UAVHENGIG GJENNOMGANG - STYRING OG KONTROLL AV UTKONTRAKTERING I NORGES BANK

7. mars 2024

BDO
tett på

INNHOLDSFORTEGNELSE

Introduksjon

1. Innledning

1.1 Bakgrunn

Utkontraktering kan medføre økt operasjonell risiko og utfordre styring og kontroll i virksomheten. Norges Banks representantskap (representantskapet) har, etter innspill fra Finansdepartementet, besluttet å gjennomgå styring, kontroll og oppfølging av utkontraktert virksomhet i Norges Bank. Gjennomgangen omfatter både sentralbankvirksomheten (SBV) og Norges Bank Investment Management (NBIM).

Tilsynssekretariatet har, på vegne av representantskapet, engasjert BDO AS (BDO) til å gjennomføre en uavhengig vurdering av styring, kontroll og oppfølging av utkontraktering i Norges Bank. BDO har derfor gjennomført en uavhengig vurdering av Norges Banks rammeverk og prosesser for, og rapportering om, risikostyring og internkontroll ved utkontraktering. Vurderingen skal gi en beskrivelse av om Norges Bank har etablert et hensiktsmessig og effektivt rammeverk for styring og kontroll med utkontraktering i tråd med krav og forventninger.

Gjennomgangen omfatter en vurdering i to deler: Del 1 – styring og kontroll av utkontraktering i Norges Bank (generelt) og Del 2 – styring og kontroll med utkontraktering av depottjenester til den globale depotbanken Citibank N.A. (Citibank). Vår gjennomgang er oppsummert i denne rapporten, hvor observasjoner, vurderinger og anbefalinger følger i kapittel 2 for Del 1 og kapittel 3 for Del 2.

1.2 Formål og metode

Det overordnede formålet med gjennomgangen er å gi representantskapet en uavhengig vurdering av om Norges Bank har etablert et hensiktsmessig og effektivt rammeverk for styring og kontroll med utkontraktering i samsvar med krav og forventninger. Videre blir NBIMs styring, kontroll og oppfølging av den globale depotbanken for internasjonale betalinger samt avregning og deponering av verdipapirer, Citibank, vurdert opp mot etablert rammeverk.

Oppdragsbeskrivelsen henviser til §§ 5, 6, 7 og 8 i «instruks for risikostyring og internkontroll i Norges Bank» og § 1-8 i «mandat for forvaltningen av Statens pensjonsfond utland (SPU)». Disse instruksene danner et viktig utgangspunkt for vurdering av styring og kontroll med utkontraktering i Norges Bank. Begge disse dokumentene er særdokumenter for Norges Bank og benyttes som grunnlag for vår uavhengige vurdering. I tillegg, for å oppnå innspill til beste praksis basert på en norm for banker og andre finansforetak, har vi vurdert det som hensiktsmessig å legge Finanstilsynets veiledning for utkontraktering til grunn for vurderingene (Rundskriv 7/2021). Rundskrivet gir klare føringer for hvordan foretak skal sikre nødvendig styring og kontroll av utkontrakterte tjenester for å redusere den operasjonelle risikoen. Rundskrivet definerer gode prinsipper for risikostyring og internkontroll i en strengt regulert bransje, og gir klare føringer for hvordan en virksomhet kan styre og kontrollere den operasjonelle risikoen knyttet til utkontrakteringen.

Videre er retningslinjer fra det europeiske banktilsynet, EBA guidelines on outsourcing arrangements (EBA/GL/2019/02), lagt til grunn for å gi Norges Bank ytterligere innspill og anbefalinger for videreutvikling av eksisterende rammeverk og praksis.

Overordnede målekriterier som er lagt til grunn for vår vurdering er:

1. §§ 5, 6, 7 og 8 i instruks for risikostyring og internkontroll i Norges Bank
2. § 1-8 i mandat for forvaltningen av Statens pensjonsfond utland (SPU)
3. EBA guidelines on outsourcing arrangements (EBA/GL/2019/02)
4. Finanstilsynets veiledning for utkontraktering (Rundskriv 7/2021)
5. Forskrift om IKT-systemer i banker mv, § 12 (IKT-forskriften)

Disse er videre utledet til følgende tema som vurderes i Del 1 og Del 2:

1. Rammeverk for styring og kontroll av utkontraktering med særlig fokus på:
   - Organisering, roller og ansvar
   - Styrende dokumenter

2. Utkontrakteringsprosessen, med særlig fokus på:
   - Risikovurderinger
   - Oppfølging av leverandører.

1.3 Fremgangsmåte

1.3.1 Omfang

I den første delen av rapporten har vi, med utgangspunkt i paragrafene og beskrivelsen i kapittel 1.2, vurdert Norges Banks styring, kontroll og oppfølging med utkontraktering i sentralbankvirksomheten (SBV) og Norges Bank Investment Management (NBIM). I del to av rapporten har vi, med utgangspunkt i paragrafene og beskrivelsen i kapittel 1.2, spesifikt vurdert Norges Banks styring, kontroll og oppfølging med den globale depotbanken for internasjonale betalinger samt avregning og deponering av verdipapirer, Citibank.

1.3.2 Utvalg

I del 2 av oppdraget blir Citibank spesifikt vurdert. I del 1 av oppdraget har BDO i tillegg gjort en spesifikk vurdering av et utvalg av leverandører:

- **Intility** er leverandør av plattform for virksomhetskritiske systemer (PVS) for SBV.
- **Orange Business Services** er leverandør av plattform for samfunnskritiske systemer (PSS) for SBV.
- **Amazon Web Services** (AWS) er leverandør av plattformtjenester for NBIM.

BDO vurderer at utvalgte utkontrakterte tjenester er hensiktsmessige for å uttale seg om, samt vurdere, Norges Banks styring, kontroll og oppfølging av utkontrakterte operasjonelle tjenester ettersom disse er av høy kritikalitet for banken og omfatter både SBV og NBIM.

1.4 Avgrensninger og forbehold

Gjennomgangen inkluderer en vurdering av Norges Banks styring, kontroll og oppfølging av utkontraktering. For å gjennomføre en helhetlig vurdering av bankens utkontraktering har BDO lagt til grunn de målekriteriene som er beskrevet i kapittel 1.2. I tillegg er etterlevelse av kriteriene testet gjennom vurdering av informasjon fra møter og intervjuer samt fremlagt dokumentasjon og utvalgte avtaler.

Vi ønsker å understreke at vår gjennomgang ikke inkluderer en juridisk vurdering av underliggende avtaleverk. Vi har heller ikke vurdert kvaliteten i kravspesifikasjonen når det gjelder tekniske, funksjonelle eller organisatoriske krav knyttet til spesifikke løsninger eller tjenesteleveranser.

1.4.1 Anskaffelser, utkontraktering og tjenestekjøp i Norges Bank

Rapporten inkluderer begreper som utkontrakteringer, anskaffelser og tjenestekjøp, og det er behov for en presisering av de ulike begrepene.

Begrepet anskaffelser benyttes i anskaffelsesloven og omfatter vare-, tjeneste-, bygg- og anleggskontrakter med en anslått verdi på 100.000 norske kroner eller mer.

I henhold til rundskriv 7/2021 fra Finanstilsynet foreligger utkontraktering når foretaket velger å la en annen juridisk enhet utføre oppgaver på vegne av foretaket. Ut ifra denne beskrivelsen legger vi til grunn at betegnelsen «utføre oppgaver» tilsvarer begrepet anskaffelse av tjenester i anskaffelsesloven. Videre forutsetter vi at disse oppgavene utføres *på vegne av* Norges Bank, og at Norges Bank dermed har et særskilt styrings- og kontrollbehov for å sikre tilstrekkelig leveransekvalitet, både på etableringstidspunktet og over tid.

I dialog med tilsynssekretariatet har vi avklart at vi legger til grunn at anskaffelse av tjenester, tjenestekjøp og utkontraktering er likeverdige begrep i denne gjennomgangen, så lenge:

- anskaffelser dreier seg om tjenestekjøp
- at tjenestekjøpet har som hovedoppgave å utføre oppgaver på vegne av Norges Bank og;
- at Norges Bank har et særskilt behov for styring og kontroll før, under og ved avslutning/avvikling av tjenesteleveransen.

Der begrepet utkontraktering er benyttet vil dette dekke alle disse forholdene.

1.4.2 Eksterne forvaltere i SPU

I oppdragsbeskrivelsen fra tilsynssekretariatet er det beskrevet at vurderingen ikke skal omfatte Norges Banks bruk av eksterne forvaltere. Derfor er § 1-8 (3) i «mandatet for forvaltningen av Statens pensjonsfond utland (SPU)» utelatt som grunnlag for vår gjennomgang.

1.4.3 Depotordning for oppbevaring av statsobligasjoner og -sertifikater (valutareservene)

Del 2 av oppdraget omfatter en gjennomgang og vurdering av de globale depottjenestene som NBIM benytter, og som er tjenesteutsatt til Citibank. Sentralbankvirksomheten har i tillegg en depotordning hos syv utvalgte sentralbanker for oppbevaring av statsobligasjoner og -sertifikater som er en del av valutareservene som Norges Bank forvalter etter sentralbankloven § 3-2. Disse er ikke en del av vår uavhengige vurdering.

1.4.4 Lov om offentlig anskaffelser

Norges Bank skal følge lov om offentlig anskaffelser av 17. juni 2016 nr. 73 (LOA) samt forskrift av 12. august 2016 nr. 974 om offentlige anskaffelser (FOA). BDOs gjennomgang skal ikke betraktes som et tilsyn av anskaffelsesregelverket og etterlevelsen av dette. De målekriteriene som legges til grunn i vår vurdering er derfor ikke direkte knyttet til LOA og FOA.

Sammendrag

Sammendrag av rapporten

Innledning

Utkontraktering kan medføre økt operasjonell risiko og utfordre styring og kontroll i virksomheten. BDO AS har på oppdrag for Norges Banks representantskap gjennomført en uavhengig vurdering av styring, kontroll og oppfølging av utkontraktering i Norges Bank. Gjennomgangen omfatter spesifikke vurderinger av utkontraktering både i sentralbankvirksomheten (SBV) og i Norges Bank Investment Management (NBIM). I tillegg har vi vurdert overordnet styring, kontroll og oppfølging basert på felles bestemmelser for begge virksomhetsområdene. Gjennomgangen er utført i perioden desember 2023 – februar 2024.

Vår vurdering av Norges Banks arbeid med utkontraktering er basert på sentrale krav og forventninger forankret i de grunnleggende dokumentene «Instruks for risikostyring og internkontroll i Norges Bank» samt «Mandat for forvaltning av Statens pensjonsfond utland». Begge disse dokumentene er særskilt utarbeidet for Norges Bank. For innspill til beste praksis basert på en norm for bank- og finansbransjen, har vi i tillegg lagt Finanstilsynets veiledning for utkontraktering (Rundskriv 7/2021) til grunn for våre vurderinger. For ytterligere innspill har vi også sett hen til European Banking Authority (EBA) sine Guidelines on Outsourcing Arrangements (EBA/GL/2019/02).

Metodene vi har lagt til grunn for våre konkrete vurderinger og anbefalinger omfatter:

- Analyse og vurdering av et utvalg styrende dokumenter
- Intervju med nøkkelpersoner fra begge virksomhetsområdene
- Gjennomgang av fire eksisterende avtaler om utkontraktering i Norges Bank. Tre av avtalene ble identifisert som relevante for nærmere vurderinger i løpet av prosjektet, mens én avtale, avtale om globale depottjenester, var spesifisert i oppdragsbeskrivelsen.

I henhold til oppdraget er rapporten inndelt i to hoveddeler:

Del 1 – Vurdering av Norges Banks rammeverk for styring, kontroll og oppfølging med utkontrakterte tjenester for både SBV og NBIM.

Del 2 – Vurdering av Norges Banks styring, kontroll og oppfølging med den globale depotbanken for internasjonale betalinger samt avregning og deponering av verdipapirer (Citibank N.A.).

Gjennomgangen viser at både SBV og NBIM har et betydelig fokus på styring, kontroll og oppfølging knyttet til utkontraktering av tjenester. Vi har imidlertid identifisert enkelte områder hvor Norges Bank kan vurdere å forbedre sitt rammeverk og praksis ved utkontraktering. Observasjoner og anbefalinger for begge virksomhetsområdene, samt felles rammeverk for utkontraktering, oppsummeres nedenfor.

Felles rammeverk for utkontraktering for SBV og NBIM

Norges Bank har etablert et rammeverk for styring, kontroll og oppfølging av utkontrakterte tjenester på tvers av begge virksomhetsområdene (SBV og NBIM), jfr. Prinsipper for risikostyring og interkontroll i Norges Bank. Rammeverket er utformet med prinsipper fastsatt av hovedstyret og videre operasjonalisert i virksomhetsområdene gjennom ulike policyer og retningslinjer, samt andre understilte dokumenter. Vi vurderer således det overordnede rammeverket i hovedsak som hensiktsmessig. Gjennomgangen har imidlertid avdekket enkelte områder som banken bør vurdere å styrke.

Det er viktig å gjennomføre grundige risikovurderinger både før avtaleinngåelse og ved løpende oppfølging av oppdragstaker. Gjennomgangen indikerer at Norges Bank sitt felles rammeverk for utkontraktering i begrenset grad spesifiserer krav knyttet til helhetlig risikovurdering og tiltak for risikoreduksjon. For å sikre tilstrekkelig gjennomføring av risikovurderinger, bør banken vurdere å presisere ytterligere krav til innhold i risikovurderingene og hvilke interne ressurser som har ansvaret for gjennomføringen. Vi observerer imidlertid at begge virksomhetsområdene hensyntar risikovurderinger gjennom kravspesifikasjon som underlag til kontrakt og i oppfølgingsaktiviteter i løpet av kontraktsperioden.

Norges Bank sitt rammeverk for utkontraktering kan i større grad inkludere retningslinjer knyttet til vurdering av oppdragstakers underleverandør(er). Gjennomgangen viser at det formelle ansvaret i stor grad er plassert hos oppdragstaker. Underleverandører kan potensielt påvirke ulike risikoelementer hos Norges Bank, slik som operasjonell- og omdømmerisiko. Vurdering av risiko forbundet med underleverandører bør derfor fremkomme tydeligere i rammeverket selv om ansvaret avtalerettslig er lagt hos oppdragstaker.

Ved utkontraktering bør Norges Bank vurdere risikoer og muligheter for å reintegrere tjenesteleveransen i egen organisasjonen og/eller overføring til andre leverandører uten at det påfører betydelige forstyrrelser i driften. Vi anbefaler at banken etablerer retningslinjer som sikrer at risikovurderingene omfatter slike muligheter og exit-strategier.

Utkontraktering i SBV

Gjennomgangen av anskaffelsesprosessen knyttet til utkontraktering i SBV viser at de ulike stegene er godt støttet av funksjonalitet og arbeidsflyt i bankens serviceportal. Det er vår vurdering at systemflyten sikrer en god oversikt knyttet til overordnet utvikling i prosessen. Videre vurderer vi at retningslinjene og rutinene ikke i tilstrekkelig grad beskriver krav til underliggende aktiviteter for de ulike stegene i serviceportalen. For å sikre at det foreligger tydelige retningslinjer, kan banken spesifisere minimumskrav knyttet til vurderinger som skal gjennomføres i de ulike stegene og hvordan disse skal dokumenteres. Videre observerer vi at serviceportalen inkluderer prosessen frem til anskaffelse, men mangler ytterligere trinn for oppfølging av oppdragstaker gjennom kontraktsperioden.

For å sikre god styring og kontroll med utkontrakteringer, er det viktig at det gjøres grundige risikovurderinger for å utforme krav i kontrakter og oppfølgingsaktiviteter overfor oppdragstaker. Nylig etablerte retningslinjer for leverandøroppfølging i SBV angir krav til oppfølging basert på kritikalitet og tilrettelegger for oppfølging av leverandør basert på risikovurdering etter at kontrakt er inngått. Disse endringene vurderer vi som positive. Det er imidlertid viktig at retningslinjene operasjonaliseres gjennom mer utfyllende rutiner.

