Deloitte.

Uavhengig attestasjonsoppdrag for Norges Banks representantskap vedrørende risikostyringen i Norges Bank Investment Management. Oppdraget omfatter en gjennomgang av utforming og implementering av organisasjonsstruktur og rammeverk for styring av operasjonell risiko.

Februar 2010

Innhold

1. Sammendrag og konklusjon

Innledning

Norges Banks representantskap (Representantskapet) har engasjert Deloitte AS (Deloitte) til å foreta en uavhengig gjennomgang av utforming og implementering av organisasjonsstruktur og rammeverk for styring av operasjonell risiko i Norges Bank Investment Management (NBIM). Betegnelsen NBIM omfatter også Norges Banks hovedstyre i tillegg til NBIMs ledelse. Vår oppgave er å gi Representantskapet betryggende sikkerhet, i overensstemmelse med Standard for Attestasjonsoppdrag 3000 (SA 3000), for at:

- NBIM har utformet og implementert organisasjonsstruktur og rammeverk for styring av operasjonell risiko i henhold til anerkjent rammeverk og relevante standarder.
- NBIM har fulgt opp anbefalingene i rapporten «Risk Management Framework Assessment Government Pension Fund – Global» (2007) utarbeidet av Ernst & Young som gjort rede for i Norges Banks brev til Finansdepartementet datert 19. desember 2007 og 12. februar 2009 (for anbefalingene som gjelder organisasjonsstruktur og operasjonell risiko). Rapporten er i det etterfølgende referert til som «den tidligere gjennomgangen av risikostyringen».

Oppdraget er todelt hvor hver oppdragsdel har forskjellig formål og bakgrunn, og vårt arbeid og vurdering er følgelig omtalt i to separate deler.

Arbeid utført og målekriterier

Som avtalt i vårt engasjementsbrev til Sentralbankrevisor datert 21. september 2009, har vi utført vårt arbeid i samsvar med SA 3000. Vår oppgave er å gi Representantskapet betryggende sikkerhet for at NBIM har utformet og implementert en organisasjonsstruktur og et rammeverk for styring av operasjonell risiko i samsvar med målekriteriene beskrevet nedenfor.

Vi har tatt utgangspunkt i de standardene som NBIM har lagt til grunn for utforming og implementering av sin risikostyring. Kriteriene som følger av disse standardene, i tillegg til anbefalingene i den tidligere gjennomgangen av risikostyringen, inngår i målekriteriene som er benyttet i vurderingen av om organisasjonsstruktur og rammeverk for styring av operasjonell risiko er etablert i henhold til anerkjent rammeverk og relevante standarder. Følgende standarder er lagt til grunn:

- COSO[1], Helhetlig risikostyring – et integrert rammeverk – september 2004 («COSO ERM»).
- Forskrift om risikostyring og internkontroll[2].

Standardene representerer anerkjente rammeverk og er relevante målekriterier for NBIMs organisasjonsstruktur og rammeverk for styring av operasjonell riskostyring. Andre internasjonale standarder foreligger, og måling mot disse kunne gitt et annet resultat.

Løpende utvikling av risikostyringen

Etter den tidligere gjennomgangen av risikostyringen i 2007, har NBIM fått ny ledelse og gjennomført en større omorganisering. Det medfører at flere elementer i organisasjonsstrukturen og rammeverket for styring av operasjonell risiko observert i 2007 er endret og har vært gjenstand for løpende utvikling. Noen elementer i den operasjonelle risikostyringen er nylig innført som en del av NBIMs pågående forbedringer av risikostyringen.

Avgrensning av oppdraget

De deler av risikostyringen som omhandles i denne gjennomgangen, er organisasjonsstruktur og rammeverket for styring av operasjonell risiko. Andre komponenter i NBIMs rammeverk for styring av risiko faller utenfor denne gjennomgangen.

COSO ERM og forskrift om risikostyring og intern kontroll omfatter begge helhetlig risikostyring. Vi har vurdert NBIMs rammeverk for styring av operasjonell risiko opp mot de deler av disse standardene som er relevante for utforming og implementering av den operasjonelle risikostyringen.

[1] The Committee of Sponsoring Organizations of the Treadway Commission.
[2] FOR 2008-09-22 nr 1080, forskrift fastsatt av Finanstilsynet.

Vi har utelukkende vurdert anbefalingene i den tidligere gjennomgangen av risikostyringen i den utstrekning de gjelder utforming og implementering av organisasjonsstruktur og operasjonell risiko. Andre anbefalinger i den tidligere gjennomgangen faller utenfor denne gjennomgangens omfang.

Oppdraget dekker ikke kontroll av om den etablerte organisasjonsstruktur eller rammeverk for styring av operasjonell risiko har vært effektiv og fungert etter forutsetningene.

Oppdraget dekker ikke vurdering av om risikoene som NBIM har identifisert, er fullstendige og dekkende for NBIMs virksomhet, eller godheten i de kontrolltiltak som er etablert.

Bakgrunn

Vi har utført vårt arbeid i henhold til SA 3000. Omfang og avgrensning av oppdraget fremgår av avsnitt 3.2 og 4.2.

Vår konklusjon må sees i sammenheng med at:

- NBIM løpende videreutvikler sine prosesser for styring av operasjonell risiko og enkelte aktiviteter er nylig innført.
- Konklusjonen er basert på NBIMs risikostyring slik den er utformet og implementert på tidspunktet for datering av denne rapporten.
- Selv om vi har gitt én konklusjon for de to separate delene i vår gjennomgang, er de av ulik karakter. Både COSO ERM og forskrift om risikostyring og internkontroll er uavhengige objektive kriterier, mens anbefalingene i den tidligere gjennomgangen av risikostyringen er gjort på bakgrunn av NBIMs organisasjon slik den var på ett bestemt tidspunkt (2007). I perioden siden den gang har NBIM fått ny ledelse og gjennomgått en større omorganisering. NBIM har i denne prosessen løpende vurdert hvordan og i hvilken grad anbefalingene i den tidligere gjennomgangen av risikostyringen er relevante å implementere i ny organisasjonsstruktur.

Konklusjon

Del 1 – Samsvar med COSO ERM og forskrift om risikostyring og internkontroll

Utforming

Forskrift om risikostyring og internkontroll

Vi mener at organisasjonsstrukturen og rammeverket for styring av operasjonell risiko i det alt vesentlige er utformet i samsvar med prinsippene i forskrift om risikostyring og internkontroll.

COSO ERM

Vi mener at organisasjonsstrukturen i det alt vesentlige er utformet i samsvar med prinsippene i COSO ERM.

Vi mener at rammeverket for styring av operasjonell risiko i det alt vesentlige er utformet i samsvar med prinsippene i COSO ERM, med unntak av følgende forhold (som er beskrevet i mer detalj i avsnitt 3.4.2):

- Konsekvenser av en operasjonell risikos påvirkning på andre operasjonelle risikoer (korrelasjon) vurderes ikke på en systematisk måte, og enkeltrisikoer kobles ikke med andre risikoer.
- Risikovurderingen tar utgangspunkt i gjenværende risiko etter at internkontrolltiltak er hensyntatt og omfatter ikke en systematisk vurdering av iboende risiko (før internkontrolltiltak).

Implementering

Vi mener at organisasjonsstrukturen og rammeverket for styring av operasjonell risiko i det alt vesentlige er implementert slik det er utformet.

Del 2 – Den tidligere gjennomgangen av risikostyringen

Vi mener at NBIM i all vesentlighet har fulgt opp anbefalingene fra den tidligere gjennomgangen av risikostyringen som gjelder organisasjonsstruktur og rammeverket for styring av operasjonell risiko slik det er redegjort for i Norges Banks brev til Finansdepartementet av 19. desember 2007 og 12. februar 2009, med unntak for følgende forhold (som er beskrevet i mer detalj i avsnitt 4.4.2):

- Manglende kobling av operasjonell risikoappetitt med stress-scenarioer.
- Nøkkelrisikoindikatorer («Key Risk Indicators», KRI) er ikke etablert som en del av overvåkningen av risikoeksponeringen.

