UiO : Universitetet i Oslo
Enhet for intern revisjon

Til **Universitetsstyret**
Fra **Enhet for intern revisjon**

Sakstype:	**Orienteringssak**
Møtesaksnr.:	**O-sak 2**
Møtenr.:	**3/2014**
Møtedato:	**6. mai 2014**
Notatdato:	**25. februar 2014**
Arkivsaksnr.:	
Saksbehandler:	**Morten Opsal**

Årsrapport 2013 fra Enhet for intern revisjon

Henvisning til lovverk, plandokumenter og tidligere behandling i styret:
Enhet for intern revisjon (EIR) har i sin instruks at vi skal bistå universitetets øverste ledelse med å se etter at en tilfredsstillende intern kontroll er etablert og at den fungerer som forutsatt slik at universitetet drives effektivt, rasjonelt, forsvarlig og i samsvar med overordnede mål, vedtak og forutsetninger.

Hovedproblemstillinger i saken:
Denne årsrapporten viser status på reviderte områdene. Rapporten omtaler også en ekstern evaluering av hvorvidt enheten følger internasjonale standarder i sitt arbeid. Rapporten fra den eksterne evalueringen er vedlagt i saken.
Videre omtaler den EIRs rolle i varslinger og rollen som personvernombud.

Morten Opsal
fungerende revisjonssjef

Vedlegg:
- EIR Årsrapport 2013
- Rapport fra PWC: Uavhengig vurdering av Enhet for intern revisjon – Universitetet i Oslo

UiO : Universitetet i Oslo

Enhet for intern revisjon

ÅRSRAPPORT 2013

OSLO, 20. februar 2014

Morten Opsal

Fungerende revisjonssjef

INNLEDNING

Enhet for intern revisjon (EIR) har i sin instruks at vi skal bistå universitetets øverste ledelse med å se etter at en tilfredsstillende intern kontroll er etablert og at den fungerer som forutsatt slik at universitetet drives effektivt, rasjonelt, forsvarlig og i samsvar med overordnede mål, vedtak og forutsetninger.

Bidraget fra EIR knytter seg til de områder det er utført revisjoner på, jf årsplan.

EIR har også i sin instruks at vi skal følge internasjonale standarder og regler, utgitt av IIA (Institute of Internal Audotors). Et av vilkårene i standardene er at det minst hvert 5. år skal foretas en ekstern evaluering av hvorvidt enheten følger standardene. EIR fikk utført en slik ekstern evaluering høsten 2013. Forberedelse, gjennomføring og deretter oppfølgingen av den eksterne evalueringen har tatt en del tid i siste halvår 2013. Mer om resultatet av evalueringen i eget avsnitt.

OPPFØLGING AV ÅRSPLAN 2013

Revisjonsplanen for 2013 ble lagt fram for universtetsstyret til orientering i junimøtet, og ble i matriseform presentert slik:

Nr	Revisjonsområder 2013	Q1	Q2	Q3	Q4
1	Oppfølging IHR			x	x
2	Oppfølging styrevedtak		x	x	x
3	Strategi 2010 - 2020		x	x	x
4	Sentraladm - koordinering				
5	Risiko ved systemer som delvis forvaltes av USIT		x	x	x
6	Tilgang til IT-systemer	x	x		
7	Impl. Kvalsystem Helseforskning	x			
8	Oppfølging av butikksalgene KHM/NHM			x	
9	EU-revisjoner	x	x	x	x
10	Risikogjennomganger	x	x	x	x
11	Ad hoc	x	x	x	x

Ad hoc oppgaver som er gjennomført i 2013:

- Oppdragspraksis
- Risikoanalyse SA5
- Bilagslønn

Endringer i årsplanen har blitt diskutert med universitetsdirektøren.

REVISJONER/OPPGAVER 2013

Nr 1: Oppfølging IHR

Innledende arbeid med revisjonen ble igangsatt høsten 2013. På grunn av fortsatt arbeid i IHR-prosjektet ut hele 2013, herunder struktur på å måle gevinster av prosjektet, ble revisjonen ikke startet opp i løpet av 2013.

Nr 2: Oppfølging styrevedtak

Styrevedtak gjennomføres i stor grad, men vedtak som gjelder hele Universitetet er for generelt formulert. Det mangler rutiner for en mer systematisk oppfølging og tydelig plassering av ansvar for vedtak som gjelder hele Universitetet.

