NORGES BANKS REPRESENTANTSKAP
Tilsynssekretariatet

Finansdepartementet
Boks 8008 Dep

0030 OSLO

Deres ref.	Vår ref.	Oslo
	MLP	8. mars 2013

ATTESTASJONSOPPDRAG – OPERASJONELL RISIKOSTYRING I FORVALTNINGEN AV STATENS PENSJONSFOND UTLAND 2012

I henhold til plan fastsatt av Norges Banks representantskap jf. vårt brev til Finansdepartementet 29. februar 2012, er det gjennomført et attestasjonsoppdrag om styring av og kontroll med IT- sikkerhet i Norges Bank Investment Management. Vedlagt følger rapport som ble behandlet av representantskapet i møte den 7. mars 2013. Rapporten blir også offentliggjort på bankens hjemmeside.

Attestasjonsoppdraget er utført av Deloitte AS. Oppdraget følger mal fra tidligere attestasjonsprosjekter som har hatt fokus på operasjonell risikostyring i forvaltningen av Statens pensjonsfond utland.

Med hilsen

Svenn Erik Forsstrøm
Direktør

Mats L. Pedersen
Fagdirektør

Vedlegg: Uavhengig attestasjonsrapport fra Deloitte AS om styring av og kontroll med IT-sikkerhet i Norges Bank Investment Management

Kopi: Riksrevisjonen
Tilsynssekretariatet er Norges Banks representantskaps sekretariat i henhold til Sentralbankloven.

Deloitte.

Uavhengig attestasjonsoppdrag for Norges Banks representantskap om Norges Bank Investment Managements utforming og implementering av styring av og kontroll med IT-sikkerhet

11. februar 2013

Innhold

1. Formål og rammer for attestasjonsoppdraget

Norges Banks representantskap ("representantskapet") har engasjert Deloitte AS til å foreta en uavhengig gjennomgang av utforming og implementering av Norges Bank Investment Managements ("NBIM") styring av og kontroll med IT-sikkerhet. Betegnelsen "NBIM" omfatter også Norges Banks hovedstyre og ledelse, i tillegg til NBIMs ledelse.

Som avtalt i vårt engasjementsbrev datert 19. juni 2012, har vi utført vårt arbeid i samsvar med ISAE 3000. Vår oppgave er å gi representantskapet betryggende sikkerhet for at NBIM har utformet og implementert styring av og kontroll med IT-sikkerhet i samsvar med målekriteriene beskrevet nedenfor.

Vi har gjennomgått utforming og implementering av NBIMs styring av og kontroll med IT-sikkerhet og har sammenholdt dette med målekriteriene.

1.1. Standarder og målekriterier

Standardene og målekriteriene vi har benyttet for denne gjennomgangen er beskrevet nedenfor.

Utgangspunktet for målekriteriene er:
- LOV 1985-05-24 nr. 28: Lov om Norges Bank og pengevesenet (Sentralbankloven)
- FOR 2009-12-17 nr. 1630: Forskrift om risikostyring og internkontroll i Norges Bank
- FOR 2010-11-08 nr. 1414: Mandat for forvaltningen av Statens pensjonsfond utland

Det fremgår av mandatet for forvaltningen at Norges Bank skal fastsette prinsipper for styring, måling og kontroll av risiko som minst oppfyller internasjonalt anerkjente standarder og metoder.
Norges Bank har fastsatt følgende prinsipper og virksomhetsovergripende retningslinjer som har betydning for IT-sikkerhet:

- Prinsipper for sikkerhet, beredskap og håndtering av kriser i Norges Bank inkludert NBIM, fastsatt av hovedstyret 15.desember 2010.
- Virksomhetsovergripende retningslinjer for sikkerhet, beredskap og håndtering av kriser i Norges Bank inkludert NBIM, vedtatt av sentralbanksjefen 28. desember 2010.

De virksomhetsovergripende retningslinjene for Norges Bank inkludert NBIM angir at:

«Styringssystemet for IT-sikkerhet i Norges Bank skal baseres på ISO/IEC 27001. For andre sikkerhetsfagområder og beredskap skal ISO/IEC 27001 benyttes så langt det passer.»

«ISO/IEC 27001:2005 Information technology - Security techniques - Information security management (ISO/IEC 27001)» er en nasjonalt og internasjonalt anerkjent standard som angir god praksis for styring av og kontroll med IT-sikkerhet. Standarden er publisert i fellesskap av International Organization for Standardization (ISO) og International Electrotechnical Commission (IEC).

Med bakgrunn i at NBIM er omfattet av kravene i de virksomhetsovergripende retningslinjene og at ISO/IEC 27001 er en anerkjent standard på området har vi brukt denne som målekriterium.