Oslo, 25. februar 2010
Deloitte AS

Aase Aa. Lundgaard

2. Innledning

Vårt oppdrag

Representantskapet har engasjert Deloitte til å foreta en uavhengig gjennomgang av utforming og implementering av organisasjonsstruktur og rammeverk for styring av operasjonell risiko i NBIM. Vår oppgave er å gi Representantskapet betryggende sikkerhet, i overensstemmelse med SA 3000, for at:

- NBIM har utformet og implementert organisasjonsstruktur og rammeverk for styring av operasjonell risiko i henhold til anerkjent rammeverk og relevante standarder.
- NBIM har fulgt opp anbefalingene i rapporten fra den tidligere gjennomgangen av risikostyringen som gjort rede for i Norges Banks brev til Finansdepartementet datert 19. desember 2007 og 12. februar 2009 (for anbefalingene som gjelder organisasjonsstruktur og operasjonell risiko).

Attestasjonsoppdrag er definert i SA 3000 som «et oppdrag der en praktiserende revisor gir uttrykk for en konklusjon som er ment å øke graden av tillit hos de tiltenkte brukerne som ikke er ansvarlig part vedrørende vurderingen av eller målingen av saksforholdet mot kriterier.»

I denne rapporten defineres begrepene fra SA 3000 som følger:

- «Tiltenkte brukere» – Norges Banks representantskap.
- «Ansvarlig part» – NBIM.
- «Saksforhold» – NBIMs organisasjonsstruktur og rammeverk for operasjonell risiko.
- «Kriterier» – de relevante standardene gjort rede for i avsnitt 3.1 og anbefalingene i 4.1.

I løpet av de siste to årene har NBIM fått ny ledelse og gjennomført en større omorganisering. Det medfører at flere elementer i organisasjonsstrukturen og rammeverket for styring av operasjonell risiko observert i 2007 er endret, og har vært gjenstand for løpende utvikling. Vi har hensyntatt denne dynamikken i vår gjennomgang.

Rapportens struktur

Oppdraget er todelt hvor hver oppdragsdel har forskjellig formål og bakgrunn, og vårt arbeid og vurdering er følgelig omtalt i to deler:

- **Del 1 – Samsvar med COSO ERM og forskrift om risikostyring og internkontroll**, gir en vurdering av NBIMs organisasjonsstruktur og rammeverk for operasjonell risiko målt mot anerkjent rammeverk og relevante standarder.
- **Del 2 – Tidligere gjennomgang av risikostyringen (oppfølging)**, gir en vurdering av om anbefalingene som ble gitt i rapporten har blitt fulgt opp og implementert i organisasjonsstrukturen og i rammeverket for operasjonell risikostyring i NBIM.

3. Del 1 – Samsvar med COSO ERM og forskrift om risikostyring og internkontroll

3.1 Metodikk og målekriterier

Vår gjennomgang har tatt utgangspunkt i de standardene NBIM har lagt til grunn for utforming og implementering av sin risikostyring. Kriteriene som følger av disse standardene inngår i *målekriteriene* som er benyttet i vurderingen av om organisasjonsstruktur og rammeverk for styring av operasjonell risiko, er etablert i henhold til anerkjent rammeverk og relevante standarder. Følgende standarder er lagt til grunn:

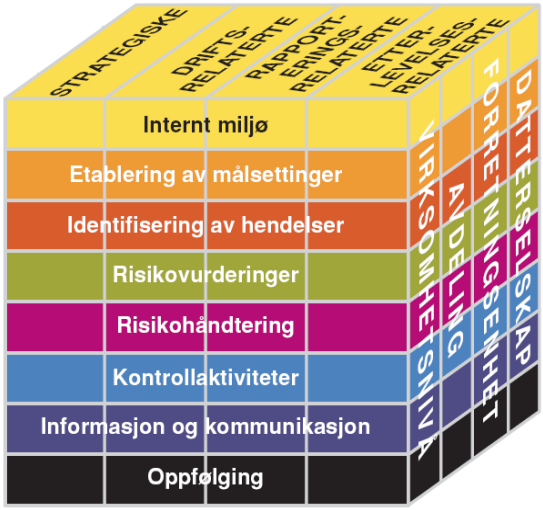
- COSO Helhetlig risikostyring – et integrert rammeverk – september 2004 («COSO ERM»).
- Forskrift om risikostyring og internkontroll.

Standardene representerer anerkjente rammeverk og er relevante målekriterier for NBIMs organisasjonsstruktur og rammeverk for styring av operasjonell riskostyring. Andre internasjonale standarder foreligger, og måling mot disse kunne gitt et annet resultat.

COSO Helhetlig risikostyring – et integrert rammeverk

COSO-rammeverket for helhetlig risikostyring er illustrert som en kube med tre flater som representerer ulike dimensjoner og områder. Rammeverket er illustrert på følgende måte:

- Fremsiden av kuben viser de åtte hovedområdene, eller komponentene i rammeverket. Disse åtte komponentene med tilhørende underpunkter utgjør hovedstrukturen i vår gjennomgang.
- Den høyre siden av kuben illustrerer at rammeverket skal implementeres i virksomhetens ulike nivåer og enheter.
- Den øvre siden illustrerer at risikostyring utøves innen rammen av organisasjonens målsettinger, og viser de fire målsettingskategoriene knyttet til strategi, drift, rapportering og etterlevelse.
- Ved bruk av rammeverket skal hver av de åtte komponentene vurderes i lys av virksomhetens målsettinger og hvordan de anvendes på ulike organisasjonsnivå i virksomheten.



Kilde: COSO - *Helhetlig risikostyring – et integrert rammeverk (2004), oversatt av Norges Interne Revisorers Forening*

Forskrift om risikostyring og internkontroll

Forskrift om risikostyring og internkontroll er gjennom tidligere vedtak i Norges Banks hovedstyre gjort gjeldende for Norges Banks virksomhet, herunder NBIM.[3]

Forskriften omhandler:

- Ansvar for risikostyring og internkontroll.
- Dokumentasjon av risikostyring og internkontroll.
- Uavhengig bekreftelse av risikostyringen og internkontroll.

Forskrift om risikostyring og internkontroll er basert på COSO ERM, men er ikke like detaljert. Følgelig kan det oppstå avvik i forhold til COSO ERM som ikke utgjør avvik målt mot forskrift om risikostyring og internkontroll.

[3] Forskrift om risikostyring og internkontroll i Norges Bank (FOR 2009-12-17 nr.1630) er gjort gjeldende med virkning fra og med 2010.

3.2 Avgrensning av oppdraget

Saksforhold

Følgende saksforhold er vurdert:

- Organisasjonsstruktur: Vi har vurdert viktige deler av NBIMs styringsstruktur, herunder risikostyrings- og compliancefunksjonen. Vi har vurdert organisasjonsstrukturen opp mot COSO komponenten internt miljø, herunder roller og ansvar i tillegg til relevante bestemmelser i forskrift om risikostyring og internkontroll.
- Operasjonell risiko: Vi har vurdert NBIMs rammeverk for styring av operasjonell risiko, herunder definisjon, identifisering, vurdering, styring, overvåkning og rapportering av risiko, samt etablering av toleransegrenser for risiko. Vi har vurdert alle åtte COSO komponenter i tillegg til relevante bestemmelser i forskrift om risikostyring og internkontroll.

Andre deler av NBIMs rammeverk for styring av risiko faller utenfor omfanget av denne gjennomgangen.

Målekriterier

COSO ERM og forskrift for risikostyring og internkontroll er anerkjente og relevante rammeverk. Disse rammeverkene omhandler helhetlig risikostyring og er ikke spesielt rettet mot styring av operasjonell risiko. Vi har vurdert NBIMs rammeverk for styring av operasjonell risiko opp mot de deler av disse standardene som er relevante for utforming og implementering av operasjonell risikostyring.

I enkelte tilfeller har det vært nødvendig å gjøre fortolkninger for å fastsette hvordan målekriteriene skulle anvendes for NBIMs virksomhet. Vi har basert fortolkningen på eksemplene som fremgår i COSO ERM, «Teknikker og verktøy», vår erfaring fra risikostyring i andre organisasjoner og diskusjoner med NBIMs ledelse.