EIR anbefaler at:

- det etableres rutiner som gjør det lettere for ledelsen og Styret å ha totaloversikt over status på gjennomføring av vedtak.
- det etableres rutiner som sikrer en felles forståelse, og en tryggere oppfølging av vedtak som inneholder formuleringen «med de endringsforslag som framkom i styremøtet» og lignende.
- vedtakene utformes på en slik måte at det forenkler oppfølgingen
- det arbeides videre med å tydeliggjøre fullmakter, roller, ansvar og myndighet i organisasjonen, noen som vil kunne bidra positivt til gjennomføring av Styrets vedtak.

Det er satt en svarfrist på rapportens anbefalinger til 7.3.2014.

Nr 3: Strategi 2010 – 2020

Revisjonen er ikke igangsatt, da området skal dekkes av UiOs ledelse i dialog med fakultetene våren 2014.

Nr 4: Sentraladm – koordinering

Revisjonen ikke igangsatt, da området etter at planen ble laget har blitt vurdert til å inngå i revisjonsområde 1: Oppfølging IHR.

Nr 5: Risiko ved systemer som delvis forvaltes av USIT

Problemstilling: Er det særskilt risiko for UiO ved fellessystemer i sektoren som forvaltes av UiO/USIT, men som har egne styrer.

Da EIR igangsatte kartlegging av området ble vi kjent med at ledelsen ved UiO har arbeidet med forholdet. Vi fikk tilgang til dokumenter og korrespondanse som viser at risikoer er dokumentert og oversendt KD og Samordna opptak (SO). Av den grunn var det ikke aktuelt med en egen revisjon av området.

Nr 6: Tilgang til IT-systemer

Revisjonen har hatt følgende formål:

Å se etter om tilgangsstyring til IT-ressurser ved UiO skjer etter retningslinjene i IT-sikkerhetshåndbokens kapittel 11: Identifikasjon, autentisering og autorisering.

Revisjonen har sett på rutiner rundt tildeling og ajourhold av:

- Generelle tilganger til UiOs IT-ressurser
- Spesielle tilganger (privilegerte brukere)
- Tilgang til IT-systemene på nivå 1 og 2 ved UiO

Det ble gjennomført 27 intervjuer med aktuelle personer i løpet av revisjonen.

Revisjonens konklusjon: Rutiner som sikrer at tilgangsstyring til IT-ressurser ved UiO skjer etter retningslinjene i IT-sikkerhetshåndbokens kapittel 11 er ikke tilfredsstillende. Det er spesielt endring og avslutning av tilganger som ikke ivaretas.

Rapporten peker på noen forhold som det må arbeides med.

- Rutiner for å sikre korrekt ajourhold av tilganger ved endringer i eller avslutninger av arbeidsforhold.
- Avklare på hvilken måte «brukere på grunnlag av kontrakt» skal behandles mht autoritativ kilde.

Vi ser det som naturlig at USIT og OPA i samarbeid gjennomgår rapporten og utarbeider plan for å forbedre påpekningene.

Svarfrist for tilbakemelding på rapporten ble satt til 15.2.2014. og er senere forlenget til 1.3.2014

Nr 7: Implementering kvalitetssystem helseforskning

Revisjonen ble ferdigstilt i februar 2013, og var med i EIRs årsrapport 2012. Det vises til status på området under kapittel Oppfølging senere i rapporten.

Nr 8: Oppfølging av butikksalgene KHM/NHM

Revisjonen ikke igangsatt, da Riksrevisjonen hadde en oppfølging av området i sin gjennomgang av UiO i 2013.

Nr 9: EU-revisjoner

EIR har fortsatt utført oppgaven med å foreta finansiell revisjon av prosjekter ved UiO som er tildelt midler fra EU, etter de regler EU har bestemt. Vi reviderte 7 EU prosjekter i 2013, en nedgang fra 17 i 2012. Vi konstaterer at kompetansen på innrapporteringen er varierende, men i hovedsak tilfredsstillende. Prosjektene som kommer til revidering har større volum enn tidligere.

Ad-hoc: Risikoanalyse SA5

EIR ble bedt om å bidra med risikoanalyse av ny organisasjonsmodell av SA5. Ny organisasjonsmodell ble behandlet i sak i UiOs styre i junimøtet 2013, hvor risikoanalysen var en del av saksdokumentene.

Ad-hoc: Bilagslønn

Bilagslønn er definert som alle honorarer og lønnsutbetalinger som ikke utbetales som et fast månedlig beløp.

Revisjonen ble satt i gang som en følge av en feilutbetaling på kr. 90.000 fra Lønnings-seksjonen (LS) i juni 2013. Personen som mottok pengene har ingen tilknytning til UiO og opplyser at han ikke kan betale tilbake pengene. Personen er politianmeldt, men anmeldelsen er henlagt av politiet, og saken sendt til inkasso.