Gjennomgangen av utkontrakteringsprosessen for Intility og Orange Business Services viser at SBV anvender standardiserte kriterier for risikovurderinger i anskaffelsesprosessen av utkontraktering, selv om dette i mindre grad er definert i styrende dokumenter. Videre viser gjennomgangen at den operasjonelle oppfølgingen av tjenesteleveransene underveis i kontraktsperioden er godt organisert og gjennomført. Det er definert en organisasjon for forvaltning og oppfølging av avtalene både på leverandørenes side og hos SBV, og det er også etablert målekriterier. Vi ser derimot at oppfølgingen gjøres innenfor ulike avdelinger i SBV, og at det ikke er en samlet koordinering og oppfølging av risikoer knyttet til leverandørene og tjenesteleveransene på tvers av SBV.

Vi oppfatter at oppfølgingskrav og aktiviteter er sterkt knyttet til tjenesteleveransene, og mindre knyttet til oppfølging av oppdragstaker som leverandør. Gjennomgangen viser at rammeverket har flere punkter som tematiserer virksomhetsstyring, men at kravene ikke er tydelige nok for å sikre en tilstrekkelig helhetlig vurdering.

Utkontraktering i NBIM

NBIM har i hovedsak etablert hensiktsmessige prosesser for å identifisere, vurdere og håndtere risiko som oppstår ved utkontraktering. Disse prosessene er operasjonalisert gjennom et detaljert rammeverk. I nylig etablerte retningslinjer for oppfølging av leverandører er det lagt til rette for en risikobasert og helhetlig tilnærming til styring, kontroll og oppfølging av utkontraktering som ivaretar de forskjellige fasene i prosessen. Retningslinjene tydeliggjør ansvarsfordelingen blant nøkkelfunksjoner i NBIM, samtidig som det stilles krav til ulike aktiviteter som skal gjennomføres og dokumenteres i forskjellige faser. Dette forankres av en overordnet prosessbeskrivelse som følger livssyklusen til tjenesteleveransen(e).

Gjennomgangen viser at NBIMs styrende dokumenter i større grad kan tydeliggjøre ansvar som ligger hos stab- og støttefunksjoner ved utkontraktering. En slik presisering bør synliggjøre hvilke funksjoner som skal involveres i de ulike fasene i utkontrakteringsprosessen.

Vi observerer mangelfulle rutiner, retningslinjer og krav knyttet til scenarioanalyser for potensielle operasjonelle hendelser ved mislykkede eller utilstrekkelige ytelser fra oppdragstaker. Vi anbefaler derfor at frekvensen for simulering av slike scenarioanalyser, samt kravene til innhold i gjennomgangene, blir definert i NBIMs rammeverk for utkontraktering.

Gjennomgang av utkontrakteringsprosessen for Amazon Web Services (AWS) viser at NBIM i stor grad etterlever krav og retningslinjer fastsatt i rammeverk for utkontraktering. Det er tydelig identifisert hvilke interne ressurser i NBIM som innehar ulike ansvarsområder knyttet til AWS-avtalen. Videre er det etablert en kjernegruppe som inkluderer nøkkelpersoner med ulik spesialkompetanse, med formål om å sikre hensiktsmessig samarbeid mellom AWS og NBIM. Vi observerer også en god praksis knyttet til identifisering og implementering av risikoreduserende tiltak, samt en grundig prosess for løpende oppfølging av disse tiltakene med oppdragstaker.

Utkontraktering av depottjenester til Citibank N.A.

NBIM har inngått kontrakt med Citibank N.A. (Citibank) for leveranse av globale depottjenester i de markeder fondet investerer (i børsnoterte verdipapirer). De styrende dokumentene for NBIM legger også føringer for utkontraktering av depottjenestene, og definerer tydelige roller og ansvar, og ulike faser gjennom livsløpet. Siden depottjenestene er definert med det høyeste kritikalitetsnivået (svært høy), er det stilt omfattende krav til utkontrakteringen for å håndtere den operasjonelle risikoen gjennom hele livssyklusen. NBIM har som følge av dette etablert detaljerte prosesser, rutiner og kontrollaktiviteter som en del av overvåkings- og oppfølgingsprosessen av tjenesteleveransene, og av Citibank som leverandør. Dette er nøye regulert gjennom avtalen med Citibank.

Citibank benytter underleverandører, blant annet lokale depotbanker, for depottjenestene som leveres til NBIM. Citibank har ansvaret for oppfølging av sine underleverandører og påtar seg ansvaret for eventuelle tap NBIM måtte lide ved hendelser hos disse. NBIM overvåker de prosessene som Citibank selv har etablert for oppfølging av underleverandører. I tillegg foretar NBIM risikovurderinger av de viktigste lokale depotbankene som benyttes av Citibank og følger opp kvaliteten på tjenestene. Når det gjelder øvrige underleverandører som Citibank benytter, utover de lokale depotbankene, er det ikke stilt særskilte krav til disse i avtalen. Dette kan eksempelvis være underleverandører som leverer applikasjoner og IT-infrastruktur til Citibank, og som benyttes i utøvelsen av tjenesteleveransen. Det er vår vurdering at NBIM i større grad bør dokumentere vurderinger av risiko forbundet med underleverandører, ut over de lokale depotbankene, og om det er scenarioer som kan medføre konsekvenser for NBIM som ikke vil dekkes gjennom avtalen med Citibank, eksempelvis relatert til omdømmetap.

Ved brudd på definerte krav i utkontrakteringsavtalen med Citibank har NBIM mulighet til å iverksette en exit-strategi og overgang til en beredskapsløsning. Fornyet beredskapsløsning er etablert hos Bank of New York (BNY) Mellon fra 01.01.2024, og det er planlagt øvelser sammen med Citibank, BNY Mellon og NBIM i løpet av 2024 for å teste evne til gjenoppretting av depottjenestene ved en eventuell krise.

Utover punktet knyttet til oppfølging av underleverandører vurderer vi at NBIM har etablert hensiktsmessig styring, kontroll og oppfølging av utkontrakteringen av depottjenestene, og at utkontrakteringen er gjennomført og overvåket på en effektiv måte gjennom hele livssyklusen fra anbudsprosess, gjennom kontraktsperioden og til definerte exit-strategier.

Oppsummert vurdering

Det er vår vurdering at styring, kontroll og oppfølging av utkontraktering i Norges Bank i all hovedsak samsvarer med målekriteriene for denne gjennomgangen. Banken har etablert et hensiktsmessig rammeverk for utkontraktering gjeldende for begge virksomhetsområdene. Vi ønsker spesielt å trekke frem NBIMs rammeverk for leverandøroppfølging «Provider lifecycle management», som vurderes som hensiktsmessig for å sikre god styring og kontroll.

Vi har identifisert enkelte områder der banken kan forbedre sitt rammeverk for utkontraktering, spesielt med hensyn til kvalitet og struktur i bankens styrende dokumenter.

Testing av etterlevelsen av bankens eget rammeverk for utvalgte utkontrakterte tjenester viser en hensiktsmessig praksis med betydelig fokus på oppfølging av tjenesteleveransen i kontraktsperioden, både i SBV og NBIM. Vi har identifisert forbedringspotensial knyttet til bankens praksis for vurderinger av oppdragstakers virksomhetsstyring, vurderinger av underleverandører samt dokumentasjon av vurderinger knyttet til terminering av utkontrakteringsavtaler (exit-strategier).

Del 1: Styring, kontroll og oppfølging

2. Del 1: Styring og kontroll av utkontraktering

2.1 Overordnet styring og kontroll av utkontraktering i Norges Bank

2.1.1 Observasjoner og vurderinger

Bakgrunn

Norges Bank har et overordnet rammeverk for styring og kontroll av utkontraktering som er grunnleggende og retningsgivende for både SBV og NBIM. Hovedpilarene i det overordnede rammeverket er organisering av funksjoner og styrende dokumenter som beskriver overordnede forventninger og krav til bankens arbeid med utkontraktering.

Organisering, roller og ansvar

Norges Bank er tydelig organisert i to virksomhetsområder; sentralbankvirksomheten (SBV) og Norges Bank Investment Management (NBIM). Hvert av disse områdene har langt på vei et selvstendig ansvar for styring og kontroll av utkontraktering, men noen roller og oppgaver er lagt på overordnet nivå, og er felles for begge områdene. Dette er hovedsakelig samlet i Norges Bank Administrasjon (NBA) i sentralbankvirksomheten hvor enkelte fellesfunksjoner ivaretas.

I bankens retningslinjer for anskaffelser er det beskrevet to sentrale roller i utkontrakteringsprosessen som gjelder på et overordnet nivå og som er felles for SBV og NBIM. Disse rollene er behovseier og prosessansvarlig for anskaffelser. Rollen som behovseier utøves av linjeansvarlig, enten fra SBV eller NBIM. Prosessansvarlig for anskaffelser ivaretas av den sentrale anskaffelsesfunksjonen, Procurement. Denne funksjonen befinner seg i SBV under Norges Bank Administrasjon, Finance, men er definert som anskaffelsesstøtte også for NBIM.

Retningslinjene definerer ansvarsområder for begge rollene. Disse er i stor grad i tråd med beste praksis og underbygger bankens mål om effektive anskaffelser. Det er imidlertid identifisert avvik fra beste praksis på noen områder.

Vi ser ikke at rollen som prosessansvarlig innebærer et tydelig ansvar for å sørge for at virksomhetsstyringen hos leverandører og eventuelle underleverandører blir vurdert. I samfunnet generelt øker forventningene til gjennomføring av slike vurderinger, f.eks. generelle krav til bærekraft eller spesifikke krav til håndtering av potensielle habilitets- eller interessekonflikter, personvern, anti-hvitvasking og anti-korrupsjonsarbeid, arbeidstakerrettigheter hos leverandører eller klimaavtrykk. En slik selskapsvurdering krever mer og mer spesialkompetanse og et særskilt ansvar i anskaffelsesfunksjonen er nærliggende.

I tillegg til rollene som behovseier og prosessansvarlig har samtaler med banken og bestemmelser fra andre styrende dokumenter vist at ytterligere funksjoner trekkes inn i utkontrakteringsprosesser, slik som Legal, IT-sikkerhet og Security & Crisis Management for risikovurderinger eller rollen som avtaleeier for leverandøroppfølging. Vi vurderer dette som hensiktsmessig, da det tilfører prosessen verdifull kompetanse. Samtidig vurderer vi det som en svakhet at andre relevante roller og prinsipper for deres samspill med

behovseier og prosessansvarlig ikke defineres nærmere i bankens øverste styrende dokumenter.

Styrende dokumenter for utkontraktering

Styrende dokumenter er vesentlige for å synliggjøre bankens forventninger og krav til styring og kontroll av utkontrakteringsprosesser. Banken har flere styrende dokumenter som til sammen utgjør et rammeverk for styring og kontroll. Følgende dokumenter har blitt oversendt som fellesdokumenter for SBV og NBIM og som vi vurderer som styrende dokumenter for utkontraktering på overordnet nivå:

- *Prinsipper for risikostyring og internkontroll i Norges Bank*
- *Retningslinjer for anskaffelser til Norges Bank*

I tillegg har vi tatt hensyn til dokumentet «instruks for risikostyring og internkontroll i Norges Bank».

Legger vi rundskrivet fra Finanstilsynet for utkontraktering til grunn, tilsier beste praksis at banken skal ha bestemmelser knyttet til

- Styring og kontroll
- Risikovurderinger
- Gjennomføring av utkontrakteringsprosessen
- Oppfølging av utkontraktering

Etter vår vurdering fastsetter de nevnte dokumentene noen viktige grunnleggende prinsipper for styring og kontroll av utkontrakteringer i Norges Bank. Prinsippene bidrar til en felles grunnleggende tilnærming til utkontraktering i SBV og NBIM.

Sammenlikner vi disse dokumentene med grunnleggende krav til utkontraktering i Finanstilsynets rundskriv, er de i tråd med forventningene om et styregodkjent og regelmessig oppdatert grunnleggende rammeverk. Det samme gjelder kravet fra Finanstilsynet om å definere ansvarlige for utkontrakteringen og for etterlevelse av retningslinjer. Banken har også fastlagt krav om habilitet i sine retningslinjer for anskaffelser. Dette er i tråd med beste praksis. Fordi dette er et område hvor det kan forekomme misforståelser når det gjelder konkret betydning av habilitet, kunne banken ha styrket retningslinjene for anskaffelser ytterligere dersom dokumentet hadde inneholdt en henvisning til bankens øvrige dokumenter som beskriver dette nærmere.

Rundskrivet krever at det klargjøres hvem som har ansvar for at nødvendige risikovurderinger gjøres og at risikoreduserende tiltak identifiseres og gjennomføres. Vi ser ikke at de to ovennevnte styrende dokumentene tydeliggjør forventninger og krav om dette. Utover å fastholde at risikostyring og internkontroll skal ivaretas ved utkontraktering, finner vi ikke noen videre beskrivelse av overordnede prinsipper om hva dette innebærer eller andre former for minimumskrav til kvalitet. I henhold til rundskrivet stilles det også krav til vurdering av risikoreduserende tiltak, og en vurdering av muligheter for å terminere avtalen uten at det skaper vesentlige forstyrrelser for banken gjennom bytte av leverandør, eller overføring av oppgavene tilbake til banken. Vi ser ikke at banken har formulert noen grunnleggende prinsipper knyttet til disse punktene.

Finanstilsynets rundskriv forventer at banker og finansinstitusjoner definerer hvordan utkontraktert virksomhet skal følges opp og overvåkes, samt hvilke rapporterings- oppfølgings- og kontrolltiltak som skal vurderes. De overordnede dokumentene fastholder at Norges Bank forventer at operasjonell risiko skal ivaretas i hele livsløpet til løsningen eller tjenesten, og at internkontroll skal være mulig. Vi vurderer likevel bestemmelsene som noe svake, da vi ikke ser at banken formulerer grunnleggende prinsipper for oppfølging av utkontraktering. Vi savner også overordnede bestemmelser knyttet til minimumskrav som stilles til rapporterings- og kontrolltiltak, eksempelvis hvordan omfang og kompleksitet av utkontrakteringen skal spille en rolle for oppfølgingen, krav om

vurdering av leverandørens selskapsstyring i tillegg til selve løsningen eller tjenesten som skal leveres og grunnleggende prinsipper om dokumentasjon av vurderinger og beslutninger.

For nærmere vurderinger relatert til utkontrakteringsprosessen viser vil til beskrivelsene i kapittel 2.2 og 2.3 nedenfor om utkontrakteringsprosessen for henholdsvis SBV og NBIM. Vi gjør også oppmerksom på at manglende eller ufullstendige bestemmelser i bankens overordnede dokumenter sammenliknet med krav og forventninger i Finanstilsynets rundskriv er vurdert som en svakhet, uavhengig av om bestemmelser er inkludert på et lavere nivå i bankens dokumenthierarki. Dette fordi vi ser det som vesentlig for bankens fokus og kvalitet i arbeidet at bankens overordnede dokumenter forankrer tydelige styringsprinsipper, krav og forventninger.

2.1.2 Anbefalinger

For å styrke bankens styring og kontroll med utkontraktering, anbefaler vi

- å videreutvikle rolleforståelsen når det gjelder prosessansvarlig for anskaffelser. Her har vi særlig pekt på behovet for å inkludere ytterligere bestemmelser knyttet til
  - ansvar for å sørge for en grundigere vurdering av leverandørers og eventuelt underleverandørers virksomhetsstyring
  - øvrige roller i utkontrakteringsprosessen og deres samspill med rollene behovseier og prosessansvarlig

- å styrke styrende fellesdokumenter vedrørende utkontraktering for banken ytterligere. Vi peker særlig på behovet for:
  - nærmere presisering av ansvar for gjennomføring av risikovurderinger og vurdering av behov for risikoreduserende tiltak.
  - å definere overordnede prinsipper for eller minstekrav til risikovurderinger knyttet til utkontraktering. Her vil det blant annet være viktig å inkludere krav til
    - Vurdering av risiko knyttet til leverandørens virksomhetsstyring. I denne sammenhengen kan det være relevant å se til krav til vurderinger i tråd med den norske anbefalingen om eierstyring og selskapsledelse fra Norsk utvalg for eierstyring og selskapsledelse, OECDs nylige oppdaterte retningslinjer for flernasjonale selskaper, åpenhetsloven og/eller forventninger til leverandøroppfølging i EUs ulike lovkrav for bærekraftsrapportering.
    - Vurdering av risiko knyttet til terminering av kontrakten, f.eks. mulighet for overføring til en annen leverandør eller inkorporering i egen drift.
  - å definere overordnede prinsipper for oppfølging, rapportering og kontrolltiltak utover å slå fast at utkontrakteringen skal omfattes av internkontroll.
  - å fastlegge prinsipper knyttet til hvilke beslutninger og vurderinger som skal dokumenteres når og hvor i utkontrakteringsprosessen.