Vi har som støtte for våre vurderinger også sett hen til:

- IKT-forskriften fra Finanstilsynet (Norges Bank/NBIM er ikke underlagt kravene i denne)
- Finanstilsynets rapport av mars 2012 – Risiko og sårbarhetsanalyse (ROS) 2011 Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Representantskapets tilsynssekretariat har vurdert målekriteriene og sagt seg enig i at de er relevante for denne gjennomgangen.

Funnene i rapporten er basert på målekriteriene og vår vurdering av om NBIM har utformet og implementert styring av og kontroll med IT-sikkerhet i samsvar med disse.

1.2. Avgrensning av oppdraget

Vårt oppdrag omfatter kun en gjennomgang av NBIMs styring av og kontroll med IT-sikkerhet og en vurdering av om styring og kontroll er hensiktsmessig utformet og implementert. Oppdraget omfatter ikke en kontroll av om NBIMs styring av og kontroll med IT-sikkerhet har vært effektiv og fungert etter hensikten; det vil si i hvilken grad prosedyrene er fulgt, om prosedyrene er gjennomført på en konsistent måte og hvem som har utført dem.

Oppdraget omfatter heller ikke en vurdering av om IT-sikkerhetsrisikoene som NBIM har identifisert, er fullstendige og dekkende, eller om risikoene er hensiktsmessig håndtert. Andre risikoer enn de som er identifisert av NBIM kan være aktuelle.

NBIM benytter et betydelig omfang av eksterne tjenesteleverandører i sin virksomhet. Vi har vurdert NBIMs styring av og kontroll med IT-sikkerhet overfor tjenesteleverandører, men vi har ikke vurdert om IT-sikkerheten er hensiktsmessig styrt eller adressert hos disse tjenesteleverandørene.

1.3. Arbeid utført

Attestasjonsoppdraget skal gi betryggende sikkerhet i henhold til ISAE 3000. Dette forutsetter at arbeidet planlegges og utføres slik at vi oppnår høy, men ikke absolutt sikkerhet for at styring av og kontroll med IT-sikkerhet hos NBIM er i samsvar med målekriteriene. Vårt arbeid er beskrevet nedenfor.

1.3.1 Nærmere om målekriteriene

De etablerte målekriteriene er knyttet til NBIMs styring av og kontroll med IT-sikkerhet. Målekriteriene omfatter overordnet styring av og kontroll med IT-sikkerhet knyttet til følgende områder:

- Risikostyring
- Styringssystem for IT-sikkerhet
- Ledelsens støtte og ressursstyring
- Opplæring, kompetanse og fokus
- Sikkerhetspolicy
- Organisering av IT-sikkerhet
- Administrasjon av aktiva
- Personalsikkerhet
- Fysisk og miljømessig sikkerhet
- Kommunikasjons- og driftsadministrasjon
- Aksesskontroll
- Anskaffelse, utvikling og vedlikehold av informasjonssystemer
- Administrasjon av IT-sikkerhetsbrudd
- Kontinuitetsplanlegging
- Samsvar og etterlevelse

I vedlegg 1 er det gitt en kort forklaring på innholdet i de enkelte områdende.

1.3.2 Vurdering av samsvar med målekriteriene

Vi har vurdert om styring av og kontroll med IT-sikkerhet i NBIM er utformet og implementert i samsvar med målekriteriene.

En komponent i styring av og kontroll med IT-sikkerhet vil være tilstrekkelig *utformet* dersom den enkeltvis eller i kombinasjon med andre elementer, med rimelig grad av sikkerhet, bidrar til å oppfylle det aktuelle målekriteriet.

Begrepet *implementert* omfatter iverksettelse på et gitt tidspunkt av de aktiviteter som følger av utformingen, men omfatter ikke den faktisk løpende gjennomføringen av aktiviteter eller i hvilken utstrekning de fungerer effektivt og etter forutsetningene.

Vurdering av utforming
Vi har mottatt dokumenter som beskriver NBIMs styring av og kontroll med IT-sikkerhet. Vi har gjennomgått dokumenter som omfatter blant annet policyer, guidelines, prosedyrer, kontrolldokumentasjon, styringsdokumenter, møtereferater, stillingsinstrukser, presentasjoner, instrukser, revisjonsrapporter og ledelsesrapporter med videre.

Vi har avholdt flere møter med ledelsen og ansatte i NBIM hvor det ble redegjort for utformingen av styring av og kontroll med IT-sikkerhet i NBIM. Vi har, basert på mottatt dokumentasjon og informasjon, sammenholdt de sentrale elementene i NBIMs utforming av styring av og kontroll med IT-sikkerhet mot målekriteriene og vurdert om det forelå vesentlige avvik.