Formålet med revisjonen var å se etter om de interne kontrollrutinene for bilagslønn var tilfredsstillende ved LS, og det ble gjort et forsøk på å finne en forklaringen på hvordan feilutbetalingen kunne skje.

Revisjonens konklusjon: Internkontrollen for bilagslønn må styrkes og rutinene bør foreligge skriftlig. For å kunne jobbe effektivt er LS avhengig av at bilag i større grad kommer feilfritt inn til avdelingen. Prosesseierskap for stipend, styrehonorar og selvstendig næringsdrivende (som faller utenfor bilagslønns-prosjektet) må tydeliggjøres. Vi anbefaler også at LS styrker ledelses-oppfølgingen med å utvikle periodiske oversikter med oppfølging av indikatorer, gjerne utarbeidet fra en risikoanalyse.

Vi har ikke funnet årsaken til feilutbetalingen og det er ikke funnet bevis for at det dreier seg om misligheter. Likevel er det mistenkelig at så mye kan ha gått feil i en enkelt registrering.

Oppfølging av revisjoner fra tidligere år

Sikkerhet mobile enheter

EIRs konklusjon fra 2012 var at Informasjonssikkerheten ikke er tilfredsstillende ivaretatt ved bruk av mobile enheter ved UiO. EIR pekte på 3 forhold som må utvikles.

a) En samlet risikoanalyse på området lages, som dokumenteres og fornyes med jevne mellomrom. Og den må inneholde risikoreduserende tiltak.
b) Prosedyre for klassifisering av informasjon implementeres i organisasjonen.
c) Et kompetanseopplegg lages for å bevisstgjøre den enkelte bruker om risikoeksponering og UiO-regler.

USIT var i hovedsak enige i konklusjonene i rapporten og uttalte at tiltakene ville bli iverksatt i løpet av 2013.

Ved oppfølging primo januar 2014 har USIT gitt følgende respons:
«USIT har opprettet en egen gruppe for mobile enheter. Vi har slitt med bemanning i gruppa, men det er på plass nå. Det står på årsplanen vår for i år, foreløpig med mål om å ha en rapport om hva UiO bør gjøre og hvilket rammeverk, SW produkt, for Mobile Device Management (MDM) vi skal benytte, klar innen 28.2. Etter det vil vi gjøre valg av rammeverk og implementere løsninger. Forventer pilotering i 2. kvartal 2014 og utrulling etter det.»

Revisjon implementering kvalitetssystem helseforskning

I svar på revisjonsrapporten skisserte daværende Forskningsadministrative avdeling (FA) en rekke opplæringstiltak som skulle bidra til å sikre etterlevelse av helseforskningsloven. Det gjenstår fortsatt å beslutte hva som skal bli obligatorisk.

Revisjonen pekte på at IT-infrastruktur som støtter kvalitetssystemet ville være nødvendig for å sikre bruk og effektivitet. FA og USIT har så langt ikke kommet med formelt svar på hvordan dette skal løses.

For å kunne tilby sikker lagring av forskningsdata er en forskningsserver helt nødvendig. USIT har etter at revisjonsrapporten ble levert fått midler til dette og regner med å være i drift mars 2014.

Internrevisjonen vil i Q1 2014 følge opp at foreslåtte tiltak fra FA blir fulgt opp, og at roller og ansvar i denne forbindelse er plassert i ny organisasjon.

Ekstern evaluering av EIR

Enhet for intern revisjon (EIR) har som mål å følge de internasjonale internrevisjons-standardene. Et av kravene i standardene er at man må gjennomføre en uavhengig kvalitetsgjennomgang av internrevisjonsfunksjonen minimum hvert 5. år. PWC ble tildelt oppgaven etter en anbudsrunde.

Evalueringen fokuserte på følgende hovedtemaer:

1. Internrevisjonens mandat og rolle (herunder uavhengighet)
2. Metodikk for årlig risikovurdering og utarbeidelse av årsplan
3. Metodikk for gjennomføring av revisjonsprosjekter
4. Metodikk for utarbeidelse av årsrapport (evt også halvårsrapport)
5. Styringsprosess knyttet til HR, herunder kompetansemåling /-utvikling
6. Universitetets oppfatning av om internrevisjonen tilfører verdi/nytte

Hovedkonklusjonen i rapporten peker på to forhold:

- Behov for en avklaring av internrevisjonens rolle i organisasjonen, og et tydeligere ambisjonsnivå fra ledelsen tilpasset rollen
- Ta i bruk en mer strukturert metodikk for internrevisjonens risikovurderinger, utarbeidelse av årsplan og gjennomføring av oppdrag.