2.2 Styring og kontroll av utkontraktering i SBV

2.2.1 Observasjoner og vurderinger

Bakgrunn

Vår gjennomgang omfatter sentralbankvirksomhetens (SBV) styrende dokumenter, organisatoriske strukturer, samt en evaluering av SBVs prosess for utkontraktering og risikovurdering av tjenesteleveranser. Videre har vi vurdert hvordan rammeverket for utkontraktering legger til rette for løpende oppfølging av oppdragstakere gjennom hele kontraktsperioden.

SBV har ansvaret for å operasjonalisere de overordnede retningslinjene for utkontraktering for å sikre et hensiktsmessig rammeverk og god styring og kontroll med egen utkontraktering. Dette ansvaret er ivaretatt gjennom utarbeidelse av en rekke styrende dokumenter som er særskilt utarbeidet for SBV.

Organisering, roller og ansvar

SBV forholder seg til det overordnede rammeverket som gjelder for Norges Bank samt organisering, roller og ansvar som beskrevet i kapittel 2.1.1. Sentralbanksjefen har det overordnede ansvaret for implementering av prinsipper og retningslinjer som hovedstyret har vedtatt.

Videre har SBV en egen retningslinje, «Ufyllende retningslinjer for styring av operasjonell risiko» som fastslår at avtaleeier er ansvarlig for å innhente risikovurderinger knyttet til internkontroll fra leverandører med høy eller svært høy kritikalitet. Rollen som avtaleeier defineres i det nye dokumentet «Retningslinjer for leverandøroppfølging» som ble vedtatt i januar 2024. Der beskrives også kriterier for vurdering av om tjenesten er av høy eller svært høy kritikalitet. Det ser ikke ut til å være henvisninger mellom de to nevnte retningslinjene, noe som vil være viktig for å sikre korrekt forståelse av begrepene.

Styrende dokumenter for utkontraktering

SBV følger overordnede prinsipper fastsatt av hovedstyret. Primært er disse prinsippene konkretisert gjennom dokumentet «retningslinjer for anskaffelser til Norges Bank» som er utviklet av Norges Bank Administrasjon (NBA), og er gjeldende for begge virksomhetsområdene.

Videre har SBV utarbeidet en rekke styrende dokumenter for å operasjonalisere anskaffelsesprosessen, og vi har fått oversendt og gjennomgått nærmere 30 relevante dokumenter. Dokumentene dekker ikke prosessen i sin helhet, men ulike delområder/-oppgaver i prosessen. Eksempler på dette er utfyllende retningslinjer for IKT-sikkerhet i anskaffelser, utvikling og forvaltning, eller tilgrensende oppgaver som også er relevante for anskaffelsesprosessen som eksempelvis prinsipper for risikostyring og internkontroll. Uavhengig av dette omfatter dokumentene vi har gjennomgått følgende temaer/områder:

1) Risikostyring, internkontroll og operasjonell risiko
2) IKT og særlig IT-sikkerhet
3) Etiske retningslinjer, forventninger til leverandører og Integrity Due Diligence (IDD)-prosess
4) Fullmakter
5) Bruk av/innhold i standarddokumenter
6) Oppfølging av leverandører

Disse styrende dokumentene inneholder en rekke utfyllende bestemmelser til de overordnede dokumentene. Den nye retningslinjen for leverandøroppfølging omhandler oppfølgingsfasen av utkontrakteringen, og vurderes å være særlig relevant. I dokumentet beskrives rollen som avtaleeier samt krav til oppfølging av leverandør og avtalen.

Det er avtaleeier som har ansvaret for oppfølging av avtalen, og dette vurderes som hensiktsmessig. Retningslinjen beskriver imidlertid ikke hvordan denne rollen er plassert i forhold til de grunnleggende rollene behovseier og prosessansvarlig (jfr. beskrivelse i kapittel 2.1.1 ovenfor). Det er viktig at det beskrives nærmere hvordan disse tre rollene skal fungere sammen. Dette for å sikre effektiv og målrettet kommunikasjon, f.eks. knyttet til risikovurderinger, gjennom hele utkontrakteringsprosessen i tråd med beste praksis.

Det følger av bankens retningslinje for oppfølging av leverandører at krav til og omfang av oppfølging skal baseres på utkontrakteringens kritikalitet. Kritikaliteten er basert på vurdering av ulike kategorier, og det listes opp seks ulike faktorer som lar seg tolkes som minstekrav til risikovurderinger. Dette vurderer vi som positivt, men vi vurderer handlingsrommet i risikovurderingene som relativt stort, slik at omfang og kvalitet i vurderingene vil kunne variere betydelig.

Utover dette inneholder retningslinjen noe mer informasjon om punkter vi har savnet i de overordnede dokumentene. Blant kriteriene som kan inngå i risikovurderingene finner vi byttekostnader til ny leverandør og tilgang til alternative løsninger. Dette er kriterier som typisk inngår i exit-strategier. Vi finner også kriteriet «påvirkning på bankens omdømme». Dette er et typisk kriterium knyttet til virksomhetsstyring hos leverandør og underleverandører.

Alle risikovurderingene som listes opp vurderes som hensiktsmessige, men for å avdekke risiko tidligst mulig, er det viktig at SBV sikrer at risikovurderingene gjennomføres allerede i planleggingsfasen av en anskaffelse. Det er også viktig at risiko som avdekkes tidlig i utkontrakteringsprosessen, følger med videre i oppfølgingsfasen og eventuelt også reflekteres gjennom krav i kontrakten. En beskrivelse av et slikt samspill er ikke inkludert i dokumentet.

Vi har på et overordnet nivå bemerket at vi savner et prinsipielt krav om dokumentasjon av sentrale vurderinger i utkontrakteringsprosessen. I det nye dokumentet for leverandøroppfølging observerer vi krav til dokumentasjon av avtaleforhold og leverandører ved oppstart av avtaleforholdet. Dette vurderer vi som positivt, men opprettholder likevel vår vurdering av at dette også bør være et prinsipielt, overordnet krav.

Det er viktig at oppdragstaker overholder reglene i personopplysningsloven og personvernforordningen (GDPR). Dette bør, i henhold til anbefalinger fra Finanstilsynet, komme frem i foretakets styrende dokumenter for utkontraktering. Personvernvurderinger er nevnt i rutinen for Integrity Due Diligence (IDD), men da primært knyttet til Norges Bank sin behandling av personopplysninger på vegne av oppdragstaker, i prosessen med gjennomføringen av IDD-undersøkelser. Det er vår vurdering at de fastsatte kravene knyttet til evaluering av personvernsrisiko, og risikoen for oppdragstakers manglende etterlevelse av GDPR-regelverket, kan beskrives ytterligere i SBVs rammeverk, jfr. dokumentene listet opp under punkt 1) – 6) nederst på forrige side. Retningslinjen om leverandøroppfølging er et hensiktsmessig dokument for denne delen av utkontrakteringsprosessen.

Samlet sett er bestemmelser for utkontraktering spredt på svært mange dokumenter. Det gjør det krevende å få en god oversikt over hvilke krav og forventninger SBV har til utkontrakteringsprosessen og til alle fasene av utkontrakteringen, selv om dokumentene inneholder mange gode enkeltbestemmelser, krav og forventninger.

Prosess for utkontraktering

SBV benytter prosessen som er beskrevet på overordnet nivå i kapittel 2.1.1 for sine utkontrakteringer. De vurderingene som er beskrevet på overordnet nivå er derfor også gjeldende for SBV. SBV har etablert et rammeverk for å vurdere operasjonell risiko. Dette

er basert på internasjonale standarder, slik som COSO, ISO, o.l. Målet er å identifisere risiko og iverksette risikoreduserende tiltak for å sikre at organisasjonen opererer innenfor etablerte risikorammer. Vi er informert om at risiko og kontroller skal dokumenteres og vedlikeholdes i SBV sitt ERM-system [redacted], og at systemet benyttes for å dokumentere all operasjonell risiko.

Gjennom intervjuer med SBV har vi i tillegg fått informasjon om den praktiske gjennomføringen av utkontrakteringen. Ut ifra dette er vår forståelse at utkontrakteringen gjennomføres i henhold til de tre fasene som bankens styrende dokumenter beskriver:

> *Forberedelser:* I denne fasen skal behovseier sikre mandat og budsjett. Behovseier skal også vurdere hvilke særskilte vurderinger som er relevante for den gjeldende anskaffelsen.
>
> *Utvikling og gjennomføring av anskaffelsen:* Denne fasen starter med registrering av anskaffelsen i bankens serviceportal. Behovseier sørger for at de ulike stegene i anskaffelsesprosessen gjennomføres og godkjennes. Det sjekkes ut om anskaffelsen treffes av anskaffelsesregelverket, eller ikke. Seksjonen Procurement bistår behovseier i prosessen og sørger for å ta anskaffelsen ut i markedet, f.eks. gjennom publisering i anbudsportalen [redacted]. Procurement styrer denne delen av prosessen til kontrakten er signert og dokumentene er lagret. Dokumentasjonen skal lagres i bankens dokumenthåndteringssystem, DNA. I henhold til «Rutine for integritetsundersøkelser av tredjeparter (IDD) i sentralbanksjefens ansvarsområde» har GRC-funksjonen ansvaret for å gjennomføre IDD for linjeorganisasjonen ved inngåelser av avtaler. For eksisterende avtaler gjøres IDD etter nærmere avtale. GRC-funksjonen har nylig tatt i bruk screeningsverktøyet [redacted] for å gjennomføre IDD. Dette verktøyet vil også kunne benyttes for regelmessig overvåkning og oppfølgning av leverandøren.
>
> *Oppfølgingsfase:* Etter at kontrakten er inngått får tjenesteeier ansvar for å følge opp leverandør og forvaltning av avtalen. Dersom oppfølgingen viser vesentlige avvik, kan Procurement involveres i oppfølgingen. Slik vi har forstått gjennom intervjuer med banken, kan denne oppfølgingen variere avhengig av fagområde og type avtale. Ett eksempel fra IT Drift viser at ansvaret for oppfølgingen ligger hos «vendor manager». Eksempler på sentrale oppgaver er å gjennomføre kontinuerlig oppfølging av krav som er stilt til leveransen i avtalen og å følge opp leverandøren. Banken har også møteplasser for å diskutere kontraktsoppfølging internt, og med leverandøren, avhengig av kritikalitet. Informasjon som er mottatt i intervjuer er at banken har stort fokus på oppfølging.

Vurdering av prosess for utkontraktering

Vi vurderer inndelingen av prosessen i faser som hensiktsmessig og i tråd med beste praksis.

Forberedelsesfasen er en viktig fase, fordi den legger grunnlaget for sentrale elementer som skal være med i det videre arbeidet som identifikasjon og vurdering av risikopunkter, kontraktselementer samt innhold og prosess for oppfølging av leverandør.

Finanstilsynets rundskriv for utkontraktering nevner ikke spesifikt hvilke punkter eller handlinger som bør være med i en slik forberedelsesfase, men kravene i rundskrivet om å vurdere hvorvidt en utkontraktering av oppgaver vurderes som forsvarlig og om eget foretak har kapasitet og kompetanse til å sikre nødvendig styring og kontroll av utkontraktert virksomhet er nærliggende som innhold i denne fasen. Vi antar at vurderinger om mulighet for utkontraktering ligger til grunn når mandat og budsjett sikres i denne delen av prosessen (jfr. mal for Business case). Vi er informert om at banken benytter et ERM-system, [redacted], for å standardisere og strukturere vurderinger og håndtering av operasjonell risiko. Vi vurderer dette som en god start, men ikke tilstrekkelig som (mal)-verktøy for risikovurderinger i utkontrakteringsprosessen. [redacted]

benyttes for registrering og oppfølging av risikoer på prosessgruppenivå, og vil kun indirekte fange opp spesifikke risikoer knyttet til leverandører og tjenesteleveranser. Det er definert noen tverrgående risikoer benevnt «tredjepartsrisiko» uten at disse direkte er knyttet til den aktuelle utkontrakteringen, leverandøren eller tjenesteleveransen.

Bruk av det interne prosessverktøyet i bankens serviceportal bidrar til at selve anskaffelsesprosessen gjennomføreres strukturert og oversiktlig, og at risikovurderinger inngår som et viktig steg i denne. Prosessverktøyet benyttes både i SBV og NBIM. Stegene i prosessen er:

- Assign
- Legal Assessment
- Procurement
- Risk Assessment
- Review contract
- Finalize Procurement

BDO har mottatt enkelte maler og skjermklipp fra intranett vedrørende forventinger til leverandører uten at det fremgår tydelige krav til bruk av disse i SBV sine overordnede retningslinjer. I tillegg vurderer vi at malene ikke dekker alle forhold som nevnes i Finanstilsynets rundskriv om vurdering av oppdragstaker og eventuelle underleverandører. Hvis vi ser bort fra denne svakheten, har vi gjennomført noen generelle vurderinger basert på beskrivelse av hva slags risikovurderinger som forventes i prosessen. Prosessoppsettet vi har gått gjennom viser følgende relevante områder for risikovurderinger:

- Integrity Due Diligence (IDD)-sjekk
- IT-sikkerhet og arkitektur
- Personvern
- Interessekonflikt

Områdene fremstår for oss som et resultat av praktisk erfaring, men ikke nødvendigvis på bakgrunn av helhetlige og systematiske vurderinger. Det fremgår ikke hva som skal vurderes innenfor hvert område, eller om det er øvrige områder som også skulle vært inkludert. Eksempler på dette kan være områder som er underlagt særlige regulatoriske krav, fysisk sikkerhet, personellsikkerhet, beredskap osv.

Vi er informert om at SBV benytter [redacted] for utlysning av alle sine anskaffelser. [redacted] inngår det spesifikke informasjonskrav knyttet til virksomhetsstyring i et såkalt ESPD-skjema (standardformular for det europeiske egenerklæringsskjemaet). Her skal leverandører opplyse om eksempelvis straffedommer knyttet til korrupsjon, hvitvasking og barnearbeid eller hvorvidt selskapet benytter miljøstyringssystemer. Dette er også relevant informasjon inn i SBV sin IDD-sjekk og ved risikovurdering av leverandør og underleverandør(er). Bankens IDD rutiner bør angi hvordan opplysninger fra ESPD-skjemaet skal vurderes og vektlegges ved IDD gjennomgang for å sikre en helhetlig vurdering.

I forbindelse med vurdering av tilbydere har vi fått innsikt i at banken sender e-post til interne deltagere i prosessen om det foreligger inhabilitet eller interessekonflikter, og ber om tilbakemelding dersom habilitetskonflikt foreligger. Etter vår vurdering kan banken styrke denne prosessen ytterligere ved å sikre dokumentasjon av systematisk og fullstendig vurdering av habilitet og interessekonflikt.

Samlet vurdering av prosessen er at den har rammer som muliggjør at banken innfrir forventningene til beste praksis basert på rundskrivet fra Finanstilsynet. Fordi faktisk innhold i de ulike prosesstegene er lite standardisert, er banken avhengig av individuell kompetanse og god internkontroll for å sikre at prosessen er i tråd med beste praksis.

Observasjoner fra intervju antyder i tillegg et behov for å forbedre prosessen for involvering av interne funksjoner ved utkontraktering. Det er særlig viktig å sikre tidlig

involvering av relevante avdelinger, som IT-sikkerhet, IT-drift og Security and Crisis Management (SCM), ved utkontraktering av tjenester som befinner seg ved skjæringspunktet mellom drift og IT. Dette vil kunne bidra til å sikre en mer effektiv og enhetlig prosess for oppfølging av ulike leverandørforhold. Vi er opplyst om at det skal etableres en ny stilling med ansvar for leverandørstyring, spesifikt rettet mot IT-sikkerhet, også kjent som «Third Party Risk Management» (TPRM). Etableringen av en dedikert rolle for TPRM betraktes som et hensiktsmessig tiltak.

