FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Vipps AS
Postboks 9236 Grønland
0134 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
19/8976			07.09.2020

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IT-tilsyn med betalingstjenesten Vipps i Vipps AS (foretaket) 11. og 12. november 2019. Vipps AS har ansvaret for IKT-virksomheten, også der den er utkontraktert. Tema for tilsynet var å vurdere hvordan Vipps AS styrer og kontrollerer utkontrakteringen til Microsoft (MS) Azure. I dette inngikk også etterlevelse av krav til IKT-sikkerhet.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 4. mars 2020 og styrets kommentarer til rapporten i brev av 30. april 2020.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Forhold knyttet til styring og kontroll med risikoanalysene

Integritet i risikoanalysene

Finanstilsynet viste i foreløpig rapport til at foretakets ulike risikoanalyser samlet framsto som lite klargjørende for hva foretaket vurderte som høyeste risikoer, i dette tilfelle for bruk av MS Azure. Finanstilsynet ba Vipps AS etablere rutiner som sikrer integritet i risikoanalysene.

Finanstilsynet har fra styrets svar merket seg foretakets forklaring på at samme risikoer fremsto ulikt i ulike risikoanalyser, og foretakets tiltak for å sikre samsvar i navngivningen av risikoer i risikoanalyser på operasjonelt nivå og selskapsnivå.

Klargjøring av hva som er akseptabelt nivå på risiko knyttet til informasjonssikkerhet

Finanstilsynet ba i foreløpig rapport foretaket utdype hvordan krav til utviklingshastighet kan påvirke operasjonell risiko, samt redegjøre for ytterligere risikoreduserende tiltak foretaket har iverksatt for å sikre at informasjonssikkerheten håndteres i henhold til foretakets sikkerhetspolicy der det heter at risikoen skal holdes på et akseptabelt nivå.

Finanstilsynet har fra styrets svar merket seg foretakets redegjørelse for hvordan sikkerheten ivaretas i utviklingsprosessen og at foretaket i styremøtet i mars 2020 besluttet kriterier som må være oppfylt for å kunne akseptere risiko i organisasjonen. Kriteriene er nedfelt i en rutine knyttet opp mot standard for operasjonell risikostyring.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf 22 93 97 02

Konsekvensanalyse - Business Impact Analyse (BIA)
Finanstilsynet anbefalte i foreløpig rapport foretaket å bruke en formell BIA som bidrag til riktigere analyser av risiko og bedre kvalitet på kriseløsninger.

Finanstilsynet har fra styrets svar merket seg at foretaket vil gjøre en samlet gjennomgang av behov og forbedringsforslag til risikoanalyser og kriseløsninger, for å se hvilke tiltak som skal prioriteres, inklusiv utarbeidelse av en formell BIA.

Dokumentasjon av valgt teknologisk plattform
På tilsynsmøtet kom det fram at Vipps AS' standarder og rutiner under policy for teknologi var uferdige. Finanstilsynet etterspurte bl.a. strategi for bruk av MS Azure-plattformen, med en beskrivelse av valgt arkitektur basert på ulike MS Azure-komponenter, og hvor Vipps AS sin påvirkning på denne og samspillet mellom kompetanse i Vipps AS og i MS, fremgår.

Fra styrets svar fremgår det at Vipps AS, siden det stedlige tilsynet, har samlet og strukturert eksisterende dokumentasjon slik at styrende dokumenter på teknologi-området i større grad er blitt formalisert og inngår som del av Vipps AS sitt rammeverk for virksomhetsstyring. Finanstilsynet har merket seg at det bl.a. er utarbeidet forbedrede standarder og rutiner for endringsstyring og arkitekturvalg, herunder for teknologisk plattform, og at øvrige sentrale standarder under policy for teknologi er planlagt ferdigstilt innen utgangen av 2020.

Utnyttelse av funksjonalitet i MS Azure
Finanstilsynet ba i foreløpig rapport Vipps AS redegjøre for planlagt ytterligere bruk av tilgjengelige verktøy i MS Azure, for å forbedre kvaliteten på driftsoppfølgingen.

I sitt svar redegjør Vipps AS for bruk av tjenester i MS Azure for drift og overvåking, og for bruk av løsninger fra andre tredjeparter eller egenutviklede verktøy der dette vurderes å gi bedre kontroll med og kvalitet på driftsoppfølgingen. Finanstilsynet har fra Vipps AS sin redegjørelse merket seg at det, på grunn av avhengigheten til norsk betalingsinfrastruktur, er avgjørende at Vipps selv har best mulig kontroll på de tekniske verdikjedene mellom Vipps og sentrale underleverandører av tjenester. Finanstilsynet har videre merket seg at Vipps AS i etterkant av tilsynet har etablert et eget team, dedikert til å følge opp alle varslinger og anbefalinger i Azure Security Center, som er et produkt basert på beste praksis og standarder MS følger globalt.

Forhold knyttet til styring og kontroll med kommunikasjon av sikkerhetskrav til MS Azure og oppfølging av leverandørens etterlevelse
Finanstilsynet ba i foreløpig rapport Vipps redegjøre nærmere for hvordan Vipps AS sikrer at endringer/oppdateringer i Vipps AS sine sikkerhetskrav avklares, reflekteres i og etterleves på MS Azure-plattformen.

Fra styrets svar har Finanstilsynet merket seg at Vipps AS fra og med 2020 i alle risikovurderinger, inklusiv den årlige risikovurderingen for MS Azure, vurderer hvilke sikkerhetstiltak leverandøren og Vipps har implementert knyttet til leveransen. Finanstilsynet har merket seg foretakets redegjørelse for hvordan Vipps AS følger opp at MS Azure etterlever eget sikkerhetsrammeverk og

for hvordan Vipps AS følger opp at endringer i Vipps AS sitt sikkerhetsrammeverk ivaretas i MS Azure sitt sikkerhetsrammeverk.

Finanstilsynet tar dette til etterretning og ber Vipps AS sikre kontinuerlig oppmerksomhet på dette området.

Forhold knyttet til styring og kontroll av tredjepartsvurderinger av MS Azure
Finanstilsynet viste i foreløpig rapport til at Finanstilsynet forventer at Vipps AS gjør selvstendige vurderinger av funn i rapporter fra tredjepartsvurderinger av MS Azure.

Finanstilsynet har merket seg fra styrets svar, at foretaket i alle risikovurderinger fra og med 2020 vil ta med foretakets vurdering av leverandørens revisjonsrapporter, egenevalueringer og sertifiseringer. I tillegg vil foretaket følge opp eventuelle funn avdekket i rapportene, og iverksette kompenserende tiltak, f.eks. en selvstendig revisjon av MS Azure.

Oppfølging av funn i Disaster Recovery-test (DR-test)
Finanstilsynet ba i foreløpig rapport Vipps AS redegjøre for hvordan foretaket vil følge opp funn fra DR-test gjennomført høsten 2019 og om planer for fremtidige DR-tester.

Finanstilsynet har fra styrets svar merket seg at Vipps har fulgt opp funnene fra DR-testen i 2019, slik at disse ble lukket i forkant av, og verifisert i orden i, ny DR-test som ble gjennomført i mars 2020.

Finanstilsynet ber om å få oversendt rapporten etter DR-testen i 2020 innen 15. oktober 2020.

Kopi av tilsynsrapporten bes sendt intern og ekstern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Åshild Johnsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.