EIR jobber sammen med ledelsen for å følge opp anbefalingene i rapporten. Styret vil bli holdt orientert om de deler av prosessen som angår styret.

Andre forhold

Varslinger

UiO har etablert et nytt system for varslinger i 2013, både for varslinger fra studenter og fra ansatte. (SI-FRA-systemet). EIR har en rolle i begge varslingskanalene ved at vi er kopimottaker av varslene når de kommer og skal følge opp at varsler blir behandlet i linjen etter hensikten.

Det har gjennom året kommet 10 varsler fra studenter og ingen fra ansatte. Alle sakene har blitt behandlet i organisasjonen, og per dato er det 1 sak som ikke er avsluttet. Det har i flere tilfeller tatt lang tid før saksbehandling ble igangsatt.

Personvernombud

EIR ivaretar funksjonen som personvernombud (PVO) for administrative behandlinger ved UiO, estimert til 20 % stilling. Den ivaretas av 1 medarbeider, godkjent av Datatilsynet.

Et register er etablert for å holde oversikt over hvilke behandlinger av personopplysninger som foregår ved UiO, og PVO har oppfølgingen av at behandlingene skjer ihht lov og at registeret er oppdatert.

Stedlige kontroller utføres ved grunnenheter, og bidrar til å sikre at registeret inneholder alle aktuelle behandlinger og at det er á jour.

Effektene av stedlige kontroller er at bevissthet og kompetanse hos besøkt enhet øker. Samtidig er det vilje til å utbedre de mangler som påpekes.

Arbeidet med stedlige kontroller vil pågå kontinuerlig og målet er å rekke over alle grunnenheter i løpet av 4-5 år.

Personvernombudet har mottatt 3 avviksmeldinger i 2013, hvorav 2 er sendt til Datatilsynet.

Annet

EIR blir jevnlig spurt om råd fra enheter ved UiO, noe vi synes er veldig positivt.

Personalsituasjonen

EIR har 4 årsverk, og alle har vært besatt gjennom året. En medarbeider har hatt foreldrepermisjon hele 2013, og vikarer har vært benyttet for å fylle stillingshjemmelen.

En medarbeider har i 2013 fullført managementprogram ved BI med tittel «Intern revisjon – governance – risikostyring – intern styring og kontroll», og oppnådd både den norske tittelen Diplomert internrevisor og den internasjonale sertifiseringen CIA (Certified Internal Auditor). Det medfører en styrking av den faglige kompetanse i enheten.

Sammendrag av prosjektoppgave «Risikostyring på UiO»

Medarbeideren som gjennomførte managementprogrammet ved BI skrev en UiO-relevant prosjektoppgave, og her er et kort sammendrag av den oppgaven.

«I 2009 ble det første rammeverket for risikostyring på UiO godkjent av Universitetsstyret. Siden den gang har UiO kommet et godt stykke på vei med risikostyring, og risikokart er nå inkludert som en naturlig del av Styrets årsplan. Analysen viser at selv om risikostyring allerede er implementert og integrert i virksomhetsstyringen på UiO, kan det likevel være nyttig å lage en plan for videre fremdrift med tydelige roller og ansvarsforhold. I tillegg er det et behov for å få en mer konsistent begrepsbruk og en mer systematisk fremstilling av informasjonen, slik at det blir enklere å se sammenhengene mellom mål, kritiske suksessfaktorer, risikoer og tiltak. Dette vil igjen forenkle oppfølgingen og spisse styringsdialogen.
Når det her, og i faglitteraturen for øvrig, snakkes om risikostyring, så er det systematikken i dette som er viktig for å kunne sikre de fordeler som metoden kan gi. Dersom risikostyringen blir enda bedre integrert, systematisert og dokumentert i styringsprosessen på alle nivåer i organisasjonen, vil UiO ha større mulighet for å fange opp og igangsette tiltak til de risikoer som kan true måloppnåelsen».

