene for å følge opp egen og utkontraktert virksomhet. Kontrollfunksjonene skal sikre at alle vesentlige risikoer i foretaket er identifisert, målt og rapportert av de relevante organisatoriske enhetene.

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

Finanstilsynet pekte i foreløpig rapport at foretakets oppfølging av IKT-risiko i de tre forsvarslinjene er mangelfull og ikke i samsvar med regelverket, jf. finansforetaksloven § 13-5 (2) og CRR/CRD IV-forskriften § 39. Finanstilsynet stilte videre spørsmål ved hvordan foretaket sikrer at foretaket har tilstrekkelig ressurser og kompetanse på IKT-området for å utføre den nødvendige oppfølgingen, både i første og andre linje, og minner om styrets ansvar for å sørge for en forsvarlig organisering av virksomheten, jf. finansforetaksloven § 8-6.

Styret skriver i sitt svar at SMNs oppfølging og kontroll av underleverandører foregår gjennom et sett av ulike styringsorganer, både på strategisk -, taktisk - og operativt nivå. Videre pekes det i styrets svar på deltagelse i ulike råd og forum som skal se til at det gjennomføres tilstrekkelig risikovurdering og kontroll av felles prosesser og aktiviteter i felleskapet i samsvar med felles krav, herunder ansvar, roller og kontroll med utkontrakterte tjenester til IKT-tjenesteleverandør. Videre pekte styret på at oppfølging av kritiske leverandører foretas gjennom etablerte samhandlingsarenaer.

I styrets svar ble det videre kommentert at det utover de etablerte arbeidsprosesser i første, andre og tredjelinje er ytterligere behov for å styrke og systematisere oppfølging av kontrollarbeidet.

Finanstilsynet merker seg styrets kommentarer om oppfølgingen av leverandører og underleverandører, og at foretaket har identifisert et ytterligere behov for styrking og systematisering av kontrollarbeidet i første, andre og tredjelinjen. Finanstilsynet vil likevel bemerke viktigheten av at SMN har tilstrekkelig IKT-kompetanse og nok ressurser i de tre forsvarslinjene til å følge opp egen og utkontraktert virksomhet.

I foreløpig rapport pekte Finanstilsynet på at informasjonssikkerhetsansvarlig er organisert i førstelinje, som medfører at informasjonssikkerhetsansvarlig ikke har en uavhengig rolle i forhold til SMNs førstelinje. Dette medfører at SMN må sikre at andrelinjen har ressurser og kompetanse som kan kontrollere og se til at foretakets IT-sikkerhetspolicy er operasjonalisert i foretaket, og at de samme kravene også gjelder for IKT-tjenesteleverandører og underleverandører.

Av styrets svar fremgår det at etterlevelsesfunksjonen gjennomfører en rekke kontroller blant annet av at IKT-forskriftens krav er operasjonalisert og etterleves, og at det er stor grad av sammenfall mellom IKT-forskriftens krav og SMNs Policy for informasjonssikkerhet. Videre skriver styret at etterlevelsesfunksjonen og risikokontrollfunksjonen har en rådgivende funksjon i utarbeidelse og revidering av Policy for informasjonssikkerhet. Etterlevelsesfunksjonen sikrer at policyen dekker IKT-forskriftens krav, og gjør deretter uavhengige etterlevelseskontroller.

Finanstilsynet merker seg styrets kommentarer, men vil likevel bemerke at SMNs risikokontroll- og etterlevelsefunksjon er kontrollfunksjoner som må kontrollere at foretakets IT-sikkerhetspolicy er operasjonalisert i foretaket, og at de samme kravene også gjelder for IKT-tjenesteleverandører og underleverandører

Finanstilsynet pekte i foreløpig rapport på at SMNs tre forsvarslinjer må ha tilgang til relevant informasjon, og at kontrollfunksjonenes uavhengighet må ivaretas også for utkontraktert virksomhet. CRR/CRD IV-forskriften stiller krav i § 38 om at foretaket skal ha en uavhengig andrelinje med tilstrekkelig kompetanse og ressurser, og at andrelinjen skal sikre at alle vesentlige risikoer, som IKT-risiko, i foretaket er identifisert, målt og rapportert av de relevante organisatoriske enhetene.