2.2.2 Etterlevelse av rammeverk for styring og kontroll - Intility

For å vurdere hvordan SBV etterlever krav og forventninger nedfelt i virksomhetens rutiner og retningslinjer, har vi sett nærmere på to utvalgte avtaler/utkontrakteringer:

- Intility og
- Orange Business Services

Bakgrunn

Intility-anskaffelsen var en del av et IT-moderniseringsprogram i Norges Bank som ble gjennomført i perioden 2019-2021, det såkalte DiffIT-programmet. Hensikten med programmet var å fornye systemer for å styrke sikkerhet og beredskap i kritiske løsninger samt øke fleksibiliteten for kjøp av IT-tjenester. Som følge av programmet ble IT-tjenester delt inn i de to kategoriene samfunnskritiske og virksomhetskritiske systemer. Intility er leverandør av plattform for virksomhetskritiske systemer (PVS) for SBV, som omfatter fagsystemer og administrative IT-systemer som ikke vurderes som samfunnskritiske.

For å vurdere etterlevelse av rammeverk har vi gått gjennom dokumentasjonen beskrevet i kapittel 4.2.1 Intility – Dokumentasjon for test av etterlevelse.

Våre vurderinger av etterlevelse knyttet til utkontraktering til Intility tar utgangspunkt i svakheter vi har påpekt i kapitlene 2.1 og 2.2. Her vurderte vi overenstemmelse mellom bankens rammeverk og beste praksis, [redacted]

- [redacted]

I vår vurdering av utkontrakteringen til Intility kartlegger og vurderer vi hvorvidt SBVs praksis viser tilsvarende svakheter som i rammeverket, eller om faktiske avtaler og prosesser innebærer bedre styring og kontroll enn bankens rammeverk skulle tilsi.

Vurderinger knyttet til minstekrav til risikovurderinger

Det mottatte dokumentet «PVS – Innstilling og anskaffelse – Styringsgruppen» viser at SBV har vurdert risiko i avtalen basert på punktene sikkerhet, juridisk, gjennomføring og økonomi. Tilsvarende punkter finner vi i dokumentet «Innstilling anskaffelse PSS – Styringsgruppen» som gjelder Orange-avtalen. Dette gir inntrykk av at SBV anvender standardiserte kriterier for risikovurderinger i den faktiske anskaffelsesprosessen, selv om dette ikke er definert i styrende dokumenter.

Vurdering av krav til leverandørens virksomhetsstyring

I innledningen til kravspesifikasjonen i bilag 1 fastslår banken at *«plattformen for virksomhetskritiske systemer skal ivareta virksomhetens behov for god driftsstabilitet og høy sikkerhet, samtidig som det legges til rette for å ta i bruk nye løsninger på en rask og effektiv måte, gjennom å utnytte innovasjon og teknologisk utvikling innenfor*

tjenestemodeller og tjenesteleveranser». For å oppfylle dette kravet må den tekniske kapasiteten i løsningen hos Intility samt den umiddelbare styringen og kontrollen av disse tjenestene være på plass. Samtidig er det ikke å forvente at Intility kan levere dette på et høyt nivå over tid, hvis den generelle virksomhetsstyringen ikke er av god kvalitet. Det er derfor å forvente at kravspesifikasjonen i bilag 1 eller administrative bestemmelser i del 6 inneholder kriterier knyttet til dette.

Kravspesifikasjon i bilag 1 er delt i tre hoveddeler:

- Generelle krav
- Tjenesteområder
- Etableringsprosjekt

Krav til Intilitys virksomhetsstyring vil være typiske for del «generelle krav». I underpunkter i dette kapitlet finner vi igjen typiske begreper fra virksomhetsstyring som krav til styring og samhandling, hendelseshåndtering, innsyn og revisjon, dokumentasjon, kontinuitet og beredskap og risikostyring. Dette er et godt utgangspunkt for krav til og vurdering av leverandørers virksomhetsstyring. Etter vår vurdering er de imidlertid ikke tilstrekkelig for å sikre beste praksis på området. Følgende punkter kan illustrere dette:

- Kravspesifikasjonen tydeliggjør forventinger om et dokumentert og operasjonalisert system for risikostyring i henhold til anerkjente standarder som f.eks. ISO 31000 eller PRINCE2, og at dette benyttes som en del av kvalitetssikringen i avtaleperioden. ISO 31000 og PRINCE2 kan benyttes som system for helhetlig risikostyring i et selskap, men kan også benyttes som system for styring og kontroll av risiko knyttet til enkeltaktiviteter og prosjekter. Av svaret til leverandøren i del 2 – leverandørens løsningsbeskrivelse, tolker vi det slik at leverandøren legger vekt på risikovurderinger i leveransen og ikke i selskapet som helhet.
- Under styring og samhandling finner vi krav om at leverandøren skal ha en service management prosess for styring, kontroll og oppfølging av tjenesteleveranser, basert på rammeverket ITIL Service Management. ITIL er et rammeverk med anbefalte prosesser for styring og kontroll av IT-tjenesteleveranser. Også dette kravet er sterkt knyttet til selve leveransen og ikke til leverandørens overordnede virksomhetsstyring.

Vårt inntrykk er at utkontrakteringen til Intility har flere punkter som tematiserer virksomhetsstyring, men at kravene ikke er tydelige nok for å sikre en tilstrekkelig vurdering av leverandørens virksomhetsstyring.

Vurdering av krav til underleverandører

Del 1 kravspesifikasjon inneholder flere krav til bruk av underleverandører. I del 1 finner vi f.eks. krav til oversikt over underleverandører og krav til å ha en prosess som sørger for underleverandørens samsvar med sikkerhetskrav i Norges Bank. Dette er viktig knyttet til kvaliteten på den leverte løsningen, men gir ikke grunnlag for å vurdere risiko hos underleverandør som et resultat av svakheter i virksomhetsstyringen hos underleverandøren. Her kan SBV fremover vurdere å integrere nye krav til risikovurdering av underleverandører basert på blant annet åpenhetsloven.

I del 6 for administrative bestemmelser har Intility gitt en oversikt over underleverandører. Den inneholder kun faktainformasjon om navn, organisasjonsnummer og liknende, uten noen videre risikovurdering av virksomheten. SBV kan imidlertid gjennomføre selvstendige vurderinger på basis av denne faktainformasjonen.

Som for virksomhetsstyring er vårt inntrykk at flere punkter tematiseres, men at banken konsentrerer seg om krav til løsning, og at minstekrav til vurdering av virksomhetsstyringsrelatert risiko hos underleverandører ikke nødvendigvis inngår i vurderingene.

Vurdering av krav til oppfølging av avtalen

Når det gjelder oppfølging av avtalen inneholder driftsavtalen og kravspesifikasjonen en rekke ulike krav som legger grunnlag for dette. Kravspesifikasjonen inneholder for eksempel krav til hendelseshåndtering, varsling av planlagte endringer, årlig selverklæring for etterlevelse av sikkerhetskontroller og gjennomføring av øvelser knyttet til kontinuitetsplaner. I del 6 for administrative bestemmelser er blant annet møteplaner for oppfølging dokumentert, krav om å gjøre informasjon tilgjengelig i leveranseperioden og krav til dokumentasjon. Vi er også informert om at SBV mottar årlige ISAE 3402/SOC-rapporter fra Intility, og at disse blir gjennomgått og evaluert som ledd i den løpende oppfølgningen av tjenesteleveransen.

Vi oppfatter at oppfølgingskravene er sterkt knyttet til selve løsningen, og mindre til oppfølging av selskapet som helhet.

Vurdering av krav til exit-strategier

Exit-strategier er håndtert i driftsavtalen med Intility. Her finner vi bestemmelser om varighet, avbestillingsmuligheter og avslutning av avtalen. Bestemmelsen om avslutning er blant annet knyttet til frist for oppsigelse, krav om bistand til forberedelser til ny avtale med annen leverandør, krav til overføring av kompetanse og en rekke mer tekniske spesifikasjoner som f.eks. overføring av sikkerhetskopier. I henhold til Finanstilsynets rundskriv og vurdering av exit-strategier forventes det at SBV kan vurdere risikoer og muligheter for å reintegrere tjenesteleveransen i egen organisasjonen og/eller overføring til andre leverandører. Vi er ikke forelagt dokumentasjon som viser at slike vurderinger er gjort.

2.2.3 Etterlevelse av rammeverk for styring og kontroll - Orange Business Services

Orange-anskaffelsen er, som Intility-anskaffelsen, en del IT-moderniseringsprogrammet i Norges Bank som ble gjennomført i perioden 2019-2021. Hensikten med programmet var å fornye systemer for å styrke sikkerhet og beredskap i kritiske løsninger samt øke fleksibiliteten for kjøp av IT-tjenester. Som følge av programmet ble IT-tjenester delt inn i de to kategoriene samfunnskritiske og virksomhetskritiske systemer. Orange er leverandør av plattform for samfunnskritiske systemer (PSS) for SBV. Denne plattformen skal ivareta Norges Bank mest kritiske systemer, og skal tilfredsstille alle lovpålagte krav og internasjonale anbefalinger. De samfunnskritiske systemene på PSS er underlagt sikkerhetsloven. Dette medfører at det gjennom avtalen ikke bare stilles krav til leveransene, men også til leverandøren Orange. Blant annet innebærer kravene at Orange skal opprettholde godkjent leverandørklarering fra Nasjonal Sikkerhetsmyndighet gjennom hele kontraktsperioden.

For å vurdere etterlevelse av rammeverk har vi gått gjennom dokumentasjonen beskrevet i kapittel 4.2.2 Orange Business Services – Dokumentasjon for test av etterlevelse.

Våre vurderinger av etterlevelse knyttet til utkontraktering til Orange tar, som for Intility, utgangspunkt i svakheter vi har påpekt i kapitlene 2.1 og 2.2. Her vurderte vi overenstemmelse mellom bankens rammeverk og beste praksis,

- [redacted]

I tillegg har vi vurdert overensstemmelsen mellom avtalen når det gjelder innhold i kravene, for å vurdere hvorvidt vi ser tegn til minstekrav.

Vurderinger knyttet til minstekrav til risikovurderinger

Vi viser til vår vurdering av dette punktet i Intility-avtalen.

Vurdering av krav til leverandørens virksomhetsstyring

Vi har sett nærmere på kravspesifikasjonen og mulighet for vurdering av leverandørens virksomhetsstyring. Kravspesifikasjonen i del 1 er delt i tre hoveddeler:

- Generelle krav
- Tjenesteområder
- Etableringsprosjekt

Inndelinger og temaer for kapitler er i stor grad identisk med Intility-avtalen, men med noen individuelle tilpasninger. For eksempel har kravspesifikasjonen for Orange-avtalen egne kapitler om personalledelse og utvikling samt kompetanse og kapasitet.

Under kompetanseplaner og kapasitet formulerer SBV blant annet krav til kompetanseutviklingsplaner og at disse følges opp med tiltak. Under personalledelse og -utvikling krever SBV at leverandøren har en strukturert og proaktiv oppfølging av medarbeidere gjennom medarbeidersamtaler og målstyring. Det kreves også en beskrivelse av organisasjonsmodellen med tilhørende styringsmodell. Vi vurderer dette som relevante delkriterier for vurdering av leverandørens virksomhetsstyring og med dette en styrking av en slik vurdering sammenliknet med kravspesifikasjonen for Intility-avtalen.

Hvis vi sammenlikner konkret innhold i de ulike kravene, pekte vi på det sterke leveransefokuset i kriterier for risikostyring hos Intility. Kravet for Orange-leveranser er tilnærmet identisk. Vi nevnte også at kravet under styring og samhandling som omhandler prosess for styring, kontroll og oppfølging av tjenesteleveranser basert på ITIL-rammeverket. ITIL-rammeverket er et sett med anbefalte prosesser for styring og kontroll av IT-tjenesteleveranser. Kravspesifikasjonen for Orange-avtalen har en annen beskrivelse av kravene, men også disse er sterkt knyttet til selve leveransen og ikke til leverandørens overordnede virksomhetsstyring.

Vårt inntrykk er at utkontrakteringen til Orange har flere punkter som tematiserer virksomhetsstyring, men at kravene heller ikke i denne avtalen er tydelige nok for å sikre en tilstrekkelig vurdering av leverandørens virksomhetsstyring. Dette er av særlig betydning for denne type avtaler, fordi banken vektlegger å tilfredsstille prinsippene for finansiell infrastruktur, PFMI. Disse prinsippene fikk i løpet av 2023 et tillegg som viser til G20/OECD Principles of Corporate Goverance hvor hensikten beskrives som:

The Principles of Corporate Governance («the Principles») are intended to help policy makers evaluate and improve the legal, regulatory, and institutional framework for corporate governance, with a view to supporting economic efficiency, sustainable growth and financial stability.

For kommende avtaler av same type, vil det være viktig å sikre at G20/OECD-prinsippene kan oppfylles.

Vurdering av krav til underleverandører

Del 1 i kravspesifikasjonen inneholder krav til bruk av underleverandører. Disse er ikke identiske med kravene til Intility-avtalen. Ett av punktene omfatter krav til beskrivelse av hvordan tilbyder identifiserer, vurderer, reduserer og rapporterer risikoer i forbindelse med bruk av underleverandører. Dette er en relativ generell vurdering som kan omfatte risiko knyttet til mangler i virksomhetsstyringen hos underleverandører. Fordi det ikke eksplisitt viser til slike risikoer, sikrer ikke kravet en slik vurdering.

Som for Intility-avtalen inneholder denne en oversikt over underleverandører. Her er imidlertid faktainformasjonen begrenset til opplisting av navn på underleverandør uten f.eks. organisasjonsnummer. Det kan innebære mulighet for forveksling av selskaper og tilsvarende unøyaktighet i eventuelle egne risikovurderinger.

Som for virksomhetsstyring er vårt inntrykk at flere punkter tematiseres, men at banken konsentrerer seg om krav til løsning, og at minstekrav til vurdering av virksomhetsstyringsrelatert risiko hos underleverandører ikke nødvendigvis inngår i vurderingene.

Vurdering av krav til oppfølging av avtalen

Når det gjelder oppfølging av avtalen inneholder driftsavtalen og kravspesifikasjonen en rekke ulike krav som legger grunnlag for dette. Kravspesifikasjonen inneholder for eksempel krav til hendelseshåndtering, jevnlig rapportering på status for problemhåndtering, krav om umiddelbar rapportering ved alvorlige sikkerhetshendelser og krav til periodisk rapportering av status for sikkerhet og sikkerhetsrisiko. I del 6 for administrative bestemmelser er blant annet møteplaner for oppfølging dokumentert, krav om å gjøre informasjon tilgjengelig i leveranseperioden og krav til dokumentasjon. Vi er også informert om at SBV mottar årlige ISAE 3402/SOC-rapporter fra Orange, og at disse blir gjennomgått og evaluert som ledd i den løpende oppfølgningen av tjenesteleveransen.

Vi oppfatter at oppfølgingskravene er sterkt knyttet til selve løsningen, og mindre til oppfølging av selskapet som helhet.

Vurdering av krav til exit-strategier

Exit-strategier fra avtalen er håndtert i driftsavtalen med Orange. Som for Intility finner vi her bestemmelser til varighet, avbestillingsmuligheter og avslutning av avtalen. Bestemmelsen om avslutning er blant annet knyttet til frist for oppsigelse, krav om bistand til forberedelser til ny avtale med annen leverandør, krav til overføring av kompetanse og en rekke mer tekniske spesifikasjoner som eksempelvis overføring av sikkerhetskopier. I henhold til Finanstilsynets rundskriv og vurdering av exit-strategier forventes det at SBV kan vurdere risikoer og muligheter for å reintegrere tjenesteleveransen i egen organisasjonen og/eller overføring til andre leverandører. Vi er ikke forelagt dokumentasjon som viser at slike vurderinger er gjort.