Universitetet i Oslo
Att: Enhet for Internrevisjon v/ leder
Kopi: Universitetsdirektøren

Oslo, 11. november 2013

Uavhengig vurdering av Enhet for Internrevisjon - Universitetet i Oslo

Bakgrunn og formål
Enhet for Internrevisjon (EIR) har som mål å følge de internasjonale internrevisjonsstandardene. Et av kravene i standardene er at man da må gjennomføre en uavhengig kvalitetsgjennomgang av internrevisjonsfunksjonen minimum hvert femte år. Kvalitetsgjennomgangen skal utføres etter fastlagte kriterier i internrevisjonsstandard PA-1312. Formålet med gjennomgangen er å vurdere i hvilken grad internrevisjonsfunksjonen oppfyller kravene i de internasjonale internrevisjonsstandardene. Det er i tillegg normalt å inkludere en vurdering av:

- Om internrevisjonen generelt er verdiskapende for virksomheten
- Mulige forbedringstiltak – der det foreligger eventuell mangelfull standardetterlevelse
- Mulige forbedringstiltak – der det er tilfredsstillende standardetterlevelse, men foreligger mangler i arbeidsformens hensiktsmessighet og effektivitet, eller arbeidsformen ikke er i tråd med god bransjepraksis.

PwC har blitt engasjert til å utføre den uavhengige kvalitetsgjennomgangen. Arbeidet har pågått i oktober/november 2013 og hatt et omfang på ca. 6-7 dagsverk.

Vurderingskriterier
Kvalitetsgjennomgangen har fokusert på følgende hovedtema:

1. Internrevisjonens mandat og rolle (herunder uavhengighet)
2. Metodikk for årlig risikovurdering og utarbeidelse av årsplan
3. Metodikk for gjennomføring av revisjonsprosjekter
    a. Planlegging
    b. Gjennomføring
    c. Rapportering
    d. Kvalitetssikring/dokumentasjon/arkivering
4. Metodikk for utarbeidelse av årsrapport (eventuelt også halvårsrapport)
5. Styringsprosesser knyttet til HR, herunder kompetansemåling/-utvikling
6. Universitetsledelsens oppfatning av om internrevisjonen tilfører verdi/nytte

Som vurderingskriterier har vi anvendt kravene i "Etiske regler og standarder for profesjonell utøvelse av internrevisjon" (som er de internasjonale profesjonsstandardene for internrevisjon), samt det vi vurderer som god bransjepraksis basert på vår erfaring med internrevisjon i statlig og privat sektor.

Konklusjon og tilsvar fra Enhet for Internrevisjon

Hovedkonklusjon

Som hovedkonklusjon vurderer vi universitetets internrevisjonsfunksjon til å ikke være i tråd med gjeldende standarder.

Ledelsen vurderer internrevisjon som en generelt viktig kontrollfunksjon, men totalt sett som lite verdiskapende i sin nåværende form.

Begrunnelse

I forhold til standardverket og god bransjepraksis foreligger det vesentlige mangler ved universitetets internrevisjonsfunksjon. Manglene springer ut fra en uklar rolle for internrevisjonen og et uklart ambisjonsnivå hos ledelsen ved universitetet for hva man ønsker med internrevisjonen.

Det foreligger ikke en systematikk for årlige risikovurderinger, prosjektprioritering og utarbeidelse av årsplaner. Rolleuklarheten og plantilnærmingen gjør at internrevisjonens prosjektportefølje fremstår lite helhetlig og uten en klar forankring i et styre- og toppledelsesbehov.

Internrevisjonens operative metodikk er mangelfull. Det foreligger nødvendig malverk, men ikke en helhetlig metodikk som sikrer at man i de ulike revisjonsstegene utfører og kvalitetssikrer nødvendige oppgaver. Vår gjennomgang av utførte revisjoner viser at vesentlige elementer i revisjonsarbeidet er mangelfullt, eksempelvis ved at de enkelte revisjonene gjennomføres uten klare scope-definisjoner, risikovurderinger, revisjonskriterier, teststrategier og konklusjoner.

Funksjonen har begrenset kapasitet (3-4 årsverk) og kompetansetilgang i forhold til omfanget av virksomheten og tematikken som skal revideres.

Av positive observasjoner fremheves det at internrevisjonen tilfredsstiller uavhengighetskravene i standardene, det er etablert en tilfredsstillende struktur for arkivering av utført arbeid, og det er en positiv holdning hos leder til kompetanseutvikling og kurs.