Styret skriver i sitt svar at SMNs førstelinje mottar rapporter fra IKT-tjenesteleverandørs andre og tredjelinje, dette for å håndtere førstelinjes arbeid med kravstilling, oppfølgning og kontroll. Videre skriver styret at både første- og andrelinje i SMN har nødvendige tilganger fra IKT-tjenesteleverandør med tilgang til eksempelvis compliance-rapporter, virksomhetsrapporter, sikkerhetsrapporter og internrevisjonsrapporter. Videre vil SMN sikre at SMNs tredjelinje får tilgang til nødvendig dokumentasjon for å ytterligere understøtte kontrollfunksjonens uavhengighet.

Finanstilsynet merker seg SMN svar, men vil likevel understreke viktigheten av bruken av dokumentasjonen relatert til de tre forsvarslinjers ansvar og oppgaver.

1.2. Overordnet risikostyring

CRR/CRD IV-forskriften § 35 stiller krav om at styret skal godkjenne og regelmessig vurdere retningslinjer for risikoer foretaket påtar seg og for å identifisere, styre, overvåke og kontrollere risikoene. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten.

Finansforetaksloven § 13-5 stiller krav til forsvarlig virksomhet og god forretningsskikk. Foretaket skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke, og rapportere risiko foretaket er eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd.

Finanstilsynet pekte i foreløpig rapport på at det forventes at styregodkjente styringsdokumenter som strategier og policyer følges opp for å sikre at foretakets drift og planer utføres i henhold til disse. Videre er det Finanstilsynets vurdering at siden det er foretakets førstelinje som står som eier av strategier for IKT-området så vil det være hensiktsmessig at det er SMNs andrelinje og tredjelinje som følger opp etterlevelsen av strategier og kontrollerer at de styrende dokumentene er operasjonalisert i henhold til disse.

Styret skrev i sitt svar at SMNs strategier er innrettet med flere formål, inkludert det å ivareta regulatoriske krav. Spesielt IT-strategien er innrettet for å dekke regulatoriske krav i IKT-forskriften. Videre skriver styret at det er SMNs førstelinje som eier IKT-strategiene. I tillegg til at disse er forretningsorienterte og setter søkelys på strategiske satsningsområder, så vil IKT-strategiene ha som et hovedmål å legge føringer for etterlevelse av regulatorisk krav, spesielt IKT-forskriften. Styret skrev videre i sitt svar at andrelinjen, særlig etterlevelsesfunksjonen, gjør kontroller av selskapets etterlevelse av IKT-forskriften og andre regulatoriske krav som treffer IKT-området og kontrollene er derfor også innrettet mot etterlevelse av strategiene og operasjonalisering av disse.

Finanstilsynet merker seg SMN svar, men vil likevel understreke viktigheten av at risikokontroll- og etterlevelsesfunksjonen utfører kontroller som skal sikre at strategier og andre styrende dokument er operasjonalisert.

Av styrets svar fremgår det at internrevisjonen jobber ut ifra en styrevedtatt revisjonsplan og at planen er utarbeidet med utgangspunkt i internrevisjonens vurdering av risikobildet, samt innspill fra konsernledelsen og risikoutvalg. Revisjonsaktivitetene inkluderer å vurdere om etablert

rammeverk er i samsvar med vedtatt risikoprofil, og at interne retningslinjer og eksterne lovkrav etterleves, samt om rapportering og informasjon til styret fra første og andre linje gir et riktig bilde av SMNs risikostyring og internkontroll.

Finanstilsynet merker seg SMN svar, men vil likevel understreke viktigheten av at internrevisjonen utfører kontroller som skal sikre tilstrekkelig kontroll av SMNs IKT-virksomhet, også hos IKT-tjenesteleverandører.

CRR/CRDIV-forskriften § 36 stiller krav om at retningslinjene for risikostyring skal omfatte en rutine for å identifisere og evaluere risikoer forbundet med nye og vesentlige endringer i produkter, tjenester og andre aktiviteter, herunder utkontraktering. Kontrollfunksjonene for risikostyring og etterlevelse skal involveres i risikovurderingene.