Vurdering av implementering
For de enkelte elementene i styring av og kontroll med NBIMs IT-sikkerhet, har vi vurdert dokumentasjon og innhentet informasjon for å underbygge vår vurdering av implementeringen, og vurdert om det forelå vesentlige avvik mot utformingen.

1.4. Endringer i NBIM

NBIM har gjennom 2012 gjennomført endringer som påvirker styring av og kontroll med IT-sikkerhet. Endringene har blant annet omfattet:

- Ny organisering hvor styring av og kontroll med IT-sikkerhet er tillagt gruppen for operasjonell risikostyring. Dette klargjør arbeidsdelingen mellom den operative linjen og risikoovervåking og kontroll. Tidligere har styring av og kontroll med IT-sikkerhet vært organisert i den operasjonelle IT-virksomheten.

- Ny organisering av styring av og kontroll med IT-sikkerhet har medført forbedring og videreutvikling av eskaleringsprosedyrer for IT-sikkerhetsrisikoer og dokumentasjon knyttet til IT-sikkerhet.

Endringene medfører at styring av og kontroll med IT-sikkerhet tydeliggjøres og får en klarere forankring på ledelsesnivå.

2. NBIMs styring og kontroll av IT-sikkerhet

2.1. Virksomhetsovergripende retningslinjer

Norges Banks hovedstyre er ansvarlig for en forsvarlig organisering av forvaltningen av Statens pensjonsfond utland og har etablert prinsipper og retningslinjer for kapitalforvaltningsvirksomheten i NBIM. Hovedstyret har etablert prinsipper for sikkerhet, beredskap og håndtering av kriser i Norges Bank inkludert NBIM, og sentralbanksjefen har gitt virksomhetsovergripende retningslinjer på området. Disse omfatter også IT-sikkerhet.

2.2. Risikostyring

NBIM styrer risiko knyttet til IT-sikkerhet sammen med øvrig operasjonell risikostyring i virksomheten. Alle identifiserte risikoer knyttet til IT-sikkerhet behandles, vurderes og håndteres gjennom sentrale prosesser. Risiko vurderes gjennom regelmessige ledelsesprosesser, prosessgjennomganger og leverandørgjennomganger. Risiko vurderes også i forbindelse med endringer og hendelser.

NBIM har verktøy, organisasjon, prosesser, kontroller og metodikk for å identifisere, vurdere og håndtere risiko. NBIMs ledelse benytter vedtatte retningslinjer for risikoklassifisering og risikoaksept.

2.3. Styrende dokumenter for IT-sikkerhet

Styring av IT-sikkerhet i NBIM er et sentralt risikoområde som er adressert i lov, forskrift, prinsipper og virksomhetsovergripende krav fra Norges Banks hovedstyre, sentralbanksjefen og NBIMs ledelse. Krav og retningslinjer knyttet til IT-sikkerhet besluttet av NBIMs ledelse, dokumenteres i styrende dokumenter i form av policyer, retningslinjer og stillingsinstrukser. Policyer er gitt av direktøren for NBIM (CEO). Retningslinjene baseres på policyene og gis av NBIMs øvrige ledere. NBIMs styrende dokumenter er formelle dokumenter som skal være godkjente og oppdaterte.

NBIM har benyttet IT-sikkerhetsstandarden ISO/IEC 27001 som et av flere rammeverk for å støtte sin styring av og kontroll med IT-sikkerhet.

2.4. Operasjonalisering av IT-sikkerhet

NBIM har operasjonalisert sin styring av og kontroll med IT-sikkerhet gjennom fastsatte ansvarsområder, bruk av interne og eksterne ressurser, prosesser, prosedyrer, kontroller, samt tekniske løsninger. Etablerte tiltak er både preventive og oppdagende. NBIM har satt IT-sikkerhetskrav internt og til eksterne tjenesteleverandører. Kravene dekker dimensjonene konfidensialitet, integritet og tilgjengelighet og følges opp ved bruk av regelmessige tester og undersøkelser.

2.5. Måling og forbedring

Styring av og kontroll med IT-sikkerhet er en kontinuerlig prosess som skal identifisere, vurdere, håndtere og følge opp IT-sikkerhetsrisiko slik at risikoen er innenfor akseptabelt nivå. Prosesser for IT-sikkerhetsstyring hos NBIM skal oppdateres løpende, minimum årlig, og utvikles slik at de tilfredsstiller de relevante kravene. Gruppen for operasjonell risiko overvåker og kontrollerer de operasjonelle prosessene knyttet til IT-sikkerhet. Internrevisjonen gjennomfører revisjoner innen IT-sikkerhet basert på sin risikotilnærming.