Intervjuene med ledelsen ga, med ett unntak, et negativt bilde. Det oppfattes uklart hvem funksjonen reviderer på vegne av, og det stilles spørsmål ved hvilke revisjoner som settes på årsplanen. Flertallet av de intervjuede savnet et strategisk fokus i revisjonene, og mente at hovedfokuset var for operativt. Videre oppfattes det som uklart hvilke kriterier som legges til grunn i de enkelte revisjonene, og det savnes helhetlige konklusjoner på reviderte tema. Flere ledere uttrykte at selv om revisjonsrapportene fremhever enkelte anbefalinger som i og for seg er relevante, frembringer ikke revisjonene noe nytt, og det mangler ofte vurderinger av tema som ledelsen anser som vesentlige. Intervjuede ledere pekte imidlertid på at funksjonen er liten, at dens rolle er uklar, at den får begrenset oppmerksomhet fra ledelsen, og at de selv burde involvere seg mer i planfasen av revisjonsarbeidet for å sikre økt nytte. Intervjuene underbygger således behovet for å definere rolle og ambisjonsnivå for internrevisjonen, kalibrere kompetanse- og kapasitetstilgang i forhold til valgt løsning, samt styrke revisjonsmetodikken – særlig i forhold til planleggingsfasen og samspill med ledelsen.

Anbefalinger

For å bringe internrevisjonen i tråd med standardene bør rollen og ambisjonsnivået for internrevisjon avklares, metodikken bør styrkes og kapasiteten/kompetansen balanseres i forhold til valgt løsning. Anbefalingene er rettet både mot ledelsen og internrevisjonsfunksjonen. Av konkrete tiltak anbefaler vi følgende:

1. Det bør entydig fastsettes og forankres hvem internrevisjonen rapporterer til og ambisjonsnivået for internrevisjon. Av særlig viktighet er det å presist definere hvem som bestemmer hvilke prosjekter internrevisjonen skal gjennomføre og hvem som er primærmottaker for internrevisors rapportering.
2. Rolle og ambisjonsnivå vil gi føringer for art og omfang av revisjonsaktiviteter og tilhørende kapasitets- og kompetansebehov. Vi anbefaler at kapasitet- og kompetansetilgang vurderes i sammenheng med den foreslåtte rolle- og ambisjonsdiskusjonen.
3. Det bør etableres en strukturert metodikk for internrevisjonens risikovurderinger, prosjektprioritering og utarbeidelse av årsplan. Metodikken bør sikre at årsplanene har en helhetlig tilnærming i forhold til rolle og ambisjonsnivå og at tilstrekkelig kompetanse og kapasitet er tilgjengelig. Årsplaner bør fremlegges ved inngangen til nytt revisjonsår. Foreslåtte enkeltrevisjoner bør være tydelige på om de har til formål å verifisere om noe er tilstrekkelig kontrollert, har til formål å gi råd om forbedring av kjente mangler, eller har til formål å kartlegge status på et område man er usikker på om er tilstrekkelig kontrollert. En forutsetning for å kunne presisere dette er at internrevisjonen har et bilde av risiko og kontrollnivå på universitetet, noe som er formålet med risikovurderingen som skal legges til grunn for årsplanforslaget.
4. Det bør utarbeides en metodikkhåndbok med overordnete føringer for hvordan man definerer, planlegger, gjennomfører, konkluderer og rapporterer et revisjonsprosjekt, inkludert kvalitetssikrings- og arkiveringsrutiner. Det anbefales økt vektlegging av tydelige og forankrede revisjonskriterer før revisjonsoppstart, noe som vil gi grunnlag for helhetlige konklusjoner på om temaet man reviderer er gjenstand for betryggende kontroll. Videre anbefales økt bruk av testing, slik at man sikrer at eventuelle positive konklusjoner på kontrollnivå baseres på tilstrekkelig og hensiktsmessig revisjonsbevis.
5. Det bør etableres en systematikk for å innhente tilbakemeldinger på gjennomførte revisjoner. Videre bør internrevisjonens rutiner for kvalitetssikring, tilbakemelding og kompetanseutvikling struktureres. I sum vil dette gi mer strukturerte læringsprosesser.

Anvendt metodikk, dokumentoversikt og intervjuoversikt
Kvalitetsgjennomgangen har vært utført gjennom intervjuer og dokumentgjennomgang. Nedenfor vises en oversikt over gjennomgått materiale:

<u>Dokumentgjennomgang:</u>
- EIRs egenevaluering av standardetterlevelse
- Instruks for EIR, samt "visjon og verdier"
- EIRs metodikk/malverk/verktøy
- Årsplan 2012 og 2013, samt årsrapport for 2012
- Dokumentasjon fra 3 utvalgte revisjonsprosjekter (to fra 2012 og ett fra 2013)
- Gjennomgang av EIRs arkiveringsstruktur (mappestruktur)på server, med gjennomgang av utvalgte underliggende filer for å vurdere innhold

<u>Intervjuer:</u>
- Fellesgjennomgang med alle i EIR der metodikk og malverk ble gjennomgått
- 1-1 intervju med Leder for internrevisjonen
- 1-1 intervjuer med de to øvrige ansatte internrevisjonen
- Rektor
- Universitetsdirektør
- IT-direktør

- Dekan HF
- Direktør virksomhetsstyring
- Økonimidirektør

Med vennlig hilsen
PricewaterhouseCoopers AS

Jonas Gaudernack
Partner, PhD
jonas.gaudernack@no.pwc.com
T: 95260769

Vedlegg: Tilsvar fra Enhet for Internrevisjon

Vedlegg: Tilsvar fra Enhet for Internrevisjon

EIR takker for utført oppdrag, og vi har tro på at rapporten vil bidra til forbedringer.