Vi har tatt utgangspunkt i de standarder som NBIM har lagt til grunn for sin risikostyring. Andre internasjonale standarder foreligger, og bruk av disse kunne gitt et annet resultat.

Kontrolleffektivitet (etterlevelse)

Oppdraget har ikke omfattet en vurdering av om den etablerte organisasjonsstruktur eller rammeverk for styring av operasjonell risiko har vært effektiv og fungert etter forutsetningene. Kontrolleffektivitet (etterlevelse) omfatter hvordan en kontrollprosedyre gjennomføres, hvor konsistent den gjennomføres, og hvem som gjennomfører den over en bestemt periode.

Risikoeksponering og internt miljø

Oppdraget har ikke omfattet en vurdering av om risikoene som NBIM har identifisert, er fullstendige og dekkende for NBIMs virksomhet, eller godheten i de kontrolltiltak som er etablert.

Andre risikoer enn de som er identifisert av NBIM, kan være aktuelle, og risikoer som faktisk er identifisert av NBIM, kan vise seg å ha andre konsekvenser enn de er vurdert å ha i dag.

3.3 Arbeid utført

Standard for Attestasjonsoppdrag 3000 (SA 3000)

Som avtalt i vårt engasjementsbrev til Sentralbankrevisor datert 21. september 2009, har vi utført vårt arbeid i samsvar med SA 3000. Vår oppgave er å gi Representantskapet betryggende sikkerhet for at NBIM har utformet og implementert organisasjonsstruktur og rammeverk for styring av operasjonell risiko i samsvar med målekriteriene beskrevet i avsnitt 3.1.

Et attestasjonsoppdrag som skal gi betryggende sikkerhet i henhold til SA 3000, krever at vi planlegger og utfører arbeidet slik at vi oppnår høy, men ikke absolutt sikkerhet for at saksforholdet er i samsvar med målekriteriene. Vårt arbeid er beskrevet nedenfor.

Vurderingsgrunnlag og målekriterier

Vi har utarbeidet en detaljert oversikt over de aktuelle målekriteriene fra COSO ERM med utgangspunkt i de åtte komponentene i rammeverket. Aktuelle bestemmelser fra forskrift om risikostyring og internkontroll ble henført til de relevante COSO ERM komponentene og innarbeidet i vurderingsgrunnlaget og målekriteriene.

Vurdering av organisasjonsstruktur og rammeverk for operasjonell risikostyring mot målekriteriene

Vi har vurdert om NBIMs organisasjonsstruktur og rammeverk for styring av operasjonell risiko var utformet og implementert i samsvar med de etablerte målekriteriene. Et element av rammeverket for styring av operasjonell risiko eller organisasjonsstruktur er utformet i overensstemmelse med kriteriene dersom det – enkeltvis eller i kombinasjon med andre elementer – med høy sannsynlighet bidrar til å nå den aktuelle målsettingen som vurderes (strategi, drift, rapportering eller etterlevelse).

Begrepet implementert omfatter iverksettelse av de aktiviteter som følger av utformingen, men omfatter ikke den faktisk løpende gjennomføringen av disse aktivitetene eller i hvilken utstrekning de fungerer etter forutsetningene.

Vi har i vår gjennomgang ikke vurdert om den etablerte organisasjonsstrukturen eller rammeverket for operasjonell risikostyring har vært effektivt og fungert etter forutsetningene.

Vurdering av utforming

Vi har mottatt dokumenter som beskriver NBIMs organisasjonsstruktur og rammeverk for styring av operasjonell risiko. Vi har gjennomgått dokumenter som omfatter policyer, prosedyrer, retningslinjer, møtereferat, mandater og ledelsesrapporter.

Vi har avholdt flere møter med ledelsen i NBIM hvor det ble redegjort for utformingen av rammeverket for styring av operasjonell risiko og organisasjonsstruktur.

Vi har sammenstilt de viktigste delene av rammeverket for operasjonell risikostyring og organisasjonsstruktur med målekriteriene, vurdert dokumentasjon og innhentet informasjon. Vi har vurdert om det forelå avvik mot de aktuelle standardene sett i sammenheng med NBIMs overordnede målsettinger. Avvikene er gjengitt i denne rapporten.

Vurdering av implementering

For de vesentlige elementene i utformingen av NBIMs organisasjonsstruktur og rammeverk for styring av operasjonell risiko har vi vurdert dokumentasjon og innhentet informasjon for å underbygge vår vurdering av implementeringen.

Vi har forespurt NBIM om aktuell dokumentasjon og informasjon og har notert våre observasjoner i arbeidsverktøyet.

Avvikene er gjengitt i denne rapporten.

3.4 Funn: COSO ERM og forskrift om risikostyring og internkontroll

Bakgrunn

Våre konklusjoner må sees i sammenheng med at:

- COSO ERM er et relativt omfattende rammeverk hvor prinsippene reflekterer en etablert organisasjonsstruktur og struktur for risikostyring som har vært virksom over en lengre periode.
- NBIM utvikler løpende sine prosesser for styring av operasjonell risiko, og på flere områder er NBIMs rammeverk for styring av operasjonell risiko forskjellig fra COSO ERM.
- COSO ERM og forskrift om risikostyring og internkontroll omfatter helhetlig risikostyring. Vi har vurdert NBIMs rammeverk for styring av operasjonell risiko opp mot de deler av disse standardene som er relevante for utforming og implementering av operasjonell risiko.

Vi har gruppert våre observasjoner på følgende måte:

Avvik i utforming målt mot COSO ERM og forskrift om risikostyring og internkontroll	Utforming: Rød	NBIMs utforming møter ikke kravene i COSO ERM og/eller forskrift om risikostyring og internkontroll, og kravene er etter vår vurdering rimelige i forhold til forventet utvikling av risikostyringen i en organisasjon av NBIMs størrelse og kompleksitet. Eventuelle røde avvik fremkommer som forbehold i vår konklusjon.
	Utforming: Gul	NBIMs utforming møter ikke kravene fra COSO ERM og/eller forskrift om risikostyring og internkontroll, men NBIM har tiltak og kontroller som bidrar til å oppfylle noen av kravene. NBIM planlegger å videreutvikle prosessene for å møte kravene, men det forutsetter en videreutvikling av rammeverket for operasjonell risikostyring som NBIM ennå ikke har gjennomført. Eventuelle gule avvik fremkommer som forbehold i vår konklusjon.
	Utforming Grønn	NBIMs utforming er ikke i full overensstemmelse med prinsippene i COSO ERM og/eller forskrift om risikostyring og internkontroll, men alternative tilnærminger som gir samme resultat eksisterer. Vi har ikke beskrevet eventuelle grønne avvik i denne rapporten. Grønne avvik fremkommer ikke som forbehold i vår konklusjon.

Avvik i implementering	Implementering: Rød	Utilstrekkelig dokumentasjon og informasjon, eller dokumentasjon og informasjon som indikerer at NBIMs implementering ikke er i henhold til utforming. Eventuelle røde avvik fremkommer som forbehold i vår konklusjon.
	Implementering: Gul	Dokumentasjon og informasjon som indikerer at NBIMs implementering er i henhold til utforming, men ikke på en fullt ut konsistent måte. Eventuelle gule avvik fremkommer som forbehold i vår konklusjon.

3.4.1 Utforming og implementering av organisasjonsstrukturen

Internt miljø og roller og ansvar

«Det interne miljøet omfatter organisasjonens verdier og holdninger og påvirker de ansattes bevissthet omkring risiko. Det interne miljøet danner grunnlaget for de øvrige komponentene i helhetlig risikostyring og gir orden og struktur. Interne miljøfaktorer består av en virksomhets filosofi for risikostyring, dens risikoappetitt, styrets «påse»-funksjon, integritet, etiske verdier, samt kompetansen hos virksomhetens medarbeidere. I tillegg kommer måten ledelsen tildeler ansvar og myndighet på, og hvordan den organiserer og utvikler virksomhetenes menneskelige ressurser. » (COSO ERM[4])

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

- NBIM har nylig gjennomgått en omorganisering som har lagt til rette for og økt fokus på risikostyring i virksomheten.