Finanstilsynet pekte i foreløpig rapport på at det er viktig at SMNs andrelinjefunksjon har en uavhengig rolle i forhold til oppgaver som skal utføres i godkjenningsprosessen for nye produkter, tjenester, systemer og prosesser. Det er videre Finanstilsynets vurdering at eierskapet av sentrale system bør plasseres slik at foretaket har en uavhengig kontrollfunksjon med mulighet til å påpeke svakheter eller mangler i viktige prosesser.

Styret skriver i sitt svar at SMN her etablert tiltak som sikrer at SMNs andrelinje funksjon er en kontrollfunksjon som verifiserer at godkjenningsprosessen for nye produkter, tjenester, systemer og prosesser er gjennomført i tråd med gjeldende retningslinjer, inkludert at riktige fagpersoner har gitt sine vurderinger.

Finanstilsynet tar styrets svar til etterretning.

1.3. Rapportering av IKT-risiko

Etter finansforetaksloven § 8-6 fjerde ledd skal styret føre tilsyn med daglig ledelse og foretakets virksomhet for øvrig, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. Styrets rolle knyttet til foretakets 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 rapport på at det meste av foretakets IKT-virksomhet er utkontraktert, og vurderer at det er viktig, for å kunne ivareta målsetningene som stilles i policyen, at det gjennomføres egne kontroller på IKT-tjenester levert av IKT-tjenesteleverandør. Det kan være kontroller som etterlevelse av SMNs styrende dokumenter, samt kontroller på områder som tilgangsstyring, endringshåndtering, utvikling, prosjektstyring, beredskap, kompetanse, tilgang på ressurser osv.

Styret skriver i sitt svar at det gjennomføres kvartalsvis kontroll av IKT-området fra avdeling Risikostyring som både omfatter intern IKT-virksomhet og utkontraktert IKT-virksomhet. Kontrollen omfatter leveranser fra utkontraktert virksomhet, intern driftsstabilitet og informasjonssikkerhet. Styret skriver videre at når det gjelder andrelinjens kontrollaktiviteter refererer SMN til etterlevelsesfunksjonens arbeidsplan og kvartalsvis etterlevelsesrapport. Det gjennomføres en rekke etterlevelseskontroller innenfor IKT. Når det gjelder tredjelinjens kontroller skriver styret at opprinnelig plan ble endret for å delta i et felles prosjekt i SpareBank 1 alliansen med samme formål.

Finanstilsynet merker seg SMN svar, men vil likevel understreke viktigheten av at alle tre forsvarslinjer gjennomfører egne kontroller som skal sikre at strategier og andre styrende dokument er operasjonalisert også hos IKT-tjenesteleverandører hvor relevant.

Finanstilsynet pekte i foreløpig rapport på at risikoer rapportert fra SMNs tredjelinje ikke hadde en oppfølgingsprosess som sikret tilstrekkelig oppmerksomhet for åpne risikoer.

I styrets svar skrives det at SMN har en eksisterende prosess for å følge opp SMNs internrevisjonsrapporter. Styret vil med bakgrunn i innspill fra kontrollfunksjonene påse at prosessen med rutiner inneholder nødvendige kontroller for å sikre en helhetlig oppfølging av risikoer med tilhørende tiltak.

Finanstilsynet tar styrets svar til etterretning.

2. Styring med og kontroll av IKT

2.1. Virksomhetens konsekvensanalyse ved avbrudd

Foretaket har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. EBAs retningslinjer for IKT og sikkerhet[1] gir en utdyping av IKT-forskriftens bestemmelse for hvordan foretaket skal sikre forretningsmessig kontinuitet basert på virksomhetens konsekvensanalyser ved avbrudd (BIA[2]).

Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i virksomhetens konsekvensanalyser ved avbrudd i foretakets kritiske forretningsprosesser. Konsekvensanalysen skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av forretningskritiske tjenester og prosesser. Prioriteringene for gjenoppretting skal basere seg på resultatene fra analysen hvor det også skal framgå hva som er akseptabel nedetid for det enkelte IKT-system. Beredskapsplanene, som viser foretakets 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 med bakgrunn i at det ikke er gjennomført en BIA har foretaket mangler i sin etterlevelse av kravene i IKT-forskriften § 11. Finanstilsynet forventer at foretaket utarbeider BIA ledet av forretningssiden, der resultatet av konsekvensanalysen blant annet vil gi oversikt over foretakets systemportefølje og angi kritikaliteten systemene har for foretakets virksomhet. Videre bør det framgå av analysen hva som er akseptabel nedetid for det enkelte IKT-system. Resultatet av analysen bør også formidles til relevante leverandører. Det legges til grunn at rutine for utarbeidelse av BIA etableres og inngår i foretakets ordinære drift.