3. Funn og konklusjon

3.1. Bakgrunn

Vi har gjennomgått NBIMs styring av og kontroll med IT-sikkerhet for å vurdere om denne i det alt vesentlige er utformet og implementert i henhold til de fastsatte målekriteriene. Formål og rammer for oppdraget fremgår i avsnitt 1.

Vi har utført vårt arbeid i henhold til ISAE 3000. Vår konklusjon er basert på NBIMs styring av og kontroll med IT-sikkerhet slik den er utformet og implementert på tidspunktet for datering av denne rapporten.

3.2. Funn

NBIM har gjennom 2012 gjennomført endringer som har styrket styring av og kontroll med IT-sikkerhet.

Tidligere har styring av og kontroll med IT-sikkerhet vært organisert i den operasjonelle IT-virksomheten.

Ny organisering hvor styring av og kontroll med IT-sikkerhet er tillagt gruppen for operasjonell risikostyring klargjør arbeidsdelingen mellom den operative linjen og risikoovervåking og kontroll. Omorganiseringen har også bidratt til forbedring og videreutvikling av eskaleringsprosedyrer for IT-sikkerhetsrisikoer og dokumentasjon. Dette medfører at styring av og kontroll med IT-sikkerhet er blitt tydeliggjort og har fått en klarere forankring på ledelsesnivå.

For å gjennomføre IT-sikkerhetsvurderinger benytter NBIM ekstern spisskompetanse i et betydelig omfang. Styring av og kontroll med IT-sikkerhet må være tett koblet med virksomhetsrisiko. NBIM har relativt begrensede interne ressurser med tilstrekkelig kompetanse til dette arbeidet og er etter vår vurdering derfor avhengig av noen få nøkkelpersoner.

3.3. Konklusjon

Utforming
Med de endringer som er beskrevet ovenfor mener vi at styring av og kontroll med IT-sikkerhet i NBIM i det alt vesentlige er utformet i samsvar med målekriteriene.

Implementering
Med unntak av de endringene som er gjennomført i 2012, mener vi at styring av og kontroll med IT-sikkerhet i det alt vesentlige er implementert slik det er utformet. En del av endringene har bare virket i en kort periode eller er i ferd med å bli implementert.

Oslo, 11. februar 2013
Deloitte AS

Aase Aa. Lundgaard
statsautorisert revisor

Vedlegg 1

Nærmere om vurderingsgrunnlaget

Risikostyring

Risikostyring handler i denne sammenheng om virksomhetens prosesser for å identifisere og kvantifisere risiko, og hvordan resultatene av en risikovurdering styrer og avgjør ledelsens tiltak og prioriteringer for å håndtere risiko knyttet til IT-sikkerhet. For hver identifiserte risiko skal det foretas en dokumentert beslutning om risikoen kan aksepteres, eller om det skal iverksettes tiltak for å redusere eller unngå den.

Styringssystem for IT-sikkerhet

Virksomheten skal etablere, implementere, drifte, måle, revidere, vedlikeholde og forbedre et dokumentert styringssystem for IT-sikkerhet. Utformingen av styringssystemet skal sees i sammenheng med virksomhetens aktiviteter og den risiko virksomheten står ovenfor.

Ledelsens støtte og ressursstyring

Ledelsen skal kunne dokumentere sin støtte til etablering, implementering, drift, måling, revisjon, vedlikehold og forbedring av styringssystemet for IT-sikkerhet. Ledelsen skal etablere en policy for styringssystem for IT-sikkerhet, forsikre at planer, mål, roller og ansvar for IT-sikkerhet er etablert og at tilstrekkelig med ressurser er gitt. Videre skal ledelsen sette kriterier for aksept av risiko, samt akseptabelt risikonivå. Det skal gjennomføres interne revisjoner av styringssystemet for IT-sikkerhet, samt ledelsens gjennomgang.

Opplæring, kompetanse og fokus

Virksomheten skal forsikre at alt personell som har fått tildelt ansvar i styringssystemet for IT-sikkerhet har tilstrekkelig kompetanse til å utføre de oppgavene de er satt til å utføre. Alt personell bør gjøres kjent med hvordan deres aktiviteter kan påvirke IT-sikkerheten, og hvordan de kan bidra til å nå målene med styringssystemet for IT-sikkerhet. Virksomheten bør identifisere den nødvendige kompetansen som trengs for personell som gjennomfører oppgaver som påvirker styringssystemet for IT-sikkerhet. Opplæring bør vurderes for å møte behovet for kompetanse på området. Kvalifikasjoner, erfaring, opplæring og utdanning av personell bør dokumenteres.