Styringsstruktur

- Norges Banks hovedstyre består av ni medlemmer hvorav to ansatterepresentanter. Fem medlemmer er eksterne (ikke ansatte i Norges Bank). Hovedstyret består av representanter fra akademia, sentralbanksjefen, visesentralbanksjefen og medlemmer med erfaring fra finansvirksomhet. Hovedstyret ledes av sentralbanksjefen.
- Mandatene for hovedstyret og revisjonsutvalget definerer hovedstyrets ansvar og myndighet.
- Hovedstyret har etablert en internrevisjon. Leder av internrevisjonen rapporterer direkte til hovedstyret gjennom revisjonsutvalget.
- Hovedstyret sørger for at virksomheten har en klar organisasjonsstruktur. Ansvaret for organiseringen er delegert til NBIMs leder som gjennom stillingsinstrukser har fastsatt rollene til de ulike ledere (»Chiefs») og gitt dem ansvaret for å organisere sine egne avdelinger.
- NBIMs leder rapporterer direkte til sentralbanksjefen (leder av Norges Banks hovedstyre).
- Stillingsinstrukser fastlegger ansvar og forventninger til de enkelte ledere in NBIM. Stillingsinstrukser er etablert for alle lederstillinger (Chief Executive Officer, Deputy Chief Executive Officer, Chief Risk Officer, Chief Compliance Officer, Chief Operating Officer, Chief Administration Officer, Chief Investment Officer, Chief Strategic Relations Officer, Chief Treasurer).
- Det er etablert komiteer med detaljert mandat for investeringsrisiko, kreditt- og motpartsrisiko, forretningsprinsipper, instrumentunivers og verdivurdering.
- Chief Compliance Officer har jevnlig møter med sentralbanksjefen.

Filosofi for risikostyring

- Hovedstyret har etablert et sett med prinsipper for risikostyring som fastsetter krav til identifisering, vurdering, overvåkning og styring av risiko, samt stresstesting og etterprøving/validering. Prinsippene klargjør definisjon av risikoklassene: markedsrisiko, kredittrisiko, motpartsrisiko og operasjonell risiko, og setter spesifikk krav til måling av disse.
- Prinsippene støttes av retningslinjer for operasjonell risikostyring, styring av motpartrisiko, og rammeverk for markedsrisiko og kredittrisiko gitt av NBIMs leder. Retningslinjene fastlegger at NBIM skal ha risikostyringssystemer for hver av risikoklassene som skal omfatte identifisering, måling, styring, godkjenning og intern rapportering av alle risikoelementer. Retningslinjene gir også anvisning for måling og overvåking av de respektive risikoklassene, samt rapportering av risiko.
- NBIMs filosofi for risikostyring blir formelt fastsatt gjennom retningslinjer fastlagt av NBIMs leder, Chief'ene og gjennom prosedyrer.

[4] Der vi refererer direkte fra COSO ERM er teksten hentet fra «COSO Enterprise Risk management - Integrated Framework – September 2004» oversatt til norsk av Norges Interne Revisorers Forening.

Risikoappetitt

- Hovedstyret har gitt NBIMs leder et investeringsmandat for å sikre at investeringsporteføljen forvaltes innenfor Finansdepartementets risikoappetitt, og i henhold til hovedstyrets prinsipper for risikostyring i NBIM.
- Videre fastsetter prinsippene at for operasjonell risiko skal kritisk og høy risiko reduseres gjennom implementering av ytterligere kontrolltiltak. Retningslinjene for operasjonell risiko fastslår at kritiske og høye risikoer er uakseptable, og fastsetter gjennom dette den faktiske risikoappetitten for operasjonell risiko.

Hovedstyrets rolle

- Hovedstyret mottar månedlig og kvartalsvis risikorapportering. Hovedstyrets leder skal også varsles umiddelbart dersom det oppstår situasjoner som er av vesentlig betydning for investeringsporteføljens avkastning og risiko.

Integritet og etiske verdier

- Virksomhetens verdier er publisert på NBIMs intranett og i ulike ledelsesdokumenter, herunder i NBIMs Styringsmodell (utkast). Forventet adferd i forhold til integritet, objektivitet og etikk er samlet i et eget dokument som omhandler etisk adferd.
- Ledelsen mener at deres vektlegging av etisk adferd og tilhørende tiltak er gode eksempler til etterfølgelse.

Kompetanse

- NBIMs leder har etablert retningslinjer for rekruttering som vektlegger akademisk bakgrunn, relevant yrkeserfaring, internasjonal erfaring og den enkeltes verdier.

Organisasjonsstruktur, roller og ansvar

- Roller og ansvar i organisasjonen er klargjort gjennom en kombinasjon av stillingsinstrukser, styre- og komitémandater og retningslinjer.
- Hovedstyret holdes informert om risikoforhold gjennom månedlig og kvartalsvis rapportering, i tillegg til de ordinære styremøtene.
- Revisjonsutvalget primære oppgave er å følge opp arbeidet som gjøres av internrevisjonen.

Personalpolitikk

- Standarder for personalpolitikk og rekruttering er fastsatt og opprettholdes gjennom sjekklister, retningslinjer, arbeidsreglement og prinsipper for etisk adferd.

Avvik fra målekriteriene som ble avdekket i gjennomgangen

- Ingen vesentlige avvik ble avdekket.

3.4.2 Utforming og implementering av rammeverket for operasjonell risikostyring

Internt miljø

«Det interne miljøet omfatter organisasjonens verdier og holdninger og påvirker de ansattes bevissthet omkring risiko. Det interne miljøet danner grunnlaget for de øvrige komponentene i helhetlig risikostyring og gir orden og struktur. Interne miljøfaktorer består av en virksomhets filosofi for risikostyring, dens risikoappetitt, styrets «påse»-funksjon, integritet, etiske verdier, samt kompetansen hos virksomhetens medarbeidere. I tillegg kommer måten ledelsen tildeler ansvar og myndighet på, og hvordan den organiserer og utvikler virksomhetenes menneskelige ressurser.» (COSO ERM)

Viktige elementer i NBIMs tilnærming dokumentert i vår gjennomgang

- Se avsnitt 3.4.1.

Avvik fra målekriteriene som ble avdekket i gjennomgangen

- Ingen vesentlige avvik ble avdekket.

Etablering av målsettinger

«Overordnede målsettinger blir etablert på strategisk nivå, og danner grunnlag for målsettinger innenfor drift, rapportering og etterlevelse. Enhver virksomhet står overfor en rekke risikoer med utspring i eksterne og interne kilder. En forutsetning for effektiv identifisering av hendelser, vurdering og håndtering av risiko er at målsettinger er etablert. Målsettingene skal samsvare med virksomhetens risikoappetitt, som påvirker nivået på risikotoleransen for virksomheten». (COSO ERM)

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

- NBIMs formål er nedfelt i utkastet til styringsmodell: «NBIM skal bevare og utvikle finansielle verdier for fremtidige generasjoner gjennom ansvarlig forvaltning».
- Formålet er understøttet av NBIMs strategiske målsettinger.
- NBIM har en treårig strategiplanleggingsprosess, og en årlig målsettingsprosess. Gjennom denne prosessen blir årlige målsettinger revurdert for å sikre at de er i overensstemmelse med strategien.
- En årlig handlingsplan utarbeides og kommuniseres i organisasjonen. Gjeldende handlingsplan inneholder 15 målsettinger satt av NBIMs leder og som er detaljert videre nedover i organisasjonen.
- Som en del av den løpende utviklingen av NBIMs risikorammeverk, har NBIM arbeidet med å koble målsettinger og strategier til de angjeldende operasjonelle risikoene og registrere resultatet i NBIMs system for operasjonell risiko.
- Operasjonell risikoappetitt er formulert på et overordnet nivå i hovedstyrets prinsipper for risikostyring.
- Risikotoleranser for finansiell risiko er implisitt definert i investeringsmandatet og for operasjonell risiko i NBIMs retningslinjer for operasjonell risiko (lav og medium gjenværende risiko).

Avvik fra målekriteriene som ble avdekket i gjennomgangen

- Ingen vesentlige avvik ble avdekket.