Vurdering av SBVs bruk av standardiserte minstekrav i sine kravspesifikasjoner

Kravspesifikasjonene som ligger til grunn for avtalene med Orange og Intility er i utgangspunktet svært like, gjennom sin inndeling i tre hoveddeler og stor likhetsgrad i kapittelinndeling og betegnelse. De spesifikke kravene knyttet til de ulike temaene oppfatter vi i stor grad som individuelle krav. Fordi banken søker to ulike løsninger, er dette til en viss grad naturlig. Likevel oppfatter vi at banken bør vurdere en sterkere bruk av standardiserte minstekrav for å øke kvaliteten i sine risikovurderinger ytterligere. Dette gjelder særlig krav til overordnet virksomhetsstyring av leverandør og underleverandører samt rammer for oppfølging av avtalen.

2.2.4 Anbefalinger for å styrke styring og kontroll med utkontraktering i SBV

For å styrke bankens styring og kontroll med utkontraktering, anbefaler vi å

- sørge for tydelig definisjon av rollen som avtaleeier og andre relevante roller som er involvert i utkontraktering, særlig hvordan disse rollene spiller sammen med rollene behovseier eller prosessansvarlig for anskaffelse
- vurdere å utvikle et selvstendig dokument for utdypende veiledning av hele utkontrakteringsprosessen for å tydeliggjøre blant annet
    - de ulike fasene av utkontrakteringsprosessen

- hva som forventes i de ulike fasene med særlig fokus på definerte minimumskrav
- hva som forventes av vurderinger knyttet til personvern
- hva som forventes av vurderinger og dokumentasjon knyttet til habilitet og interessekonflikter
- hva som forventes av vurderinger knyttet til leverandørens og underleverandørers virksomhetsstyring
- hva som forventes av vurderinger knyttet til exit-strategi
- hva som forventes av aktiviteter og vurderinger i fasen for oppfølging, spesielt hvordan kritiske resultater fra risikovurderinger i anskaffelsesfasen overføres til oppfølgingstiltak i fasen for oppfølging
- tilknytning til andre dokumenter i SBVs dokumenthierarki
- forventninger til malbruk og andre verktøy
- forventninger til dokumentasjon av viktige vurderinger og sentrale beslutninger.

2.3 Styring og kontroll av utkontraktering i NBIM

2.3.1 Observasjoner og vurderinger

Bakgrunn

Vår gjennomgang omfatter organisatoriske strukturer og styringsdokumenter, vurdering av NBIMs overordnede prosess for utkontraktering og risikovurdering av tjenesteleverandører, samt oppfølgingen av disse.

NBIMs rammeverk for utkontraktering bygger på en tydelig delegering av oppgaver for å sikre et effektivt system for kontroll og innsyn. Dette er operasjonalisert gjennom en rekke styrende dokumenter, policyer, retningslinjer og rutiner som er fastsatt på forskjellige organisatoriske nivåer og som er gjeldende for NBIM.

Organisering, roller og ansvar

CEO NBIM har det overordnede ansvaret for implementering av de prinsipper og retningslinjer som hovedstyret har vedtatt. Videre operasjonaliseres styrets retningslinjer ved at CEO NBIM beslutter policyer og delegerer fullmakter til toppledelsen. Dette danner grunnlaget for detaljerte rammeverk og prosessbeskrivelser, som blir fastsatt av den ansvarlige lederen i NBIMs ledergruppe.

Styrende dokumenter for utkontraktering

NBIM følger overordnede prinsipper fastsatt av hovedstyret. Primært er disse prinsippene konkretisert gjennom dokumentet «retningslinjer for anskaffelser til Norges Bank» utviklet av Norges Bank Administrasjon (NBA), som er gjeldende for begge virksomhetsområdene. Retningslinjene spesifiserer at anskaffelsesprosessen skal være kostnadseffektiv, samtidig som prosessen skal sikre en konsolidering av kontrakter innenfor områder hvor behovene overlapper. Det forventes også at NBIM skal opptre som en profesjonell oppdragsgiver, med en systematisk oppfølging av kontrakter og leverandører.

For å tilpasse risikoen og operasjonene som er særegne for NBIM, er det utarbeidet spesifikke retningslinjer og prosedyrer. NBIMs prosessrammeverk («Management Framework») fastsatt av Chief of Staff (CoS) beskriver overordnede prinsipper knyttet til risikostyring og kontroll i utøvelsen av den daglige driften. Blant annet legger rammeverket føringer for strategi, planlegging, prosessbeskrivelser og virksomhetsstyring.

Policy for «Sourcing and service provider management» er vedtatt av CEO NBIM, og beskriver generelle krav knyttet til anskaffelser og utkontraktering. Utkontraktering skal kun gjennomføres i tråd med NBIMs overordnede strategi og når oppdragstaker har tilstrekkelig kapasitet til å opprettholde kontinuitet i tjenesteleveransene. Videre skal finansiell, operasjonell og omdømmerisiko analyseres før avtaleinngåelse (due diligence), og resultatene av analysen skal godkjennes på rett ledernivå. Retningslinjene er basert på et grunnleggende linjeansvar, der behovseieren som innehar linjeansvaret også disponerer budsjettet, og har mandatet samt fullmakten til gjennomføring av anskaffelsen.

CoS har fastsatt retningslinjer for anskaffelser («Sourcing»). Retningslinjene spesifiserer krav om at utkontraktering skal gjennomføres i tråd med «Lov om offentlig anskaffelser» (LOA), og at alle leverandører skal behandles med forutsigbarhet og transparens. Chief Technology and Operating Officer (CTOO) i NBIM har det overordnede ansvaret for retningslinjen «Lifecycle management», samt ansvaret for å sikre at tjenesteleverandører blir korrekt klassifisert i tråd med fastsatte retningslinjer.

Gjennom NBIMs nylig implementerte retningslinjer for leverandøroppfølging «Provider lifecycle management», samt understilte dokumenter, er det lagt til rette for en helhetlig tilnærming til risikostyring og oppfølging av oppdragstakere. Retningslinjen eies av CTOO, og tydeliggjør ansvarsfordelingen blant nøkkelpersoner og stiller krav til ulike aktiviteter som skal gjennomføres i ulike faser. Dette understøttes av en overordnet prosessbeskrivelse som følger livssyklusen til tjenesteleveransen.

Vurdering av NBIMs styrende dokumenter for utkontraktering

Vår gjennomgang viser at retningslinjer for utkontraktering i stor grad samsvarer med anbefalingene fra EBA. Videre innehar NBIM hensiktsmessige prosesser for identifisering, vurdering og håndtering av risiko knyttet til utkontraktering. Disse prosessene er også grundig beskrevet gjennom aktuelle policyer, retningslinjer og rutiner. Dette er i tråd med forventinger fastsatt av Finanstilsynets rundskriv. Videre beskriver EBA i sine retningslinjer viktigheten av å sikre god forankring og forståelse av rammeverket for utkontraktering i hele organisasjonen. Gjennomgangen av NBIMs styrende dokumenter, samt intervjuer med ressurser fra ulike virksomhetsområder, tyder på god forståelse av internt rammeverk i organisasjonen. Policy og rutiner presiserer også krav om at NBIM skal opprettholde tilstrekkelig kompetanse og kapasitet internt. Kravene er etablert for å sikre kontroll over oppdragstaker og tjenesteleveransen(e) gjennom hele utkontrakteringsprosessen. Dette samsvarer med de forventingene Finanstilsynet har til banker og andre finansforetak.

Vi observerer enkelte områder som kan forbedres, for å sikre en hensiktsmessig utvikling av NBIMs styrende dokumenter for utkontraktering. Det er viktig at NBIM definerer hvilke interne ressurser som er ansvarlig for den utkontrakterte tjenesten. Av NBIMs rammeverk fremkommer det at Relationship Owner (RO) har det overordnede ansvaret for alle tjenesteleveranser for sitt virksomhetsområde, men at dette ansvaret kan delegeres til en annen ressurs. Blant annet kan ansvaret fordeles fra områdelederen (Chief of area) til Global Head. NBIMs overordnede rammeverk beskriver imidlertid ikke hvilke kriterier som må være oppfylt for at dette ansvaret kan delegeres, noe som er i kontrast til Finanstilsynets forventninger.

Gjennomgangen viser at NBIM kan ytterligere spesifisere hvordan stab- og støttefunksjoner skal involveres i de ulike stadiene ved inngåelse av en utkontrakteringsavtale, og ved løpende oppfølging av oppdragstaker. EBA beskriver i sine retningslinjer at det skal defineres tydelige ansvarsforhold knyttet til involvering av kontrollfunksjoner i andrelinje (eksempelvis risikostyring og compliance), samt andre støttefunksjoner som juridisk-, IT- og økonomiavdelingen. Det forventes tydelige retningslinjer knyttet til hvordan disse funksjonene skal bidra med dokumentasjon, oppfølging og kontroll av utkontrakterte tjenester. Det er vår oppfatning at NBIM i større grad bør tydeliggjøre dette ansvarsforholdet i sitt overordnede rammeverk.

Prosess for utkontraktering

I henhold til NBIMs rutiner blir tjenesteleverandøren tildelt en Relationship Owner (RO) som har det overordnede ansvaret for alle tjenesteleveranser knyttet til oppdragstakeren, og en Relationship Manager (RM), som har ansvaret for styring og kontroll av leverandørforholdet i samsvar med gjeldende retningslinjer. RM har også ansvaret for å sikre tilstrekkelig løpende oppfølging av tjenesteleverandøren. Dette fremkommer av NBIMs nylig implementerte retningslinjer for leverandøroppfølging «Provider lifecycle management». Videre fremkommer det av NBIMs retningslinjer for «Service Provider Management» at Service/ System Owner (SO) har ansvaret for å dokumentere kvaliteten i de ulike tjenesteleveransene, og sikre at de er i samsvar med etablerte krav. Samtidig er Service / System Manager (SM) ansvarlig for å sikre at tjenesteleveransene er i tråd med overordnet strategi for området. SM er også ansvarlig for å sikre oppfølging av at tjenesten(e) er i samsvar med «Policy for operasjonell risiko». Videre skal SM sikre at dokumentasjon som foreligger i systemet for leverandørstyring [redacted], til enhver tid er korrekt og oppdatert.

I *planleggingsfasen* skal det gjennomføres nødvendige prosesser for å tydeliggjøre behovet for utkontraktering. Dette omfatter utarbeidelse av en «business case», kartlegging av eksisterende leveranser innenfor det relevante virksomhetsområdet, samt en vurdering av behovet for intern utvikling for å sikre tilpasning til egen drift («build or buy»). I denne fasen skal planen for utkontraktering godkjennes innenfor vedtatte budsjetter og rammer. Potensielle oppdragstakere blir forhåndsvurdert, og kravspesifikasjoner som skal inkluderes i kontraktsvilkårene, blir gjennomgått i samarbeid med relevante interne funksjoner. Dette inkluderer blant annet Procurement, IT-sikkerhet og juridisk avdeling.

For *innfasingen* av nye leverandører er følgende retningslinjer særlig relevant; «Policy for Procurement» og «Policy for Sourcing and Service Provider Management». Sentrale aktiviteter ved innfasing av nye tjenesteleverandører inkluderer vurdering av oppdragstaker basert på kritikalitet og risiko, herunder strategisk betydning av den aktuelle leveransen. Risiko og kontroller skal dokumenteres og vedlikeholdes i NBIMs ERM system [redacted], herunder relevante risikofaktorer på aggregerte nivåer. Videre skal informasjonssikkerhetsrisiko, samt operasjonell risiko, dokumenteres i [redacted]. Operasjonelle konsekvensvurderinger ved bortfall av en tjeneste blir angitt med kritikalitet og dokumentert i [redacted].

I *oppfølgingsfasen* skal det gjennomføres regelmessige statusmøter med oppdragstaker. Det er fastsatt krav om minimum 1-2 oppfølgingsmøter per år for oppdragstakere som er definert som «kritisk» eller «svært kritisk» med tanke på operasjonell kritikalitet. Complianceavdelingen benytter screeningsverktøy [redacted] for å gjennomføre Integrity Due Diligence (IDD) både i forkant av inngåelse og oppfølging av tjenesteleverandører. Ved identifisering av bekymringsfulle funn (red flags), eskaleres prosessen til aktuelle interne nøkkelpersoner, eksempelvis RO. Dette bidrar til å sikre en effektiv håndtering og oppfølging av eventuelle bekymringsverdige forhold knyttet til oppdragstakeren. For leverandører som er pålagt å levere standardrapporter til NBIM, gjennomgås disse internt. Dette inkluderer blant annet tredjepartsrapporteringer slik som ISAE / SSAE / SOC-rapporter. RM er ansvarlig for å sikre at disse rapportene deles med Compliance, som gjennomfører en selvstendig 2. linje vurdering av rapportene, samt ellers sikrer tilgjengelighet for relevante interessenter (bl.a. eksternrevisor). Interne kommentarer på tredjepartsrapporter skal arkiveres i NBIMs arkivsystem, DNA. I tillegg skal RM, med bistand fra nødvendige stab- og støttefunksjoner, sørge for regelmessig oppfølging av cybersikkerhetsrisiko og eventuelle endringer i oppdragstakers ESG-profil.

I *avslutningsfasen* av et oppdragsforhold er RM ansvarlig for å sikre at viktige aktiviteter gjennomføres, i samråd med nødvendige IT-ressurser. NBIMs rammeverk understreker viktigheten av å holde oversikt over termineringsdatoer, samt informere

tjenesteleverandøren om intensjonen om å avslutte kontraktsforholdet. RM har også ansvaret for å sikre at administrative oppgaver, som sluttfakturering, returnering av NBIMs utstyr, samt etterlevelse av prosesser for retur eller sletting av NBIMs data, blir gjennomført i henhold til vedtatte retningslinjer.

Vurdering av NBIMs prosess for utkontraktering

NBIMs prosess for utkontraktering, basert på etablert rammeverk og underliggende retningslinjer og rutiner, samsvarer i stor grad med fastsatte målekriterier. Vi identifiserer en tydelig sammenheng mellom NBIMs rammeverk for utkontraktering og Finanstilsynets prinsipp om at det skal gjennomføres grundige vurderinger av oppdragstaker, basert på underliggende kritikalitet. Dette er særlig viktig i oppstartsfasen og i forberedelsene før avtaleinngåelse med oppdragstaker. Disse bestemmelsene harmoniserer også med uttalte forventinger fra EBA, jf. GL kapittel 30. Videre forventes det at operasjonell- og sikkerhetsrisiko, vurderes fortløpende i lys av det endrede risikobildet som oppstår som en konsekvens av utkontraktering. Grundig due diligence av oppdragstakere bør blant annet omfatte evaluering av leverandørens økonomiske situasjon, operasjonelle kapasitet til å oppfylle den aktuelle avtalen, organisasjonsstruktur, samt potensiell innvirkning på oppdragsgivers omdømmerisiko.

NBIMs omfattende retningslinjer og rutiner for løpende oppfølging av leverandører, inkludert regelmessig gjennomføring av due diligence basert på fastsatte kriterier, virker å være i tråd med nevnte målekriterier. Spesielt hensiktsmessig fremstår retningslinjene knyttet til krav om at løpende risikovurderinger skal gjennomføres og dokumenteres. Det er også definert en klar ansvarsfordeling for NBIMs oppfølging av oppdragstaker(e). Dette er i tråd med forventninger fastsatt av Finanstilsynet, som understreker krav til rutiner som sikrer jevnlig kontroll av viktige elementer av oppdragstakers utførelse av utkontrakterte tjenester.

I henhold til Finanstilsynets rundskriv forventes det at foretak vurderer muligheten for å avslutte avtalen med oppdragstaker(e), uten å påføre betydelige forstyrrelser i driften. Samtidig er det viktig å sikre at juridiske krav og forpliktelser overfor oppdragstaker blir ivaretatt. Gjennomgangen indikerer at exit-strategier og retningslinjer knyttet til terminering av avtaler i hovedsak er underlagt kravspesifikasjonene i avtaleverket med den aktuelle oppdragstakeren. Dette er lite omtalt i NBIMs overordnede rammeverk for utkontraktering, noe som potensielt kan føre til manglende konsistens ved implementeringen av ulike avtaler.