- At en enhets ROLLE i en organisasjon er klar og tydelig er særdeles viktig. Av rapporten framgår det at så ikke er tilfelle hva gjelder Enhet for Internrevisjon ved UiO (EIR). At jeg som leder for EIR opplever at vi har en klar rolle er til liten hjelp hvis det er en utbredt oppfatning at så ikke er tilfelle. Dette er et grunnleggende problem som må avklartes raskt.

  Tiltak: *EIR vil foreslå at dette fremmes som egen sak for universitetsstyret, og saken bør ta opp i seg EIRs rapporteringslinjer. EIRs formål, fullmakter og ansvar (slik de i dag er beskrevet i instruksen bør også vurderes)*

- Videre ser jeg det som meget positivt at rapporten tar opp spørsmålet om universitetsledelsens ambisjonsnivå for EIR. I følge rapporten er det uklart.

  Tiltak: *EIR er med i et stort og godt fungerende nettverk for internrevisjoner ved universiteter og høgskoler i Norden. Vi har underrettet nettverket om at vi har hatt en ekstern kvalitetsgjennomgang, og vi har bedt om å få informasjon om hvordan ambisjonsnivået er beskrevet ellers i nettverket.*

- EIR har i alle sine årsplaner (siden 2003) understreket at vi i våre revisjoner ønsker å fokusere på det som er viktig for UiO. Planene har alltid vært gjenstand for diskusjoner med universitetsdirektør, og har alltid blitt lagt fram for Styret som orienteringssak. Jeg mener at EIR alltid har vært lydhøre i forhold til de innspillene vi har mottatt fra universitetsledelsen. Videre har vi alltid knyttet våre planer opp mot overordnede strategier og plandokumenter. *Men jeg har ingen problemer med å se at vårt arbeid preges av at det blir «nålestikk» inn i organisasjonen, og at tilnærmingen i vårt revisjonsarbeid bør være mer systematisk og helhetlig. Slik EIR har arbeidet til nå har vi ikke fått godt nok grunnlag for å kunne avgi en overordnet og helhetlig erklæring om forhold knyttet til kontroll: Mislighetsrisiko, hensiktsmessige risikostyringsprosesser, governance;, Jfr IIAs/NIRFs definisjon av «intern revisjon».*

  Tiltak: *Dette punktet kan sees i sammenheng med spørsmålet om ledelsens ambisjonsnivå for EIR. Ledelsen må klargjøre forventningene til EIR, og det må fortløpende følges opp om EIRs leveranser tilfredsstiller ledelsens behov.*

- At det ikke er samsvar mellom den negative tilbakemeldingen EIR får fra de intervjuede lederne, og de tilbakemeldingene jeg som leder for EIR de siste 11 årene har mottatt, og som jeg har formidlet videre til enhetens medarbeidere, finner jeg overraskende. Dette må avklares i dialog med universitetsledelsen.

  Tiltak: *Saken må tas opp til diskusjon snarest mulig mellom styreleder/rektorat, universitetsdirektør og leder for EIR.*

Mangler ved EIRs opplegg for årlige risikovurderinger/Systematisk risikovurdering tilknyttet årsplanleggingen.

- Det foretas risikovurderinger, men det er korrekt at de ikke er tilstrekkelig systematiske. De er heller ikke tilstrekkelig dokumenterte.

  Tiltak: *EIR er i ferd med å lage en skisse for et systematisk og dokumenterbart opplegg for årlige risikovurderinger. Det vil bli brukt i arbeidet med årsplan 2014. Vi vil gjerne ha tilbakemeldinger mht om dette opplegget er tilfredsstillende. Vi ser fortsatt et behov for å diskutere valg av revisjonsområder med universitetsledelsen (til nå universitetsdirektøren) før den endelige årsplanen utarbeides og fremlegges for Styret (pr. i dag som orienteringssak).*

MANGELFULL METODIKK

Manglende Scope

- EIR avtaler alltid FORMÅLET med revisjonen med den enheten som skal revideres, eller med den lederen som «eier» revisjonsområdet. Hensikten med det er å sikre oss at vi «treffer» best mulig med revisjonen og at den oppleves som nyttig. Vi har ansett dette som å være tilstrekkelig for å sikre et riktig «scope».