Identifisering av hendelser

«Ledelsen identifiserer potensielle hendelser som, hvis de inntreffer, vil påvirke virksomheten, og avgjør om de innebærer muligheter eller om de kan ha negativ innvirkning på virksomhetens evne til å implementere strategi og oppnå målsettinger. Hendelser med negative konsekvenser utgjør risikoer som krever vurdering og håndtering fra ledelsen. Hendelser med positive konsekvenser innebærer muligheter som ledelsen kanaliserer tilbake til prosessene for fastsettelse av strategi og målsettinger. Når ledelsen identifiserer hendelser, vurderer den en rekke interne og eksterne faktorer som kan gi opphav til risikoer og muligheter innenfor organisasjonens totale virksomhet.» (COSO ERM)

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

- NBIM har implementert et system for operasjonell risiko for å fange opp, vurdere og kategorisere risiko. Dette systemet, sammen med rammeverket for operasjonell risikostyring, gir en felles metodikk og begrepsapparat for operasjonell risiko.
- Fra og med inneværende år er strategiske målsettinger, fastsatt gjennom den strategiske planleggingsprosessen, eksplisitt koblet til risikoer gjennom NBIMs system for operasjonell risiko.
- NBIM har dokumentert sine prosesser og diskuterer jevnlig hvordan potensielle risikoer kan påvirke organisasjonen.
- Ansvaret for å ajourholde risikoene i systemet ligger hos NBIMs ledere selv om de fleste ansatte har adgang til å legge inn risikoer i systemet.
- Risikovurderingen tar utgangspunkt i gjenværende risiko etter kontrollaktiviteter. Risiko identifiseres i forhold til relevant prosess for å sikre en mest mulig fullstendig risikovurdering på prosessnivå.
- NBIM fanger opp faktorer som påvirker risiko ved at brukerne beskriver de underliggende årsakene til de enkelte operasjonelle risikoene i systemet.

Avvik fra målekriterier som ble avdekket i gjennomgangen

COSO-prinsipp	Konsekvenser av en operasjonell risikos påvirkning på andre operasjonelle risikoer (korrelasjon) vurderes ikke på en systematisk måte, og enkeltrisikoer kobles ikke med andre risikoer.	Avviksvurdering	Design: Gul

Målekriterier COSO ERM

- Ledelsen forstår hvordan hendelser henger sammen.
- Der hvor det finnes en sammenheng mellom hendelser, eller der hendelser virker sammen, vurderer ledelsen dem samlet.

NBIMs tilnærming og beskrivelse av avvik

- NBIM kobler ikke enkeltrisikoer med hverandre på spesifikk basis. Sammenheng mellom enkeltrisikoer fanges indirekte opp på prosessnivå. I tillegg er det gjennom risikokategoriseringen mulig å gruppere like risikoer.
- NBIMs ledelse oppfordrer organisasjonen til å vurdere mulige sammenhenger mellom risikoer.
- Det er imidlertid ingen formell prosess rundt vurdering av sammenheng (og korrelasjon) mellom enkeltrisikoer, og slike sammenhenger registreres ikke i systemet for operasjonell risiko.
- Dette reduserer muligheten til å analysere gjensidige påvirkninger, og å forstå potensielle dominoeffekter av risiko som inntreffer (unntatt gjennom risikokategorisering eller tilhørighet til en enkelt prosess).

Risikovurdering

«Risikovurdering gjør det mulig for en virksomhet å vurdere i hvilken grad potensielle hendelser kan ha konsekvenser for måloppnåelsen. Ledelsen vurderer hendelser fra to synsvinkler – sannsynlighet og konsekvens – og bruker vanligvis en kombinasjon av kvalitative og kvantitative metoder. De positive og negative konsekvensene av potensielle hendelser bør undersøkes for hele virksomheten, enkeltvis eller i kategorier. Både iboende og gjenværende risiko blir vurdert.» (COCO ERM)

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

- NBIM vurderer risiko i to trinn, før planlagte tiltak og aksjoner og etter planlagte tiltak og aksjoner.
- NBIM vurderer risiko ut i fra to perspektiv; sannsynlighet og konsekvens og etter en skala som i hovedsak bygger på kvalitative faktorer.
- Operasjonelle risikoer grupperes i henhold til operasjonelle risikoområder (mennesker, prosess, teknologi og eksterne).
- NBIM har implementert et IT-system som støtte for operasjonell risikostyring.
- Tapshendelser registreres i NBIMs systemet for operasjonell risiko og inngår i risikovurderingene.

Avvik fra målekriteriene som ble avdekket i gjennomgangen

COSO-prinsipp	Risikovurderingen tar utgangspunkt i gjenværende risiko etter at internkontrolltiltak er hensyntatt og omfatter ikke en systematisk vurdering av iboende risiko (før internkontrolltiltak).	Avviksvurdering	Design: Gult

Målekriterier COSO ERM

- Ledelsen vurderer iboende risiko.

NBIMs tilnærming og beskrivelse av avvik

- NBIM vurderer gjenværende risiko. Imidlertid vurderes ikke iboende risiko (definert i COSO som «risikoen for en virksomhet når en ser bort fra de tiltak ledelsen iverksetter for å endre enten risikoens sannsynlighet eller konsekvens») på en systematisk måte.
- Det er i vurderingene ikke systematisk lagt til grunn COSO-definisjonen av iboende risiko, det vil si å se bort fra intern kontrolltiltak som ledelsen har iverksatt. Ledelsen er i gang med å innføre en mer systematisk tilnærming til vurdering av iboende risiko.
- Uten en systematisk prosess for å vurdere iboende risiko kan ledelsen ikke på en systematisk måte beregne hvor mye risiko som reduseres gjennom kontroller. Det er nyttig informasjon i en kost/nytte-vurdering av kontrollaktiviteter. Risikoer som oppleves å ha sterke risikoreduserende kontroller kan få mindre oppmerksomhet enn de fortjener, fordi den gjenværende risikoen beregnes til å være lav eller medium.

Risikohåndtering

«Når ledelsen har vurdert alle relevante risikoer, bestemmer den hvordan den vil håndtere dem. Alternative former for risikohåndtering er å unngå, redusere, dele og akseptere risiko. Når ledelsen vurderer hvordan risiko skal håndteres, vurderer den effekten på risikoens sannsynlighet og konsekvens, i tillegg til kostnad og nytte. Ledelsen velger en måte å håndtere risiko på som bringer gjenværende risiko i samsvar med ønskede risikotoleranser. Ledelsen identifiserer tilgjengelige muligheter og ser risikoen ut fra et helhetlig porteføljesyn, og avgjør så om den totale gjenværende risikoen er innenfor virksomhetens risikoappetitt.» (COSO ERM)

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

- NBIMs prosess for styring av operasjonell risiko angir at «risikoreduserende tiltak og kontroller skal identifiseres for alle risikoer som er høye eller kritiske» og har derigjennom fastsatt NBIMs risikotoleranse.
- Risikoeiere vurderer risiko både «før tiltak» (det vil si før innføring av nye kontroller ut over de som allerede er implementert) og etter tiltak. Innføring av nye kontrollprosedyrer og tiltak representerer en mulighet til å redusere gjenværende risiko ned til lavt eller medium.

- Risikoeiere skal i sin vurdering av risikohåndtering ta hensyn til «kostnad, implementeringsutfordringer og risikoreduserende effekt» og «fastsette hvilke tiltak og kontroller som skal implementeres basert på risikoreduserende effekt så vel som kost/nytte».
- Risikohåndteringen skal løpende registreres i NBIMs system for styring av operasjonell risiko for de operasjonelle risikoene som er identifisert. Tiltak og kontroller velges for å bringe gjenværende risiko ned til lav eller medium, det vil si innenfor fastsatte risikoappetitt.
- Kontroller og risikoer er kartlagt på prosessnivå. En ny kontroll som innføres, vil derfor risikovurderes i sammenheng med den aktuelle prosessen.
- NBIMs leder har jevnlige møter med sine nærmeste medarbeidere for å være orientert om nye situasjoner som har inntuffet. I tillegg avholdes det månedlige ledergruppemøter hvor spørsmål knyttet til operasjonell risiko diskuteres.
- Ledelsen vurderer risiko på ulike nivåer i organisasjonen, herunder også på virksomhetsområder.
- Kvartalsvis rapportering til hovedstyret omfatter operasjonell risiko på virksomhetsnivå. Nylig er det iverksatt rapportering av gjenværende risiko mot risikoappetitt ved å vise samtlige kritiske og høye risikoer i tabellformat i tillegg til den eksisterende rapporteringen av kritiske og høye risikoer.