Prosess for risikovurdering i NBIM

NBIMs overordnede prinsipp for utkontraktering er at tjenesteleveransen(e) og oppdragstaker skal vurderes basert på iboende risiko og kritikalitet. NBIMs retningslinjer for leverandøroppfølging «Provider lifecycle management» beskriver at klassifiseringen av oppdragstakers kritikalitet skal baseres på den totale risikoen knyttet til de leverte tjenestene, og hvor avgjørende disse er for NBIMs prosesser («operational impact»). Videre skal den operasjonelle risikoen avtalen utgjør for NBIM vurderes. Ulike risikofaktorer, inkludert omdømmerisiko, compliancerisiko, samt regulatorisk risiko skal identifiseres og dokumenteres i ERM-systemet [redacted]. Basert på disse vurderingene blir oppdragstaker og tjenesteleveranser rangert på en skala fra «lav» til «svært høy».

Videre har NBIM etablert prosedyrer for å systematisk vurdere operasjonell risiko, gjennom sitt operasjonelle risikorammeverk (ERM). Rammeverket er basert på internasjonale standarder, slik som COSO, ISO, o.l. Målet er å identifisere risiko og iverksette risikoreduserende tiltak for å sikre at organisasjonen opererer innenfor etablerte risikorammer. ERM implementerer en risikomatrise basert på kvantitative og kvalitative vurderinger av potensielle konsekvenser og sannsynlighet for at en identifisert risiko inntreffer. Utfallet av vurderingen i risikomatrisen avgjør hvilket organisatorisk nivå

risikoen må løftes til og vurderes på. Eksempelvis må hovedstyret godta kritiske risikoer, hvor potensiell konsekvens eller sannsynlighet for at risikoen inntreffer er definert som veldig høy.

Vurdering av effekten av tiltak for risikoreduksjon, i henhold til ERM-rammeverket, utføres basert på gjenværende restrisiko etter at tiltakene er gjennomført. Dette samsvarer både med Finanstilsynets forventinger knyttet til implementering av risikoreduserende tiltak, samt EBAs anbefalinger om at finansforetak bør sikre muligheten til å redusere spesifikke risikofaktorer.

Vurdering av NBIMs prosess for risikovurderinger

Finanstilsynet forventer at omfanget og innholdet i risikovurderinger skal gjenspeile foretakets kompleksitet, samt alvorlighetsgraden av den spesifikke risikoen som blir evaluert. NBIMs prosess for å sikre en grundig risikovurdering omfatter evalueringer knyttet til kompleksitet og alvorlighetsgrad i avtalen, i henhold til nevnte forventninger.

Imidlertid har vi identifisert enkelte mangler, basert på nevnte målekriterier. EBA spesifiserer krav om scenarioanalyser knyttet til mulige risikohendelser, i kapittel 12.2 i sine retningslinjer. Spesielt vektlegges analyser av potensielle operasjonelle hendelser ved mislykkede eller utilstrekkelige ytelser fra oppdragstaker. Vår gjennomgang av NBIMs rammeverk for utkontraktering, viser at overordnede retningslinjer og rutiner i liten grad redegjør for krav knyttet til scenarioanalyser.

Videre forventer Finanstilsynet at foretaket vurderer eventuelle underleverandører, «sub-contractors», før avtale om utkontraktering gjennomføres. Dette er spesielt viktig i situasjoner hvor den aktuelle avtalen kan påvirke foretakets virksomhet og renommé i vesentlig grad. EBA understreker betydningen av å vurdere underleverandører som er lokalisert i tredjeland, eller har sin primære virksomhet i et annet land enn hovedleverandøren. I dokumentet «Conduct of Business Code for Providers of Goods and Services» fremgår det at oppdragstaker skal sikre overholdelse av relevante krav i egen verdikjede. Utover disse bestemmelsene er oppfølging av underleverandører i liten grad beskrevet i NBIMs overordnede rammeverk. Det fremstår som at det formelle ansvaret for oppfølging av underleverandører i stor grad tilfaller oppdragstaker, noe som ikke samsvarer med nevnte forventinger fastsatt av Finanstilsynet og EBA.

2.3.2 Etterlevelse av rammeverk for styring og kontroll – Amazon Web Services

Bakgrunn

Etter en fullført offentlig anskaffelsesprosess i 2018, valgte NBIM Amazon Web Services (AWS) som hovedleverandør av skyplattform, [redacted] Overføringen av tidligere IT-løsninger, inkludert eksisterende serverløsninger, til AWS-plattformen ble fullført i 2019 og prosjekt ISAC («Insourcing, Security, Automation and Cloud») ble avsluttet.

AWS er en ledende global leverandør av skytjenester med en omfattende produktportefølje bestående av over 200 ulike tjenester. Disse distribueres til kundene via et nettverk av moderne datasentre som er strategisk plassert rundt om i verden. For NBIM leverer AWS infrastruktur knyttet til nettverk, datakraft, lagring og visualisering (IaaS). I tillegg håndterer AWS drift av operativsystemer og programvare (PaaS). AWS leverer også fullverdige applikasjoner og tjenester (SaaS) innenfor visse områder, der NBIM håndterer infrastrukturen som kode, tilgangsstyring og overvåkning av kritiske data. For å vurdere etterlevelse av rammeverk har vi gått igjennom dokumentasjonen beskrevet i kapittel 4.2.3.

Organisering og ansvar

NBIM har i sine retningslinjer eksplisitt angitt at rollen som Relationship Owner (RO) automatisk tilfaller den aktuelle lederen for et område. Når det gjelder AWS-avtalen ligger dette ansvaret hos Chief Technology and Operating Officer (CTOO) NBIM, men er delegert til Global Head of Technology. Rollen som Relationship Manager (RM) er tildelt Head of Service Provider Management, mens System Manager (SM) er tildelt Head of Cloud Services. Videre har NBIM en oppdatert oversikt som inneholder beskrivelser av hvilke interne ressurser som innehar de forskjellige rollene knyttet til AWS-avtalen. Denne oversikten inkluderer også oppdragstakers navn, en beskrivelse av tjenesteleveransen og klassifiseringen av kritikalitet. AWS har satt sammen en kjernegruppe («Core NBIM Account Team») bestående av ansatte med variert spesialkompetanse for å sikre kontinuerlig oppfølging med NBIM. I tillegg er det etablert et team med AWS-ledere som har et overordnet ansvar for avtalen. Det er vår oppfatning at dette styrker oppfølgingen og samhandlingen mellom NBIM og AWS. Dette bekreftes av nøkkelpersoner i NBIM som vi har intervjuet i forarbeidet til denne rapporten. Tilbakemeldingene indikerer at nåværende organisatorisk struktur legger til rette for en effektiv og dynamisk samarbeidsmodell. Videre samsvarer dette med EBAs retningslinjer som stiller krav om at avtaleansvarlig skal sikre løpende dialog og oppfølging med oppdragstaker.

Planlegging og innfasing skytjenester levert av AWS

Det er vår vurdering at NBIMs innfasing av AWS som tjenestelevandør generelt tilfredsstiller de krav og retningslinjer som er fastsatt i overordnet rammeverk for utkontraktering. Målbildet av prosessen ble etablert med forankring i NBIMs vedtatte strategi, hvor automatisering av rutineoppgaver og forbedret IKT-sikkerhet var viktige komponenter for valg av ny leverandør.

I forbindelse med NBIMs prosjekt for overgang til skybaserte IT-løsninger, [redacted], ble det gjennomført en omfattende evaluering av ulike tjenesteleverandører. Dette omfattet blant annet identifisering av potensielle risikofaktorer, inkludert «røde flagg», samt risikovurderinger relatert til IKT-sikkerhet i tråd med NBIMs operasjonelle risikorammeverk (ERM).

Det er også gjennomført og dokumentert relevante forundersøkelser av AWS (Due Diligence) i forkant av avtaleinngåelse i tråd med interne rutiner. Som en del av dette har det blitt gjennomført vurderinger av både operasjonelle og omdømmerelaterte aspekter knyttet til oppdragstakeren. Gjennomgangen vår indikerer at disse undersøkelsene er godkjent på rett ledernivå. For eksempel viser dokumentasjonen som er gjennomgått at SM har evaluert og godkjent dokumentet «System Manager Check» under onboardingen av AWS-tjenesten [redacted]. I denne prosessen har også tidligere CTOO/COO NBIM godkjent en overordnet vurdering av samme tjeneste fra AWS, som fremkommer av dokumentet [redacted]. Kravspesifikasjoner er gjennomgått og dokumentert i samarbeid med relevante interne funksjoner, slik som juridisk og IT. Dette gjelder både ved etableringen av hovedplattformen og ved onboarding av nye tilleggstjenester.

I tråd med internt rammeverk og de forventningene som er fastsatt av Finanstilsynet, er det gjennomført og dokumentert andrelinjekontroller før avtaleinngåelse, blant annet av Compliance- og risikofunksjonen i NBIM. Complianceavdelingen er ansvarlig for å gjennomføre Integrity Due Diligence (IDD) ved onboarding av nye tjenesteleverandører, i tråd med retningslinjer for leverandøroppfølging («Provider lifecycle management»). Dersom gjennomgangen avdekker relevante risikoer (røde flagg), skal disse eskaleres i henhold til NBIMs operasjonelle risikorammeverk (ERM). Gjennomgangen indikerer at det utføres månedlige IDD-sjekker av AWS. Disse blir formidlet av andrelinjen til SM i tråd med etablert rammeverk.

Løpende oppfølging av AWS

Tydelige krav til oppfølging av oppdragstakere er definert i NBIMs rammeverk. Videre er det etablert krav om at leverandører skal levere standardrapporter som blir gjennomgått internt i NBIM. Dette inkluderer blant annet rapporter knyttet til avtalte serviceleveranser (SLA), hendelsesrapportering, samt tredjepartsrapporter som ISAE / SSAE / SOC-rapporter. Det utstedes årlige SOC-rapporter for AWS, som blir utført av EY USA. Rapportene inkluderer blant annet en beskrivelse av de ulike tjenestene AWS leverer, samt en vurdering av tiltak gjennomført for å sikre god risikostyring og internkontroll. For perioden oktober 2022 til mars 2023 er det ikke rapportert om noen avvik i SOC-rapporten. SOC-rapportene følges opp og gjennomgås av NBIMs andrelinje (compliance) årlig, i tråd med interne retningslinjer. Denne praksisen samsvarer også med EBAs forventinger om at finansforetak skal sikre at de mottar relevante tredjepartsrapporter knyttet til oppdragstakers drift, jf. GL kapittel 90.

NBIMs rammeverk gir detaljerte retningslinjer for hvordan oppfølging av oppdragstaker skal gjennomføres, med formål om å identifisere endringer i risikobildet og sikre implementering av risikoreduserende tiltak. Interne ressurser i NBIM, plassert på ulike organisatoriske nivåer, følger opp tilsvarende resurser i AWS. Dette inkluderer årlige gjennomganger med CTOO NBIM og Managing Director i AWS, kvartalsvise møter på leder-/direktørnivå, samt operative teammøter med deltakelse fra både NBIM og AWS to ganger i måneden. Vår gjennomgang indikerer at NBIMs rammeverk for leverandøroppfølging i stor grad etterleves ved løpende oppfølgingen av AWS.

Risikovurdering

Overordnet rammeverk beskriver at oppdragstakers kritikalitet skal evalueres basert på den totale risikoen knyttet til samtlige tjenesteleveranser. Særlig skal operasjonelle, finansielle og sikkerhetsmessige hensyn vurderes. I henhold til interne retningslinjer skal risikovurderingen gjennomføres ved onboarding av nye oppdragstakere, og ved vesentlige endringer som kan påvirke iboende risiko knyttet til en eksisterende avtale. Prosessen skal bl.a. dokumenteres i NBIMs system for leverandørstyring, [redacted] Basert på disse vurderingene klassifiseres oppdragstaker på en skala «lav» til «svært høy», noe som setter føringer for krav til videre oppfølging av tjenesteleverandøren. Den overordnede vurderingen har plassert AWS i kategorien «svært høy». For slike oppdragstakere skal ulike og detaljerte kontroller i andrelinje utføres. Før avtalen ble inngått, gjennomførte «Security Compliance and Control» (InfoSec), «Security Operations» (SecOps), og NBIMs «Cloud Center of Excellence» (CCoE) sine vurderinger av viktige faktorer knyttet til avtalen. Ulike risikoaspekter ble evaluert, inkludert AWS [redacted] sin behandling av persondata, overholdelse av GDPR-regelverket, retten til innsyn og revisjon, samt regulering av adgangskontroller.

Videre er avtalens sikkerhetsrisiko vurdert og dokumentert i tråd med rammeverket for operasjonell risiko. Dette er presentert i en matrise som vurderer den overordnede sikkerhetsrisikoen forbundet med avtalen, basert på sannsynligheten for at en gitt risiko skal inntreffe og den potensielle konsekvensen. Relevante tiltak for reduksjon av sikkerhetsrisiko er dokumentert av CCoE og SecOps.

Vi observerer at NBIM i stor grad gjennomfører og dokumenterer risikovurderinger i henhold til internt rammeverk for leverandøroppfølging. Videre er det observert en hensiktsmessig tilnærming for implementering av risikoreduserende tiltak, samt en grundig prosess for oppfølging av disse tiltakene med AWS.

2.3.3 Anbefalinger for å styrke styring og kontroll med utkontraktering i NBIM

Basert på vår gjennomgang av rammeverket for utkontraktering, presentert i kapittel 2.3.1, har vi identifisert enkelte tiltak som kan bidra til å styrke NBIMs rammeverk ytterligere, herunder styrende dokumenter og operasjonalisering i utkontrakteringsprosessen:

- Tydeliggjøring av ansvar hos stabs- og støttefunksjoner ved utkontraktering.
    - Her bør det beskrives ytterligere hvilke funksjoner som skal involveres i de ulike stadiene i utkontrakteringsprosessen.
- Integrering av retningslinjer for avslutning av avtaler (exit-strategier) i NBIMs rammeverk for utkontraktering.
- Etablere prinsipper for å analysere potensielle operasjonelle hendelser, spesielt ved tilfellet av mislykkede eller utilstrekkelige ytelser fra oppdragstaker, i regelmessige scenarioanalyser.
    - Frekvens og krav til innhold i slike analyser kan spesifiseres i policy og rutinedokumenter på et overordnet nivå.
- Detaljere bestemmelser og retningslinjer knyttet til risikovurdering av oppdragstakers underleverandører i NBIMs rammeverk for utkontraktering.

Del 2: Utkontraktering depot- og verdipapiravregning, Citibank N.A.

3. Styring og kontroll av utkontrakterte depottjenester

Del 2 av oppdraget består i å gi en uavhengig vurdering av Norges Banks styring, kontroll og oppfølging med utkontrakterte depottjenester.

Den globale depotbanken som benyttes for internasjonale betalinger samt avregning og deponering av verdipapirer, Citibank N.A. (Citibank), er hovedobjektet for vurderingen. I tillegg inngår også en vurdering av beredskapsløsningen som Norges Bank kan benytte i en eventuell krisesituasjon, en såkalt «contingent custodian».

Det er NBIM som forvalter den globale depottjenesten på vegne av Norges Bank.

3.1 Styring og kontroll - utkontraktering av depottjenester

NBIMs rammeverk, *Management Framework*, beskriver overordnede prinsipper for hvordan de ulike avdelingene i NBIM skal operere. Dette rammeverket er også gjeldende for utkontraktering av depottjenestene. NBIM har ikke utarbeidet særskilte policyer eller retningslinjer for utkontraktering av depottjenestene eller for beredskapsløsningen for depottjenester utover disse. Det vises til kapittel *2.3 Styring og kontroll av utkontraktering i NBIM* ovenfor for en generell vurdering av styring og kontroll av utkontrakterte tjenester.