Styret skriver i sitt svar at det er etablert et prosjekt for etablering av rammeverk og rutine for BIA i SMN, samt gjennomføring av en første iterasjon av en BIA. Videre skriver styret at prosjektet har levert en prosessbeskrivelse av BIA med en rutinebeskrivelse som nå ligger tilgjengelig for alle ansatte i felles dokumentbibliotek, og metodeprodukter utarbeidet i forbindelse med

[1] EBA/GL/2019/04: EBA Guidelines on ICT and security risk management.
[2] BIA – Business Impact Analysis

datainnsamling. Videre at prosjektet har analysert innvirkningen uønskede hendelser eller avbrudd har på forretningsprosesser og hvilken påvirkning det kan ha på organisasjonens evne til å opprettholde forretningskontinuitet, levere tjenester og oppfylle sine forpliktelser.

Finanstilsynet tar styrets svar til etterretning og bekrefter mottak av SMNs BIA.

2.2. Kriseberedskap

I IKT-forskriftens § 11 framgår kravene til at foretaket skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Videre at det minst årlig skal gjennomføres opplæring, øvelse og testing, med dokumentasjon av testresultater, som viser at kriseløsningen virker som forutsatt. Også EBAs retningslinjer for IKT og sikkerhet gir anbefalinger om utarbeidelse av kontinuitetsplaner, respons- og gjenopprettingsplaner, testing og kommunikasjonsplaner ved kriser.

Finanstilsynet pekte i foreløpig rapport på at foretaket selv er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig. Når BIA foreligger må beredskapsplaner oppdateres slik at de samsvarer med risikoene avdekket i analysen. Det er viktig at test av kriseløsningen gjennomføres på foretaksnivå og at foretaket gjør testene til sine egne for å vurdere egnetheten til kriseløsningen og robustheten til organisasjonen. Resultatet skal dokumenteres jf. IKT-forskriftens § 11.

Styret skriver i sitt svar at SMN har etablerte dokumenter knyttet til beredskapsplan for avdeling IT og Sikkerhet, samt kontinuitetsplaner for IKT-området. Videre skriver styret at det er planlagt revisjon av dokumentene og at disse vil sammenfattes til en felles rutine for lokal beredskap og kontinuitet i avdeling IT og Sikkerhet.

Styret skriver også at det hvert år gjennomføres ulike katastrofeøvelser på kriseløsningene i SMN. Det varierer hvilke deler av kriseløsningen som testes, men formålet er å teste at de ulike delene av kriseløsningen har redundans som sikrer at reserveløsninger funger som de skal ved bortfall av de primære tjenestene. Den ferdigstilte BIA for SMN vil i tiden framover brukes til å revidere systemers kritikalitet opp mot funn i BIA for å sørge for at systemer knyttet til viktige forretningsprosesser er identifisert og kategorisert med riktig kritikalitet og videre at beredskapsplaner samsvarer med etablert BIA, inkludert vurdering av testmetoder og testfrekvens for systemer identifisert som samfunnskritiske, virksomhetskritiske eller viktige for foretaket. Videre skriver styret at kravene fra BIA vil bli brukt i kravstilling til leverandører og underleverandører ift. test av kriseløsninger hos disse.

Finanstilsynet tar styrets svar til etterretning.

2.3. Utkontraktering

I henhold til IKT-forskriften § 2 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 foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av samme paragraf 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".

Foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det framgår av bestemmelsen at foretaket 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 det er naturlig at hovedleverandør av IKT-tjenester, er den leverandøren som får størst oppmerksomhet når det gjelder oppfølging av IKT-tjenesteleveranser, men at det er viktig at SMN har rutiner, tilstrekkelig kunnskap og ressurser for oppfølging av alle IKT-tjenesteleverandører med utgangspunkt i de krav SMN har i sine styringsdokumenter og risikovurderinger.