Avvik fra målekriteriene som ble avdekket i gjennomgangen

- Ingen vesentlige avvik ble identifisert.

Kontrollaktiviteter

«Kontrollaktiviteter er de retningslinjer og rutiner som bidrar til å sikre at ledelsens valgte former for risikohåndtering blir gjennomført. Kontrollaktiviteter utføres i hele organisasjonen på alle nivåer og i alle funksjoner. De omfatter en rekke ulike aktiviteter, blant annet godkjennelser, fullmakter, verifikasjoner, avstemminger, gjennomgang av driftsresultater, sikring av aktiva og arbeidsdeling.» (COSO ERM)

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

- Policyer fastsettes på NBIM ledernivå, og godkjennes av NBIMs leder.
- Policyene utfylles på nivået under med mer detaljerte retningslinjer. Rutiner og prosedyrer gir ytterligere detaljinformasjon om de konkrete aktivitetene.
- De viktigste forretningsprosessene er kartlagt for å øke forståelsen av dem og for å lette identifikasjon av risiko og kontrollaktiviteter. Kontrollaktiviteter blir vurdert på prosessnivå.
- Kontrolltiltak blir vurdert med hensyn til kostnader, implementeringsutfordringer og risikoreduserende effekt.
- En kombinasjon av ulike kontrolltyper benyttes for å sørge for god risikohåndtering.

Avvik fra målekriteriene som ble avdekket i gjennomgangen

- Ingen vesentlige avvik ble identifisert.

Informasjon og kommunikasjon

«Viktig informasjon identifiseres, fanges opp og formidles i en form og på et tidspunkt som setter de ansatte i stand til å ivareta sine ansvarsområder. Informasjonssystemer bruker data som er generert internt, så vel som informasjon fra eksterne kilder, og leverer informasjon for risikohåndtering og veloverveid beslutningstaking angående målsettingene. Effektiv kommunikasjon gjennomsyrer virksomheten, både nedover, sideveis og oppover i organisasjonen. Alle ansatte mottar et klart budskap fra toppledelsen om at ansvaret for helhetlig risikostyring må tas alvorlig.

De forstår sin egen rolle i den helhetlige risikostyringen og hvordan de enkelte aktivitetene og handlingene henger sammen med andres oppgaver. De må ha kanaler for formidling av viktig informasjon oppover i organisasjonen. Det er også effektiv kommunikasjon med eksterne aktører, slik som kunder, leverandører myndigheter og aksjonærer.» (COSO ERM)

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

Informasjon

- Informasjon om operasjonell risiko (inklusive risikoer, kontrollaktiviteter, tiltak og hendelser) registreres i NBIMs system for operasjonell risiko. En mengde ekstern informasjon hensyntas når risiko vurderes; for eksempel rapporter fra tjenesteleverandører, men denne informasjonen registreres ikke i systemet.
- All informasjon som legges inn i systemet lagres, herunder også informasjon om tidligere hendelser.
- Det legges vekt på at data i systemet for operasjonell risiko er pålitelig. Registrering av data gjøres i en forhåndsdefinert meny der det er mulig. Det foreligger brukerveiledninger for å sikre at nøyaktige data legges inn. Den ansvarlige for operasjonell risiko følger opp dersom inkonsistente data fremkommer.
- NBIMs system for operasjonell risiko har et fleksibelt brukergrensesnitt som gjør det mulig å tilpasse rapporteringen til de forskjellige brukernes behov.
- Avdelingen for *Control and Compliance* og Chief'ene har mulighet til å se informasjon om operasjonell risiko på tvers av organisasjonen. Dette bidrar til å bryte ned silotankegang.
- Vesentlige områder som er satt ut til eksterne tjenesteleverandører følges opp av ansvarlige hos NBIM, både med hensyn til kvantitative og kvalitative kriterier. Det fremgår av NBIMs policy for styring og oppfølging av eksterne tjenesteleverandører at det raskt skal iverksettes tiltak dersom leverandøren ikke utfører de avtalte oppgavene i overensstemmelse med NBIMs definerte krav til tjenesteleveransen eller fastsatte risikoindikatorer.
- Rapportering til hovedstyret gjøres kvartalsvis i samsvar med styrets krav, herunder informasjon som muliggjør en måling av operasjonell risiko mot operasjonell risikoappetitt.
- Den månedlige rapporten fra ledergruppen og den kvartalsvise rapporten som gis til hovedstyret, har en fast mal. Eventuelle tilbakemeldinger på formatet og informasjonen som gis blir løpende hensyntatt.

Kommunikasjon

- Gjennom policyer og retningslinjer har ledelsen kommunisert forventning til den enkeltes adferd og ansvarsområder. Detaljerte prosedyrer understøtter policyene og retningslinjene er utarbeidet etter en standardmal. Prosedyrene henviser til den underliggende policyen som setter «tonen» for organisasjonen.
- NBIM er en oversiktlig virksomhet. Prosessene er definerte, og beskrivelser er tilgjengelige på intranettet. Det gis detaljerte anvisninger på hvordan ansatte skal forholde seg til ulike scenarioer, og prosessen for operasjonell risiko fanger opp uventede hendelser.
- Ansatte i NBIM er underlagt et etisk regelverk og prinsipper for god forretningsmessig adferd (conduct of business). En policy for varsling legger til rette for en kommunikasjonskanal utenfor de normale rapporteringslinjene.
- NBIM har bevisst utviklet en flat ledelsesstruktur for å fremme lett tilgang til ledelsen.
- NBIMs leder sørger for at hovedstyret mottar informasjon om de viktigste aspektene vedrørende NBIMs rammeverk for operasjonell risikostyring, herunder informasjon om nye risikoer. Dette gjøres gjennom jevnlige møter og rapporter.
- Det avholdes jevnlige møter med eksterne aktører, inkludert myndigheter og departement, så vel som tjenesteleverandører.
- NBIM publiserer kvartalsvise og årlige rapporter. I disse redegjøres det for investeringsavkastning og risikoeksponering.

Avvik fra målekriteriene som ble avdekket i gjennomgangen

- Ingen vesentlige avvik ble avdekket.

Oppfølging

«Helhetlig risikostyring følges opp, og det vurderes om de ulike komponentene er til stede og fungerer over tid. Slik vurdering oppnås gjennom løpende oppfølgingsaktiviteter, frittstående evalueringer, eller ved en kombinasjon av de to. Omfanget og hyppigheten av de frittstående evalueringene avhenger primært av risikovurderingen og hvor effektive de løpende oppfølgingsrutinene er. Mangler ved den helhetlige risikostyringen rapporteres til ledelsen, og alvorlige forhold rapporteres til toppledelsen og styret.» (COSO ERM)

Viktige elementer i NBIMs tilnærming som ble dokumentert i vår gjennomgang

- Løpende oppfølgingsaktiviteter er en del av ledelsesansvaret på de ulike nivå i organisasjonen. For eksempel: Operasjonell risikoeksponering følges opp av risikoeierne; enheten med ansvar for operasjonell risiko utfordrer risikoer som er identifisert og foreslåtte kontrollaktiviteter; Compliance-avdelingen følger opp at investeringsgrenser og mandat overholdelse; og ytterligere oppfølging av operasjonell risiko finner sted i de regelmessige møtene i ledergruppen.
- Svakheter som identifiseres gjennom den løpende oppfølgingen fanges opp i NBIMs system for styring av operasjonell risiko.
- Separate evalueringer av rammeverket for operasjonell risiko er også gjennomført:
    - Etter hovedstyrets prinsipper skal NBIM utføre en årlig evaluering av risikostyringssystemene. Resultatene skal dokumenteres og gjennomgås internt. En egenvurdering av risikorammeverket ble utført av NBIMs leder i 2007 og oppdatert i 2008.
    - Operasjonell risiko ble vurdert av internrevisjonen for omlag ett år siden.
- Rapporter fra de separate evalueringene er utarbeidet. Funnene fra den tidligere gjennomgangen av risikostyringen er blitt eskalert til ledelsen i NBIM og hovedstyret i Norges Bank.