Bakgrunn

NBIM har utkontraktert tjenester knyttet til internasjonale betalinger samt avregning og deponering av verdipapirer til den globale depotbanken, Citibank. Citibank ble første gang valgt som depotbank i 2014[1] i tråd med NBIMs strategiske mål om å oppnå høyest mulig operasjonell automatisering og effektivitet i alle markeder der NBIM hadde investert, og samtidig oppnå økt effektivitet og robusthet i organisasjonen til en konkurransedyktig kostnad. Avtalen med Citibank ble fornyet etter en ny anbudsprosess som ble initiert i 2021, og som endte med at ny kontrakt ble inngått i mai 2022. I NBIMs strategi frem mot 2025 er det fremdeles et tydelig mål om å benytte én global depotbank for å sikre en effektiv modell for gjennomføring av transaksjoner og sikring av investeringer[2].

I tillegg til den ene globale depotbanken har NBIM inngått avtale om en beredskapsløsning for depottjenester (contingent custodian). Anskaffelsesprosessen i 2021-2022 resulterte i at Bank of New York Mellon (BNY Mellon) ble valgt som ny leverandør av beredskapsløsningen. Overgangen til BNY Mellon trådte i kraft fra 1. januar 2024. JP Morgan har fungert som beredskapsløsning for depottjenester frem til dette tidspunktet.

[1] https://www.nbim.no/no/oljefondet/nyheter/2014/citibank-valgt-som-ny-depotbank/

[2] https://www.nbim.no/contentassets/71d5f5ade5fb4717acdedb412f30fdac/spu-strategi-25.pdf

3.2 Etterlevelse av rammeverk for utkontraktering av depottjenester

3.2.1 Observasjoner og vurderinger

Organisering, roller og ansvar

Det overordnede ansvaret for styring og kontroll med utkontrakterte tjenester er plassert hos CEO NBIM. Dette er videre delegert til relevant leder i ledergruppen, det vil si til Chief Technology and Operating Officer (CTOO). Ansvaret for styring, kontroll og oppfølging med den globale depotbanken er videre operasjonalisert til 4 definerte roller i tråd med NBIMs *Management Framework*.

Ansvar og roller er definert i *Policy: Sourcing and Service Provider Management* og i retningslinjene *Guideline - Provider lifecycle management* og *Guideline - Service Provider Management*. I disse dokumentene er rollene Relationship Owner, Relationship Manager, Service Owner og Service Manager tydelig definert. Videre er ansvaret plassert og operasjonalisert i virksomheten gjennom dedikerte personer med angitte ansvarsområder.

Dette er:

- *Relationship Owner* – dette ansvaret tilligger «the Chief of an area», og er plassert hos CTOO NBIM. Rollen er overordnet ansvarlig for styring og kontroll av leverandørforholdet overfor Citibank og er øverste eskaleringspunkt hvis det er behov for å løfte problemstillinger knyttet til leverandørforholdet.
- *Relationship Manager* – dette ansvaret er plassert hos en dedikert ressurs hos NBIM. Rollen er operasjonelt ansvarlig for styring og kontroll av leverandørforholdet til Citibank under hele livsløpet for avtalen, herunder innfasing, løpende håndtering og oppfølging, og avslutning av tjenesten.
- *Service Owner* – dette ansvaret tilligger den som har rollen som «Global Head of Fund Administration». Rollen er overordnet ansvarlig for styring og kontroll av tjenesteleveransene, og er øverste eskaleringspunkt hvis det er behov for å drøfte tema knyttet til kvaliteten på tjenestene fra Citibank.
- *Service Manager* – dette ansvaret er plassert hos dedikerte ressurser i NBIM, herunder Head of Transaction Management, Head of Asset Servicing og Head of Tax and Investment Control. Rollene er operasjonelt ansvarlige for styring og kontroll av tjenesteleveranser og kvaliteten på de løpende tjenestene fra Citibank. Rollene er ansvarlige for å påse at tjenestene er i overensstemmelse med definerte krav og kriterier definert i Service Level Agreement (SLA) og Statement of Work (SoW) samt de strategiske målsettingene med utkontrakteringen, og i samsvar med *Policy for Operational Risk Management*.

For hver av rollene er det identifisert ansvarlige på tilsvarende nivå i organisasjonen hos Citibank. Gjennomgangen viser med dette at organisering, roller og ansvar for utkontraktering av depottjenestene til Citibank er definert og plassert i NBIMs organisasjon. Dette vurderes derfor å være i tråd med anbefalingene i EBA guidelines, kapittel 6.

Styrende dokumenter

NBIMs rammeverk, *Management Framework*, beskriver overordnede prinsipper for hvordan de ulike virksomhetsområdene i NBIM skal operere. Dette rammeverket er også gjeldende for utkontraktering av depot- og verdipapiravregning. NBIM har ikke utarbeidet særskilte policyer eller retningslinjer for utkontraktering av depottjenestene eller for beredskapsløsningen for depottjenester. Det vises til kapittel 2.3 Styring og kontroll NBIM ovenfor for en generell vurdering av styring og kontroll av utkontrakterte tjenester.

I selve styringsstrukturen for avtalen med Citibank er det beskrevet hvordan depottjenestene skal følges opp og overvåkes. Styringsstrukturen gir blant annet føringer for *Service Strategy, Service Management, Relationship Management* og *Service Risk*.

- *Service Strategy* – beskriver formålet med utkontraktering av depottjenestene, og stiller krav til at oppfølging og evaluering av utkontrakteringen er i overensstemmelse med NBIMs strategiske mål. Et viktig mål er at kvaliteten på tjenestene bidrar til å operasjonalisere målene om en effektiv modell for gjennomføring av transaksjoner og sikring av investeringer.
- *Service Management* – omfatter den operasjonelle håndteringen av krav og oppfølging av tjenesteleveranser og kvalitet løpende under kontraktsperioden. Alle overordnede krav er definert i en tjenestenivåavtale, *Service Level Agreement* (SLA), først ved inngåelse av avtalen i 2014, og deretter oppdatert i ny avtale av 2022. I tillegg er selve operasjonaliseringen av SLA-kravene beskrevet i en oppdragsbeskrivelse, *Statement of Work* (SoW), som oppdateres årlig. SoW/SLA blir rapportert, overvåket og fulgt opp etter angitte intervaller. Det er i alt 12 funksjonelle områder med en rekke underpunkter som måles, og hvert av de funksjonelle områdene teller inn på en totalt vektet servicegrad. Dette overvåkes fra NBIMs side løpende.
- *Relationship Management* – definerer kommunikasjon og løpende oppfølging av leverandørforholdet og tjenesteleveransene gjennom hele kontraktsperioden. Det er utpekt dedikerte roller i NBIM, og Citibank har etablert en tilsvarende organisering på sin side. Det er en plan for møtepunkter med angitte deltakere, frekvens og formål gjennom året, og denne blir gjennomført og fulgt opp.
- *Service Risk* – risikostyring og risikohåndtering av de globale depottjenestene blir fulgt opp både på leverandørnivå og tjenestenivå. Alle leverandører og tjenester blir gradert avhengig av kritikalitet og risiko. Depottjenesten er vurdert å være en strategisk viktig tjeneste med høy kritikalitet og høy risiko. Det er dermed krav om at risiko skal overvåkes og revurderes periodisk. På grunn av kritikaliteten av tjenesten er det også opprettet en beredskapsløsning for depottjenestene hos BNY Mellon. Det gjennomføres også regelmessige Integrity Due Diligence (IDD)-vurderinger av Citibank og BNY Mellon.

De styrende dokumentene for NBIM vurderes å være hensiktsmessige for å tilrettelegge for god styring og kontroll av utkontraktering av depottjenestene. Rammeverk og prosesser er godt forankret i organisasjonen, og disse er operasjonalisert i den løpende oppfølgingen. NBIM vurderes å ha kompetanse og kapasitet internt for å sikre tilstrekkelig styring og kontroll med Citibank som leverandør, og de utkontrakterte depottjenestene. Dette er i tråd med de forventningene Finanstilsynet angir i rundskrivet, og som de stiller til øvrige banker i Norge. Det vurderes også at styring og kontroll er i henhold til anbefalingene fra EBA guidelines kapittel 6.

Utkontrakteringsprosessen

NBIMs implementerte retningslinjer for leverandøroppfølging, nedfelt i «Provider lifecycle management» med tilhørende dokumenter, legger til rette for helhetlig risikostyring og oppfølging av leverandører. Livssyklusen er bestående av fire faser: *Phase in of new providers, Operational criticality classification, Management* og *Phase out/End of life,* og gjenspeiler EBAs krav om å definere samt spesifisere aktiviteter knyttet til implementerings-, monitorerings- og styringsfasen.

Som følge av kompleksiteten i depotløsningen er NBIM avhengig av å anskaffe løsningen fra en tredjepart, og det er et begrenset antall aktører som kan levere globale depottjenester. I forbindelse med fase 1 i livssyklusen gjennomførte NBIM en *Request for Proposal* (RFP), i perioden fra januar 2021 til september 2022. RFP-prosessen er en del av *Service Strategy* i styringsstrukturen til NBIM, med hensikt om å finne en leverandør som kunne sikre høy kvalitet i tjenesteleveransen. RFP-prosessen endte med fem aktuelle tilbydere. De fem tilbyderne ble målt opp mot hverandre basert på tre hovedtemaer: *Cost*

Benchmarking, *Service Benchmarking* og *Evolving Technologies*. På bakgrunn av NBIMs vurdering av tilbyderne innenfor de tre hovedtemaene og påfølgende due diligence-prosess, ble det vurdert at Citibank skulle fortsette som leverandør av de globale depottjenestene (*Global Custodian*), mens BNY Mellon ble valgt som ny beredskapsløsning (*Contingent Custodian)*. NBIMs *Request For Proposal*-prosess vurderes å være i samsvar med EBAs retningslinjer og Finanstilsynet rundskriv, ettersom det ble gjennomført en forsvarlig og grundig vurdering av *Global Custodian* og C*ontingent Custodian* i forbindelse med anskaffelsen.

EBAs retningslinjer stiller videre krav om definering av prosess og kriterier for risikoidentifikasjon, -vurdering og styring. Fase 2 i NBIMs livssyklus legger til grunn at tjenestens kritikalitet skal redegjøres for, slik at oppfølgings- og overvåkingsaktiviteter kan utføres i overensstemmelse med kritikaliteten. Depottjenestene er av svært høy kritikalitet for NBIM, og er således definert med det øverste nivået av kritikalitet.

Med bakgrunn i at depottjenestene er definert med «svært høy» kritikalitet for NBIM, er det etablert detaljerte interne prosesser, rutiner og kontrollaktiviteter for å sikre hensiktsmessig overvåking og oppfølging av tjenesteleveransen. De overordnede prinsippene for overvåking og oppfølging er nedfelt i fase 3 i «Provider lifecycle management», og de detaljerte kravene for oppfølging av depottjenestene i monitoreringsfasen er beskrevet i tjenesteavtalen med tilhørende SoW og SLA.

Den fjerde fasen omhandler terminering og utfasing av leverandøren. EBAs retningslinjer for utkontraktering stiller forventninger til at det skal være etablert rutiner for termineringsprosessen og at det for kritiske funksjoner, som depottjenestene, skal foreligge en exit-strategi for uforutsett terminering. Depottjenestene leveres i dag fra Citibank som *Global Custodian,* mens BNY Mellon er valgt som beredskapsløsning, *Contingent Custodian*. Dette er resultatet av RFP-prosessen fra 2021-2022. Det utføres årlige interne vurderinger av om BNY Mellon skal erstatte Citibank som *Global Custodian*, og NBIM har anledning til å bytte *Global Custodian* syv år framover uten at det må foreligge en ny RFP-prosess. Ved uforutsette hendelser eller brudd på avtalen med Citibank, har NBIM definert en plan for overgang til BNY Mellon i løpet av én måned. Det skal gjennomføres en beredskapsøvelse sommeren 2024 som tester NBIMs overgang fra Citibank til BNY Mellon. Tilsvarende beredskapsøvelser har blitt utført tidligere år for daværende *Contingent Custodian,* JP Morgan. NBIMs retningslinjer for terminering og exit-strategi for depottjenestene vurderes å være i henhold til EBA sine retningslinjer for utkontraktering.

Bankens risikovurdering

Depottjenestene levert av Citibank er av svært høy kritikalitet for banken og følgelig er risikooppfølging sentralt i utkontrakteringsprosessen. NBIMs ERM-rammeverk legger føringer for vurdering av operasjonell risiko samt iverksetting av risikoreduserende tiltak. Som en konsekvens av at depottjenestene er utkontraktert er det to perspektiver som må hensyntas i risikohåndteringen:

- Operasjonell risiko tilknyttet tjenesteleveranser.
- Operasjonell risiko tilknyttet Citibank som oppdragstaker.

Finanstilsynets rundskriv stiller flere krav til omfanget og innholdet i risikovurderingene. Det må blant annet vurderes hvilke risikoer som følger av utkontrakteringen og at det foreligger rutiner for iverksetting av risikoreduserende tiltak. Risikoen knyttet til tjenesteleveransene er beskrevet i oppdragsbeskrivelsen, *Statement of Work* (SoW), og det er etablert interne rutiner og kontroller hos NBIM for oppfølging og etterlevelse av kravene. Potensielle avvik blir eskalert internt i banken til ulike instanser basert på kritikaliteten av avviket, med utforming og innføring av tilhørende risikoreduserende tiltak. Når det gjelder risikoen knyttet til oppdragstaker ble denne initielt håndtert som en

del av RFP-prosessen, og det foreligger interne rutiner for løpende oppfølging. De årlige tredjepartsrapportene (SOC) for Citibank understøtter at oppdragstaker har etablert en hensiktsmessig internkontroll, og NBIM utfører due diligence-gjennomganger av leverandøren kvartalsvis. I tillegg til å støtte opp under Finanstilsynets rundskriv, støtter også NBIMs rutiner opp under EBAs krav om at det skal foreligge prosess og kriterier for risikovurdering og -styring. Videre påpeker Finanstilsynets rundskriv viktigheten av etablerte rutiner for dokumentering av risikovurderinger. I NBIM dokumenteres og håndteres risikoene i bankens ERM-system, [redacted], med tilhørende beskrivelse, leverandøransvarlig, kritikalitet og risikonivå. NBIMs rutiner er følgelig i henhold til Finanstilsynets krav.

Overvåking og oppfølging

Som nevnt i underkapittelet *Styrende dokumenter* definerer styringsstrukturen i avtalen med Citibank hvordan NBIM skal sikre overvåking og oppfølging depottjenestene. Som følge av kritikaliteten av tjenesteleveransen foreligger en detaljert og tilpasset SoW som fastsetter NBIM sine krav til leverandøren, og denne revideres årlig. Denne inneholder blant annet kravspesifikasjon, Citibank sitt ansvar for ivaretakelse av kravet, ansvarlig og hyppighet. NBIM sin styringsstruktur i kombinasjon med definerte etterlevelseskrav i SoW samsvarer med Finanstilsynets rundskriv for utkontraktering, da det er iverksatt tiltak som tilrettelegger for forsvarlig overvåkning og oppfølging av utkontraktert virksomhet.

Legger vi rundskrivet fra Finanstilsynet til grunn sikrer NBIM videre at retningslinjer og rutiner blir etterlevd, og at avvik blir fanget opp, håndtert og mitigert. For å sikre overvåking og oppfølging av kravene er NBIM organisert i tre funksjonelle områder: *Transaction Management, Asset Servicing* og *Tax Operations*. Mandatet til de funksjonelle områdene er å sikre at Citibank etterlever kravene, og dette kontrolleres gjennom NBIM sine interne rutiner og kontroller. NBIMs rutiner og kontroller har som formål å fange opp potensielle avvik, og dette følges opp gjennom faste møtepunkter, ad hoc-dialog og mottak av rapporter. Citibank har på sin side omtrentlig 40 årsverk som er dedikert til NBIM, for å understøtte NBIM sine retningslinjer og rutiner relatert til overvåking og oppfølging.

I tillegg til den løpende oppfølgingen av kravene, foreligger det også formaliserte rapporteringskrav og møtepunkter. Hvert kvartal avholdes det *Strategic Review Meeting* og *Service Review Meeting* mellom avtalepartene. Videre er Citibank påkrevd å rapportere *Service Level Agreement performance*-rapport kvartalsvis som definerer tjenesteytelse og planlagte tiltak for å redusere eventuelle vesentlige avvik. I tillegg er det etablert faste rapporteringer internt i NBIM og til hovedstyret, herunder:

- Rapport til «Chief Governance & Compliance Officer» månedlig.
- Rapport til hovedstyret om NBIMs risikobilde inkludert kritiske og signifikante hendelser kvartalsvis.
- Offentlig rapportering halvårlig og årlig.
- Rapport til hovedstyret om NBIMs risikobilde og internkontroll årlig.