  Tiltak: *Vi vil i framtidige revisjonsoppgaver være mer bevisste på å avgrense revisjonsprosjektene.*

  Manglende revisjonskriterier

- Jeg ser at vi ikke har vært gode nok på dette i vår metodikk, men det dreier seg også om valg av metodikk. I mange av våre revisjonsprosjekter har vi benyttet COSO-rammeverket. (PWC har i denne kvalitetsgjennomgangen gitt uttrykk for at man ikke er tilhenger av det). I de tilfellene har vi vurdert internkontrollen ved en systematisk gjennomgang og vurdering av elementene i COSOs fem komponenter:

  Kontrollmiljøet, **R**isikovurdering, **I**nformasjon/kommunikasjon, **K**ontrollaktiviteter og **L**edelsesoppfølging. Jeg mener at dette gir et godt grunnlag for en helhetlig vurdering av internkontrollsystemet på det området som er revidert.
  Når vi bruker COSO-rammeverket så er det fordi det har fått en verdensomspennende utbredelse etter lanseringen i 1992.
  Dessuten er det tatt i bruk av Riksrevisjonen, og vår tanke har vært at det vil lette dialogen med dem.

  Tiltak*: I de tilfellene vi ikke benytter COSO-rammeverket i framtidige revisjoner, vil vi være bevisste på å definere REVISJONSKRITERIER.*

  MANGLENDE TEST-STRAEGI

- Strategien er klar; det kreves mer testing for med rimelig sikkerhet å kunne verifisere at f.ex . en rutine fungerer etter forutsetningene. Det er prinsippet/strategien vi arbeider etter.

KOMPETANSETILGANG

- EIRs fagområde er kontroll og styring. Min vurdering er at kompetansen er tilfredsstillende hva gjelder kontroll og styring. Enhetens budsjettsituasjon har vært, og i den nærmeste tiden vil være slik at det er rom for å kjøpe inn ekstern kompetanse. Dette blir, og vil bli vurdert også i framtiden.
- Det er korrekt at det ikke foreligger en systematisk kompetanseplan for enheten. Men som leder for enheten har jeg god oversikt over de tre faste medarbeidernes planer og ønsker. «Kompetanse» er alltid tema i medarbeidersamtalene.
- Når vi har ledige stillinger, vurderer vi først om stillingen skal videreføres og vi har dialog med universitetsdirektøren om det. Det har i min tid som revisjonssjef ikke forekommet at en stilling ikke har blitt godkjent videreført. Dernest diskuterer vi internt hvilken kompetanse/hvilke egenskaper vi trenger før vi kunngjør stillingen.

Tiltak: *Til nå har jeg ikke sett behovet for en formalisert kompetanseplan, men vil heretter utarbeide det. Dessuten kommer jeg fortsatt til å være velvillig innstilt overfor ethvert ønske om kurs et dersom det kan bidra til å styrke enheten.*

KVALITETSSIKRING

- EIR har et eget kvalitetssikringsprogram, det er utviklet innen vårt nordiske netteverk. Det er korrekt og beklagelig at det ikke har blitt benyttet som det burde. Årsaken er at i en så liten revisjonsenhet som EIR, er revisjonssjefen involvert i større eller mindre grad i alle revisjoner. Og som en konsekvens av at jeg har dyktige medarbeidere med høy integritet og stor ansvarsbevissthet har ikke kvalitetssikringsprogrammet blitt benyttet som det burde; hvilket jeg beklager.
- Revisjonssjefen kvalitetsikrer og medsignerer alle revisjonsrapporter.

Tiltak: *Kvalitetssikringsprogrammet vil bli tatt i bruk umiddelbart.*

- Et ledd i kvalitetssikringen er ellers dette: EIR har to samlinger/seminarer pr. år. Som regel like før sommerferien og like før eller like etter jul. Hensikten er å diskutere hva som har gått bra og dårlig siste halvår, og å konkretisere planer og å tildele oppgaver for de kommende månedene.
- Dessuten har vi alltid en seanse der vi vurderer oss selv opp mot instruksen, og mot det internt utviklede dokumentet «Visjon og verdier». Se referat fra samlingene.

Som nevnt innledningsvis , tror vi at vi gjennom, en samvittighetsfull oppfølging av rapporten, vil oppnå forbedringer.

Oslo, 15. november 2013
S.Svanberg
Avd.dir/revsj.EIR