Avvik fra målekriteriene som ble avdekket i gjennomgangen

- Ingen vesentlige avvik ble avdekket.

4. Del 2 – Den tidligere gjennomgang av risikostyringen

4.1 Metodikk og målekriterier

Den tidligere gjennomgangen av NBIMs rammeverk for risikostyring ble utført i 2007 og omhandler følgende områder:

- Virksomhetsstyring
- Operasjonell risiko
- Markedsrisiko
- Kredittrisiko
- Avkastningsmåling og verdivurdering

Vi har vurdert om NBIM har fulgt opp de anbefalingene som er relevante for utforming og implementering av NBIMs organisasjonsstruktur og rammeverk for styring av operasjonell risiko, slik det er gjort rede for i brev datert 19. desember og 12. februar 2009 til Finansdepartementet.

Anbefalingene i den tidligere gjennomgangen av risikostyringen utgjør målekriteriene som vi har målt NBIMs nåværende organisasjonsstruktur og rammeverk for styring av operasjonell risiko opp mot.

4.2 Avgrensning av oppdraget

Omfang

Vi har utelukkende vurdert anbefalingene i den tidligere gjennomgangen av risikostyringen i den utstrekning de gjelder organisasjonsstruktur og operasjonell risiko. Andre anbefalinger i den tidligere gjennomgangen faller utenfor denne gjennomgangens omfang.

Kontrolleffektivitet (etterlevelse)

Oppdraget dekker ikke kontroll av om den etablerte organisasjonsstruktur og rammeverket for styring av operasjonell risiko har fungert effektivt og etter forutsetningene. Kontrolleffektivitet (etterlevelse) omfatter hvordan en kontrollprosedyre gjennomføres, hvor konsistent den gjennomføres, og hvem som gjennomfører den over en bestemt periode.

Risikoeksponering og internt miljø

Oppdraget dekker ikke vurdering av om risikoene som NBIM har identifisert er fullstendige og dekkende for NBIMs virksomhet eller godheten i de kontrolltiltak som er etablert.

Andre risikoer enn de som er identifisert av NBIM kan være aktuelle, og risikoer som faktisk er identifisert av NBIM kan vise seg å ha andre konsekvenser enn de er vurdert å ha i dag.

4.3 Arbeid utført

Standard for Attestasjonsoppdrag (SA 3000)

Som avtalt i vårt engasjementsbrev til Sentralbankrevisor datert 21. september 2009, har vi utført vårt arbeid i samsvar med SA 3000. Vår oppgave er å gi Representantskapet betryggende sikkerhet for at NBIM har fulgt opp anbefalingene i den tidligere gjennomgangen av risikostyringen som er gjort rede for i Norges Banks brev til Finansdepartementet datert 19. desember 2007 og 12. februar 2009 (for anbefalingene som gjelder organisasjonsstruktur og operasjonell risiko).

Et attestasjonsoppdrag som skal gi betryggende sikkerhet i henhold til SA 3000 krever at vi planlegger og utfører arbeidet slik at vi oppnår høy, men ikke absolutt sikkerhet for at saksforholdet er i samsvar med målekriteriene. Vårt arbeid er beskrevet under.

Vurdering av om anbefalingene er fulgt opp

I vurderingen av om NBIM har fulgt opp anbefalingene knyttet til organisasjonsstruktur og operasjonell risikostyring, har vi undersøkt om organisering, rutiner og prosesser er endret i tråd med anbefalingene.

Vi har ikke vurdert om den etablerte organisasjonsstrukturen eller rammeverket for operasjonell risikostyring har vært effektivt og fungert etter forutsetningene.

Nærmere om våre prosedyrer

Vi har:

- Identifisert anbefalingene fra den tidligere gjennomgangen av risikostyringen som var relevante for organisasjonsstrukturen og rammeverket for operasjonell risikostyring. Vi har ikke sett på de anbefalingene som var knyttet til markeds- eller kredittrisiko.
- Diskutert svarene fra Norges Bank gjengitt i brevene datert 19. desember 2007 og 12. februar 2009 med NBIM.
- Diskutert de tiltakene som var iverksatt av NBIM som følge av anbefalingene i den tidligere gjennomgangen av risikostyringen, og vurderte i hvilken grad NBIM hadde svart på anbefalingene.
- Søkt å finne dokumentasjon og informasjon som kunne understøtte våre vurderinger.
- Utarbeidet en oversikt over avvik knyttet til oppfølging av anbefalingene.

4.4 Funn: Den tidligere gjennomgangen av risikostyringen

Bakgrunn

Våre konklusjoner må sees i sammenheng med at:

- Anbefalingene i den tidligere gjennomgangen av risikostyringen er gjort på bakgrunn av NBIMs organisasjon slik den var på ett bestemt tidspunkt (2007). I perioden siden den gang har NBIM fått ny ledelse og gjennomgått en større omorganisering. Det medfører at flere elementer i organisasjonsstrukturen og rammeverket for styring av operasjonell risiko observert i 2007 er endret og har vært gjenstand for løpende utvikling.
- Basert på denne endringen og den løpende utviklingen hos NBIM er noen av de opprinnelige anbefalingene mindre relevante nå enn da den tidligere gjennomgangen av risikostyringen fant sted.
- Vi har kun vurdert anbefalingene som gjelder organisasjonsstruktur og operasjonell risiko.

Rapport fra den tidligere gjennomgangen av risikostyringen	Nivå 1	NBIM har ikke fulgt anbefalingen i den tidligere gjennomgangen av risikostyringen slik det er redegjort for i Norges Banks brev til Finansdepartementet datert 19. desember 2007 og 12. februar 2009, og implementeringen av anbefalingen er fortsatt relevant. Eventuelle avvik på nivå 1 fremkommer som forbehold i vår konklusjon.
	Nivå 2	NBIM har kun delvis fulgt - eller er i ferd med - å følge anbefalingen i den tidligere gjennomgangen av risikostyringen slik det er redegjort for i Norges Banks brev til Finansdepartementet datert 19. desember 2007 og 12. februar 2009, og implementeringen av anbefalingen er fortsatt relevant. Eventuelle avvik på nivå 2 fremkommer som forbehold i vår konklusjon.
	Nivå 3	NBIM har ikke nøyaktig fulgt anbefalingen i den tidligere gjennomgangen av risikostyringen slik det er redegjort for i Norges Banks brev til Finansdepartementet datert 19. desember 2007 og 12. februar 2009, men andre tiltak som er gjennomført oppfyller samme målsetting. Eventuelle avvik på nivå 3 fremkommer ikke som forbehold i vår konklusjon.

4.4.1 Respons på anbefalingene i den tidligere gjennomgangen av risikostyringen

Norges Bank beskriver i brevene datert 19. desember 2007 og 12. februar 2009 til Finansdepartementet, hvordan anbefalingene i den tidligere gjennomgangen av risikostyringen er fulgt opp. Nedenfor er det gitt et sammendrag av Norges Bank respons på anbefalingene.