NBIMs rapporteringer, både internt og mot leverandør, er i henhold til Finanstilsynet rundskriv for utkontraktering ettersom det er etablert faste rapporterings-, oppfølgings- og kontrolltiltak som regelmessig vurderes.

Videre stiller rundskrivet krav om regelmessig gjennomgang av oppdragstakers systemer for å ha mulighet til å iverksette tiltak om det avdekkes avvik. I tillegg til at NBIM har designet interne kontrollrutiner, utstedes det årlige SOC-rapporter for Citibank som omfatter *Global Custody* og *Securities Lending,* utført av KPMG. SOC-rapportene dekker prosessene og kontrollene leverandøren har implementert for å sikre effektiv internkontroll for depottjenestene, herunder kontroller knyttet til underleverandører, tilgangsstyring samt endrings- og hendelseshåndtering. For perioden som strekker seg fra oktober 2021 til

desember 2023, er det ikke rapportert om noen avvik i SOC-rapportene. NBIM har også rutiner for årlig oppfølging og gjennomgang av SOC-rapportene for å vurdere om det bør utføres endringer i eksisterende rutiner og kontroller eller iverksettes ytterligere kontroller. Samtidig gjennomfører NBIM periodiske due diligence-gjennomganger av leverandørene. For Citibank blir disse utført kvartalsvis grunnet kritikaliteten av tjenesteleveransen. Implementerte retningslinjer og rutiner for overvåking og oppfølging av leverandøren vurderes å være i henhold til EBAs retningslinjer for utkontraktering.

Oppfølging av underleverandører

Citibank benytter underleverandører, blant annet lokale depotbanker, i 71 markeder for depottjenestene som leveres til NBIM. 58 av markedene er filialer eller datterselskap av Citibank, én lokalbank er delvis eid av Citibank, én er en internasjonal verdipapirsentral (Euroclear) og elleve er finansinstitusjoner levert av en tredjepart. I avtalen mellom Citibank og NBIM er det definert at leverandøren har ansvaret for underleverandørene som benyttes i tjenesteleveransene til NBIM. Med dette innebærer det at Citibank er ansvarlig for å stille sikkerhetskrav til underleverandørene, samt følge opp etterlevelsen av disse. Videre står Citibank ansvarlig for eventuelle tap som forårsakes av underleverandørene i tjenesteleveransene mot NBIM.

Citibank har tilgjengeliggjort en oversikt over de underleverandørene som benyttes i leveransene direkte mot NBIM. Det stilles krav i SoW om at Citibank skal informere NBIM om endringer i underleverandørene før disse trer i kraft. NBIM foretar risikovurderinger av de viktigste lokale depotbankene som benyttes av Citibank, herunder filialene og datterselskapene av Citibank samt Euroclear. I de markedene som leveres av tredjepart, og som NBIM har investeringsmidler i, benyttes anerkjente finansinstitusjoner. De lokale depotbankene er også under tilsyn av lokale finanstilsynsmyndigheter. NBIMs vurderinger av operasjonell- og omdømmerisiko anses derfor som begrenset for Citibanks lokale depotbanker. I tillegg fører NBIM løpende operasjonell statistikk på kvalitet i depottjenestene i hvert enkelt marked de opererer eller investerer i, og kvalitetsbrudd eskaleres til Citibank. Til tross for at NBIM utfører risikovurderinger, er det kommunisert at vurderingene kunne vært bedre dokumentert, og med henvisning til hvilket rammeverk som benyttes i prosessen. Det utføres videre en årlig due diligence-prosess hos Citibank for å følge opp underleverandørene, og NBIM har gjort en vurdering av denne prosessen for å påse at prosessen er hensiktsmessig i henhold til NBIM sine retningslinjer. Dette støtter opp under EBAs retningslinjer for utkontraktering som understreker at tjenesteleverandør skal føre tilsyn med underleverandører i tråd med virksomhetens retningslinjer.

Når det gjelder øvrige underleverandører som Citibank benytter, utover de lokale depotbankene, er det ikke stilt særskilte krav til disse i avtalen. Dette kan eksempelvis være underleverandører som leverer applikasjoner og IT-infrastruktur til Citibank N.A. og som benyttes i utøvelsen av tjenesteleveransen.

Dersom underleverandører benyttes i utkontrakteringen, stiller Finanstilsynets rundskriv krav om at dette skal følge av avtalen. SoW foreligger som et detaljert vedlegg til avtalen mellom Citibank og NBIM. Her defineres spesifikke krav i tjenesteleveransen, inkludert krav til Citibank sine underleverandører, som er i tråd med Finanstilsynets rundskriv. Under seksjonen *Network Management* i SoW stilles det krav knyttet til oppfølging av underleverandører, herunder krav om at Citibank skal fasilitere for direkte kontakt mellom NBIM og underleverandørene. Det stilles også krav om at leverandøren månedlig skal rapportere ytelse på tjenestene som leveres fra underleverandørene til Norges Bank. Videre er Citibank pålagt å rapportere endringer og fremtidsplaner for underleverandørene årlig. Øvrige krav relatert til underleverandører i SoW omhandler depot- og verdipapirtjenestene, og er ikke direkte knyttet til oppfølgingen av underleverandørene. SoW gjennomgås og oppdateres årlig for å sørge for at definerte krav er hensiktsmessige.

3.2.2 Anbefalinger for å styrke styring og kontroll av utkontrakterte depottjenester

BDO vil repetere anbefalingen knyttet til bestemmelser, risikovurdering og oppfølging av underleverandører fra kapittel *2.3.3 Anbefalinger* ovenfor, da denne også er relevant for utkontraktering av depottjenester:

- Detaljere bestemmelser og retningslinjer knyttet til risikovurdering av oppdragstakers underleverandører, utover de lokale depotbankene, i NBIMs rammeverk for utkontraktering. Det er vår oppfatning at det formelle ansvaret i stor grad er plassert hos oppdragstaker. Underleverandører har potensial til å påvirke ulike risikoelementer, for eksempel operasjonell- eller omdømmerisiko. Videre bør rammeverket spesifisere hvor mange ledd i verdikjeden en slik vurdering skal omfatte.

Det er ikke identifisert øvrige anbefalinger knyttet til oppfølging av de globale depottjenestene som leveres fra Citibank eller til beredskapsløsningen som leveres fra BNY Mellon.

Vedlegg

4. Vedlegg

4.1 Oppsummerte anbefalinger

ID	Kapittel	Anbefaling
1	2.1 Overordnet styring og kontroll	For å styrke bankens styring og kontroll med utkontraktering, anbefaler vi å videreutvikle rolleforståelsen når det gjelder prosessansvarlig for anskaffelser. Her har vi særlig pekt på behovet for å inkludere ytterligere bestemmelser knyttet til: - ansvar for å sørge for en grundigere vurdering av leverandørers og eventuelt underleverandørers virksomhetsstyring - øvrige roller i utkontrakteringsprosessen og deres samspill med rollene behovseier og prosessansvarlig.
2	2.1 Overordnet styring og kontroll	For å styrke bankens styring og kontroll med utkontraktering, anbefaler vi å styrke styrende fellesdokumenter vedrørende utkontraktering for banken ytterligere. Vi peker særlig på behovet for: - nærmere presisering av ansvar for gjennomføring av risikovurderinger og vurdere behov for risikoreduserende tiltak. - å definere overordnede prinsipper for eller minstekrav til risikovurderinger knyttet til utkontraktering. Her vil det blant annet være viktig å inkludere krav til o Vurdering av risiko knyttet til leverandørens virksomhetsstyring. I denne sammenhengen kan det være relevant å se til krav til vurderinger i tråd med den norske anbefalingen om eierstyring og selskapsledelse fra Norsk utvalg for eierstyring og selskapsledelse, OECDs nylige oppdaterte retningslinjer for flernasjonale selskaper, åpenhetsloven og/eller forventninger til leverandøroppfølging i EUs ulike lovkrav for bærekraftsrapportering. o Vurdering av risiko knyttet til terminering av kontrakten, f.eks. mulighet for overføring til en annen leverandør eller inkorporering i egen drift. - å definere overordnede prinsipper for oppfølging, rapportering og kontrolltiltak utover å slå fast at utkontrakteringen skal omfattes av internkontroll. - å fastlegge prinsipper knyttet til hvilke beslutninger og vurderinger som skal dokumenteres når og hvor i utkontrakteringsprosessen.
3	2.2 Styring og kontroll SBV	Sørge for tydelig definisjon av rollen som avtaleeier og andre relevante roller som er involvert i utkontraktering, særlig hvordan disse rollene spiller sammen med rollene behovseier eller prosessansvarlig for anskaffelse.
4	2.2 Styring og kontroll SBV	For å styrke bankens styring og kontroll med utkontraktering, anbefaler vi å vurdere å utvikle et selvstendig dokument for utdypende veiledning av hele utkontrakteringsprosessen for å tydeliggjøre blant annet: - de ulike fasene av utkontrakteringsprosessen - hva som forventes i de ulike fasene med særlig fokus på definerte minimumskrav - hva som forventes av vurderinger knyttet til personvern - hva som forventes av vurderinger og dokumentasjon knyttet til habilitet og interessekonflikter - hva som forventes av vurderinger knyttet til leverandørens og underleverandørers virksomhetsstyring - hva som forventes av vurderinger knyttet til exit-strategi - hva som forventes av aktiviteter og vurderinger i fasen for oppfølging, spesielt hvordan kritiske resultater fra risikovurderinger i anskaffelsesfasen overføres til oppfølgingstiltak i fasen for oppfølging - tilknytning til andre dokumenter i SBVs dokumenthierarki - forventninger til malbruk og andre verktøy - forventninger til dokumentasjon av viktige vurderinger og sentrale beslutninger.

5	2.3 Styring og kontroll NBIM	Styrke styrende dokumenter og operasjonalisering i utkontrakteringsprosessen, herunder: - Tydeliggjøring av ansvar hos stabs- og støttefunksjoner ved utkontraktering. o Her bør det beskrives ytterligere hvilke funksjoner som skal involveres i de ulike stadiene i utkontrakteringsprosessen. Presiseringen bør inkludere involvering av kontrollfunksjoner i andrelinje, samt andre støttefunksjoner som eksempelvis juridisk, IT og risk. - Integrering av retningslinjer for avslutning av avtaler (exit-strategier) i NBIMs rammeverk for utkontraktering. - Etablere prinsipper for å analysere operasjonelle hendelser, spesielt ved mislykkede eller utilstrekkelige ytelser fra oppdragstaker, i regelmessige scenarioanalyser. o Frekvens og krav til innhold i slike analyser kan spesifiseres i policy og rutinedokumenter på et overordnet nivå. - Detaljere bestemmelser og retningslinjer knyttet til risikovurdering av oppdragstakers underleverandører i NBIMs rammeverk for utkontraktering.
6	3.1 Styring og kontroll depottjenester / 3.2 Etterlevelse av rammeverk depottjenester	Detaljere bestemmelser og retningslinjer knyttet til risikovurdering av oppdragstakers underleverandører, utover de lokale depotbankene, i NBIMs rammeverk for utkontraktering. Det er vår oppfatning at det formelle ansvaret i stor grad er plassert hos oppdragstaker. Underleverandører har potensial til å påvirke ulike risikoelementer, for eksempel operasjonell- eller omdømmerisiko. Videre bør rammeverket spesifisere hvor mange ledd i verdikjeden en slik vurdering skal omfatte.

4.2 Oversikt over gjennomgåtte dokumenter

Listen nedenfor viser dokumenter vi har gjennomgått, og som våre analyser og vurderinger bygger på. Dokumentene er i hovedsak mottatt fra banken. Enkelte dokumenter er eksterne, offentlig publiserte dokumenter. Vi gjør oppmerksom på at det kan forekomme direkte sitater eller annen form for gjengivelse fra disse dokumentene i rapporten uten at dette er eksplisitt markert. Dette fordi vi mener dette gjør leseflyten i rapporten bedre, og at rapporten ikke underligger akademiske krav til kildereferanser.

ID	Dokument	Relevant for
1	[redacted]	Felles
2		Felles
3		Felles
4		Felles
5		Felles
6		Felles
7		Felles
8		NBIM
9		NBIM
10		NBIM
11		NBIM
12		NBIM
13		NBIM
14		NBIM

15	[redacted]	NBIM
16		NBIM
17		NBIM
18		NBIM
19		NBIM
20		SBV
21		SBV
22		SBV
23		SBV
24		SBV
25		SBV
26		SBV
27		SBV
28		SBV
29		SBV
30		SBV
31		SBV
32		SBV
33		SBV
34		SBV
35		SBV
36		SBV
37		SBV
38		SBV
39		SBV
40		SBV
41		SBV
42		SBV
43		SBV
44		SBV
45		SBV
46		SBV

47	[redacted]	SBV
48		SBV
49		SBV
50		SBV
51		SBV
52		SBV
53		SBV
54		SBV
55		SBV
56		SBV
57		SBV
58		SBV
59		SBV
60		SBV
61		SBV
62		SBV
63		SBV
64		SBV

4.2.1 Intility - Dokumentasjon for test av etterlevelse

ID	Dokument	Relevant for
1	Driftsavtale - Norges Bank virksomhetskritiske systemer 1250209_1_1	Intility
2	PVS Bilag 1 - Kravspesifikasjon 1250211_1_1	Intility
3	PVS Bilag 2 - Leverandørens løsningsbeskrivelse 1250212_1_1	Intility
4	PVS Bilag 6 - Administrative bestemmelser 07052020 1250236_1_1	Intility
5	PVS - Innstilling og anskaffelse - Styringsgruppen	Intility

4.2.2 Orange Business Services - Dokumentasjon for test av etterlevelse

ID	Dokument	Relevant for
1	Driftsavtale - Norges Bank samfunnskritiske systemer 1251340_1_1	Orange
2	PSS Bilag 1 - Kravspesifikasjon 1251342_1_1	Orange
3	PSS Bilag 2 - Leverandørens løsningsbeskrivelse 1254473_1_1	Orange
4	PSS Bilag 6 - Administrative bestemmelser 1254494_1_1	Orange

4.2.3 Amazon Web Services - Dokumentasjon for test av etterlevelse

ID	Dokument	Relevant for
1	Generell introduksjon AWS i NBIM	Amazon
2	SOC 1 - Spring 2023	Amazon
3	SOC 1 - Terms and conditions	Amazon
4	Confluence ved onboarding for tjenesten fargate	Amazon
5	Confluence ved onboarding for IT-solutions	Amazon
6	Confluence ved onboarding av AWS-Services	Amazon
7	2nd line assessment (NBIM Compliance)	Amazon
8	NBIM Code of Conduct Assessment AWS	Amazon
9	«Sign-off Compliance» AWS 2018	Amazon
10	Security Evaluation of AWS - 2018	Amazon

4.2.4 Citibank N.A. - Dokumentasjon for test av etterlevelse

ID	Dokument	Relevant for
1	231219 NBIM Presentation to BDO on Citi custody services and management	Citibank
2	231222 NBIM Presentation to BDO - Avtaleverk om utkontraktering av depottjenester Citi	Citibank
3	Citi - GC Bridge Letter - covering period to 31 December 2023	Citibank
4	Citi SOC 1 Sept30 2023 - GlobalCustodySecuritiesFinanceSystem	Citibank
5	Hendelse a - NBIM hendelseslogg	Citibank
6	Hendelse b - Citi Incident Report	Citibank
7	SLA - GCA Schedule 1 2_SRD Introduction schedule_Execution	Citibank
8	SLA - Global Custody Agreement (GCA)- Schedule 1 - Service Level Agreement (SLA)	Citibank
9	SOC - GC Bridge Letter - covering period to 31 December 2022	Citibank
10	SOC - GC Citi Securities Services SOC-Report Oct 31-Sep 22	Citibank
11	SOW - NBIM Citi SOW Draft Dec 2023 - for legal review in January24	Citibank