Styret skriver i sitt svar at SMNs viktigste IKT-leverandør har en viktig rolle ift. å følge opp underleverandører av IKT-tjenester levert til SMN. Videre skriver styret at det er et omfattende arbeid hvor det brukes mye ressurser gjennom kravstilling, løpende oppfølgning og kontroller, både på strategisk, taktisk og operativt nivå. Av styrets svar framgår det også at SMN selv følger opp de IKT-leverandører som ikke inngår i hovedavtalen med hovedleverandør.

Finanstilsynet tar styrets svar til etterretning.

Finanstilsynets pekte i foreløpig rapport på at det er viktig at SMN sikrer at krav, blant annet fra sikkerhetspolicyen for den interne organisasjonen, også gjøres gjeldende for leverandører. Finanstilsynet presiserer viktigheten av at SMN må være trygg på at alle leverandører og underleverandører presenterer all informasjon som er nødvendig for å gjennomføre oppfølging av utkontrakterte tjenester. Dette inkluderer at avtaler inneholder tilstrekkelige bestemmelser om innsynsrett for å kunne utøve den nødvendige oppfølgingen av leverandører og underleverandører.

Styret skriver i sitt svar at SMN gjennom avtaler om innsyn, kontroll og revisjon av den utkontrakterte virksomheten sikres juridisk gjennomgang av avtaler i SMNs produktgodkjenningsprosess. Styret skriver videre at SMN vil fortsette å kravstille leverandører på dette området.

Finanstilsynet tar styrets svar til etterretning.

2.4. IKT-sikkerhet

IKT-forskriften § 5 stiller krav om at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det framgår av bestemmelsen at foretaket må sikre at leverandørens aktiviteter kontrolleres. 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.

Finanstilsynet pekte i foreløpig rapport på at foretaket i begrenset grad følger opp leverandører, samt underleverandører, når det kommer til tilgangsstyring, herunder kontroll av leverandørers ansatte og deres tilgang til foretakets systemer.

Styret skriver i sitt svar at SMN utøver utstrakt kontroll av hovedleverandør av IKT-tjenester både på strategisk, taktisk og operativt nivå, herunder at det gis innspill til internrevisjon, oppfølging av kontrollplaner og bestilling av ISAE 3000-rapporter, samt styrerapportering på sikkerhetsområdet, internrevisjonsrapporter og compliance-rapporter. Videre skriver styret at SMNs krav til tilgangsstyring er spesifisert i fellesavtalen, og at oppfølgingsansvaret hos IKT-tjenesteleverandør ligger hos systemforvalter/produkteier som har dette i sine rollebeskrivelser.

I styrets svar vises det til at det for denne type oppfølging alltid vil være forbedringspotensial i måten en følger opp leverandører og underleverandører når det gjelder tilgangsstyring og - kontroll, og at dette er et område som det er oppmerksomhet rundt.

Finanstilsynet tar styrets svar til etterretning.

2.5. Hendelsesrapportering

Operasjonelle hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data skal uten ugrunnet opphold rapporteres til Finanstilsynet, jf. IKT-forskriften § 9 tredje ledd. Foretaket skal rapportere hendelser som foretaket selv kategoriserer som alvorlige eller kritiske, jf. § 9 tredje ledd annet punkt. Foretaket kan videre rapportere andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk. EBAs retningslinjer for IKT og sikkerhet beskriver nærmere hvilke krav som stilles til deteksjonsløsninger og hendelseshåndtering.

Finanstilsynet pekte i foreløpig rapport på at foretaket må sikre at policyer og rutiner for hendelseshåndtering baseres på oppdaterte risikovurderinger. Slike policyer og rutiner bør dokumenteres i tilstrekkelig grad, og gjøres gjeldende både for egne interne systemer og for systemer levert av tjenesteleverandører.

Styret skriver i sitt svar at rutine for IT-hendelser viser foretakets egen håndtering av IKT-sikkerhetshendelser relatert til interne systemer driftet av SMN. Videre skriver styret at SMN har deteksjonsløsninger som er aktive 24/7. I styrets svar står det videre at som et ledd i SMNs videre operasjonalisering av oppfølging av utkontraktert IKT virksomhet vil rutiner oppdateres slik at banken sikrer at dette er tydeliggjort godt nok også for oppfølgning av den utkontrakterte IKT virksomheten.

Finanstilsynet tar styrets svar til etterretning.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.