Sammendrag av Norges Banks beskrivelse til Finansdepartementet vedrørende anbefalinger i den tidligere gjennomgangen:

	Brev datert 19. desember 2007	Brev datert 12. februar 2009
Organisasjonsstruktur	- Norges Bank vil vurdere om det for bankens styrende organer er behov for mer detaljert fastsettelse av ansvar, dokumentasjon og rapportering. - Norges Bank er enig i at det bør foreligge et dokument som beskriver risikorammer, eskaleringsprosedyrer, kontrolltiltak og rapportering til bankens styrende organer.	- Internrevisjonen har prioritert risikostyring og internkontroll i NBIM i løpet av 2008 og har blant annet gjennomgått status for oppfølging av den tidligere gjennomgangen av risikostyringen. - Formålet var å gi hovedstyret bekreftelse på at tiltak var innført i overensstemmelse med Norges Banks svarbrev til Finansdepartementet. - Internrevisjonen konkluderte med at NBIMs nye organisasjonsmodell gir en klarere rolle- og ansvarsdeling i organisasjonen. Det er etablert organisasjonsenheter som måler og rapporterer risiko uavhengig av investeringslinjen. - Internrevisjonen vurderte at dette er viktige organisasjonsmessige tiltak for å sikre god risikostyring og internkontroll.
Rammeverk for styring av operasjonell risiko	- Norges Bank er enig i de styringsprinsipper som er foreslått i den tidligere gjennomgangen av risikostyringen. - Norges Bank er også enig i at det nylig avsluttede prosjektet innen operasjonell risiko sikrer at disse prinsippene ivaretas. - Norges Bank er videre enig i prinsipper, beskrivelse og anbefalinger innen alle deler av det operasjonelle risikoområdet som er gitt i den tidligere gjennomgangen av risikostyringen. - Norges Bank kan bekrefte at prosjektet knyttet til operasjonell risiko ble avsluttet som planlagt og at operasjonell risiko har vært rapportert månedlig etter de nye retningslinjene siden juni 2007. - Alle NBIMs avdelinger har utpekt ansvarlige for operasjonell risiko. - Hovedstyret har definert sine risikorammer, og vil motta rapportering hvert kvartal. Første slik rapportering var for andre kvartal 2007.	- Den nye organiseringen av virksomheten betyr også omfattende endringer i arbeidsprosessene. - NBIM arbeider med å tilpasse styringen av operasjonell risiko til sine nye arbeidsprosesser.

Som fremhevet i punktene over, sa Norges Bank seg enig i:

- En del av anbefalingene, og ville vurdere nærmere andre anbefalinger som gjaldt organisasjonsstruktur.
- Anbefalingene knyttet til operasjonell risiko.

Vi har i gjennomgangen vurdert om anbefalingene for styring av operasjonell risiko og organisasjonsstruktur som Norges Bank sa seg enige i har blitt fulgt opp av NBIM. Våre funn er gjengitt på de etterfølgende sidene.

4.4.2 Oppfølging av anbefalinger knyttet til organisasjonsstruktur og styring av operasjonell risiko

Anbefaling fra den tidligere gjennomgangen av risikostyringen	Manglende kobling av operasjonell risikoappetitt med stress-scenarioer.	Type implementerings-avvik	Nivå 2

Anbefaling fra den tidligere gjennomgangen av risikostyringen

- COSO krever at risikoappetitt defineres, noe NBIM har gjort på et overordnet nivå. Den tidligere gjennomgangen av risikostyringen anbefalte mer spesifikke krav:
  - Det bør foreligge «en definisjon av operasjonell risikoappetitt. Definisjonen bør være eksplisitt koblet til viktige operasjonelle risiko-scenarioer som er av vesentlig betydning for NBIMs ledelse og dets styrende organer[5].»
  - «Vi anbefaler at klare og spesifikke formuleringer av operasjonell risikoappetitt utvikles som en del av utrullingen av det nye rammeverket for styring av operasjonell risiko.»
  - «Spesifikk rapportering av stress-scenarioer knyttet til operasjonell risiko som er av størst betydning for de styrende organer med ansvar for operasjonell risiko.»

NBIMs tilnærming og beskrivelse av implementeringsavvik

- I henhold til policy for operasjonell risikostyring skal operasjonell risiko identifiseres, analyseres og reduseres i overensstemmelse med NBIMs risikotoleranse (risikoappetitt). Risikotoleranse er angitt som kritisk, høy, moderat og lav gjenværende risiko, hvor kritisk og høy er utenfor toleransegrensen og risikoreduserende tiltak må iverksettes, med mindre de uttrykkelig er godkjent av NBIMs leder og ansvarlig Chief.
- Risikotoleransegrensene er vist i risikomatriser med fargerkoder i rødt, oransje, gult og grønt.
- NBIMs metodikk for vurdering av operasjonell risiko innebærer at potensielt uønskede hendelser (risikofaktorer) vurderes i forhold til sannsynlighet og konsekvens mot ett eller flere risikostyringsmål (dimensjoner for konsekvens). Konsekvensdimensjonene er operasjonelt, finansielt, omdømme og personell. En risikofaktors plassering i den overordnede risikomatrisen er bestemt av den høyeste plassering i de fire underliggende risikomatriser (operasjonelt, finansielt, omdømme og personell).
- Vurdering av hver risikofaktors plassering i risikomatrisene gir spesifikke risikotoleransegrenser for den enkelte risikofaktor.
- Overordnede risikotoleransegrenser er godkjent, men vi har ikke sett dokumentasjon som viser at spesifikke risikotoleransegrenser har blitt diskutert eller godkjent i styret, selv om vi forstår at de implisitt inngår i risikovurderingsprosessen.
- Risikotoleransegrensene er ikke aggregerte og er ikke «eksplisitt koblet til viktige operasjonelle risiko-scenarioer som er av størst betydning for NBIMs ledelse og dets styrende organer.» Vår forståelse er at det ikke er noen formell analyse av stresscenarioer knyttet til operasjonell risiko, med unntak av scenarioplanlegging innenfor rammene av mulig forretningsavbrudd.

[5] Oversatt fra den opprinnelige engelske rapporten.

Anbefaling fra den tidligere gjennomgangen av risikostyringen	Nøkkelrisiko indikatorer (Key Risk Indicators, KRI) er ikke etablert som en del av overvåkningen av risikoeksponeringen.	Type implementeringsavvik:	Nivå 2

Anbefaling fra den tidligere gjennomgangen av risikostyringen

- COSO krever at oppfølgingsaktiviteter skal være en integrert del av virksomhetens normale, løpende virksomhet, og krever at de utføres rettidig og tilpasses dynamisk til endrede forhold. Den tidligere gjennomgangen av risikostyringen anbefalte mer spesifikke krav:
    - En «ny prosess for overvåkning og rapportering, basert på indikatorer for nøkkelrisikoer (KRI), som bygger på den eksisterende overvåkingen av kontrollbrudd, risikotrender og andre risikorelaterte måltall som utarbeides».
    - «Kravene til overvåkning og rapportering av operasjonell risiko bør angi en klar definisjon av når hendelser skal rapporteres oppover i organisasjonen (eskaleringsprosedyre). Definisjonen bør angi hva som utgjør en betydelig hendelse som skal rapporteres direkte til NBIMs ledelse eller til relevante styrende organer».
    - «Regelmessige uavhengige gjennomganger av eskaleringsprosessene på tvers av risikoklassene for å sikre at prosedyrene er effektive og virker etter forutsetningene».

NBIMs tilnærming og beskrivelse av implementeringsavvik

- Løpende oppfølging er del av lederansvaret på de ulike nivå i organisasjonen. For eksempel: Operasjonell risikoeksponering følges opp av risikoeierne; enheten med ansvar for operasjonell risiko utfordrer risikoer som er identifisert og foreslåtte kontrollaktiviteter; Compliance-avdelingen følger opp at investeringsgrenser og mandater overholdes; og ytterligere oppfølging av operasjonell risiko finner sted i de regelmessige møtene i ledergruppen.
- Prosedyren for styring av operasjonell risiko gjør det klart at kritiske hendelser skal meldes gjennom linjen umiddelbart, eller så snart som praktisk mulig etter at hendelsen har inntruffet.
- Svakheter identifiseres gjennom løpende oppfølging og fanges opp i NBIMs system for operasjonell risiko.
- Det er imidlertid ikke etablert en:
    - Helhetlig sentralisert prosess for oppfølging og rapportering av nøkkelrisikoindikatorer.
    - Klar og entydig definisjon av eskaleringsprosedyrer for hvordan hendelser som har sammenheng med operasjonell risiko (hendelser eller nye risikoer) skal rapporters, eller til hvem. Det er heller ingen definisjon av en betydelig hendelse som skal rapporteres til ledelsen eller styret. Risikoprinsippene som styret har fastlagt fastslår at «Styret skal informeres om hendelser av særskilt betydning eller av uvanlig art».
    - Uavhengig gjennomgang av eskaleringsprosessen i sammenheng med den operasjonelle risikostyring.