Sikkerhetspolicy

Det er viktig at virksomhetsledelsen gir sin støtte til arbeidet med IT-sikkerhet, og at deres formidling av forventninger og krav til IT-sikkerheten er tydelig og i tråd med virksomhetskrav og relevante lover og forskrifter. Ledelsens støtte, forventninger og krav bør være nedfelt i virksomhetens sikkerhetspolicy, som bør være formidlet og revidert på en hensiktsmessig måte.

Organisering av IT-sikkerhet

Organisering av IT-sikkerhet handler om virksomhetens overordnede tiltak for å opprette og sikre iverksettelsen av IT-sikkerhet innenfor virksomheten. Tildeling av sikkerhetsroller og -ansvar, samt koordinering og revidering av IT-sikkerhet i hele virksomheten er sentralt i styringen av IT-sikkerhet. Krav satt til eksterne interessenter eller tredjeparter, samt håndtering og oppfølging av disse, er en viktig del av dette sikkerhetsarbeidet.

Personellsikkerhet

Målet med personellsikkerhet er å sikre at ansatte, innleide konsulenter og tredjepartsbrukere forstår sin sikkerhetsrolle og sitt ansvar, og er egnet for rollen de har, samt å redusere risikoen for uønskede handlinger. Personellsikkerhet omfatter blant annet at roller og ansvar skal være definert og dokumentert, at tilgangsrettigheter endres eller fjernes ved avslutning av ansettelse, kontrakt eller avtale.

Administrasjon av aktiva

Målet med administrasjon av aktiva er å oppnå og opprettholde nødvendig beskyttelse av virksomhetens aktiva. Alle aktiva bør registreres og tildeles en eier, og ansvaret for opprettholdelse av nødvendige sikringstiltak bør tilskrives bestemte roller. Eieren kan eventuelt delegere iverksettelsen av bestemte sikringstiltak, men vedkommende er fortsatt ansvarlig for behørig beskyttelse av aktiva.

Fysisk og miljømessig sikkerhet

Målet med fysisk og miljømessig sikkerhet er å forhindre uautorisert adgang til, skade på og forstyrrelse av virksomhetens lokaler og informasjon og informasjonsbehandlingsutstyr. Det kan for eksempel være snakk om ulike former for beskyttelsestiltak som bruk av fysiske sikkerhetssoner, adgangskontroller osv.

Kommunikasjons- og driftsadministrasjon

Kommunikasjons- og driftsadministrasjon handler om å sikre korrekt og sikker drift av informasjonsbehandlingsutstyr gjennom etablering av retningslinjer og rutiner for håndtering av endringer, styring av tredjepartstjenester og systemteknisk sikkerhet. Videre handler det om tiltak for å hindre uautorisert tilgang til systemer og for å oppdage eventuell uautorisert tilgang.

Aksesskontroll

Aksesskontroll handler om å etablere policyer, rutiner og kontroller for å sikre at tilgang til informasjonsbehandlingsutstyr og virksomhetsprosesser er gitt til de som trenger det, at tilganger samtidig er tilstrekkelig begrenset og at systemet hindrer uautorisert tilgang.

Anskaffelse, utvikling og vedlikehold av informasjonssystemer

Anskaffelse, utvikling og vedlikehold av informasjonssystemer handler om å forebygge og oppdage tekniske sårbarheter som kan føre til negative følger for virksomhetens drift eller sikkerhet. I denne sammenhengen handler dette også om håndtering av risiko for informasjonslekkasjer.

Administrasjon av IT-sikkerhetsbrudd

Administrasjon av IT-sikkerhetsbrudd handler om virksomhetens håndtering og rapportering av IT-sikkerhetshendelser og svakheter i forbindelse med informasjonssystemer. Målet er å redusere konsekvenser av slike, og å forebygge at de oppstår.

Kontinuitetsplanlegging

Kontinuitetsplanlegging for IT-sikkerhet handler om å motvirke avbrudd i forretningsaktivitetene og beskytte kritiske driftsprosesser fra konsekvensene av større feil i informasjonssystemer eller katastrofer, og å sikre at de gjenopptas i rett tid. IT-driftskontinuitet og IT-sikkerhetsaspekter er en viktig del av kontinuitetsplanleggingen.

Samsvar og etterlevelse

Samsvar og etterlevelse handler i denne sammenheng om virksomhetens aktiviteter for å sikre og kontrollere at informasjonssystemer og prosedyrer er i samsvar med retningslinjer og krav til IT-sikkerhet.