UiO : Universitetet i Oslo

Til **Universitetsstyret**
Fra **Enhet for internrevisjon**

Sakstype: ORIENTERINGSSAK
Møtesaksnr.: O-sak 2
Møtenr.: 4/2013
Møtedato: 17. juni 2013
Notatdato: 5. juni 2013
Arkivsaksnr.:
Saksbehandler: S.Svanberg

EIR – ÅRSRAPPORT 2012 – ÅRSPLAN 2013

Rapport fra EIR for 2012 påpker at:

- Det er økt forståelse for nytten av, og hensiktsmessigheten med risikostyring som et hjelpemiddel for å nå mål
- Der er større bevissthet mht hva som må til for å etterleve lover og regler
- Det er stor bevissthet mht å sikre eiendeler og andre aktiva
- IHR-prosessen har sitt utspring i ønsket om en mer økonomisk og rasjonell drift
- Det er besluttet at mål og formål med IHR-prosessen skal følges grundig

EIR ser det som en oppgave ikke bare å påpeke feil og mangler, men også alltid å anbefale forslag som kan gi forbedringer. Dialogen er god, men det tar ofte for lang tid å få på plass endringer.

ÅRSPLANEN for 2013 inneholder noen områder som er overført fra forrige årsplan. Ellers er det lagt vekt på å utarbeide en plan som støtter opp om ledelsens pioriteringer. Oppfølging av IHR-implemengteringen, Oppfølgingen av straategiplan 2010 – 2020, og oppfølging av styrevedtak er eksempler på det.

Sveinung Svanberg
revisjonssjef

ENHET FOR INTERN REVISJON

ÅRSRAPPORT 2012

OSLO, 9. april 2013

Sveinung Svanberg

Revisjonssjef

INNLEDNING

«Det nye Økonomireglementet for Staten» ble gjort gjeldende fra desember 2003. I dag; nesten ti år senere, henvises det fortsatt til «Det nye» når man henviser til Økonomireglementet. Noe av det som var nytt, var kravet om Risikostyring: «Styring, oppfølging og kontroll må tilpasses virksomhetens egenart samt risiko og vesentlighet», heter det i §4 Grunnleggende styringsprinsipper.

Formålet med Økonomireglementet var å oppnå en mer effektiv styring med bruken av statlige midler, samt å legge grunnlag for en bedre mål- og resultatoppnåelse.
Når det stadig refereres til «det nye..» så har det sammenheng med at risikostyring fremdeles er noe fremmed for mange statsetater. Det er et stykke vei igjen å gå før man er der man bør være. Men det er gjort mye godt arbeid og vårt inntrykk er at UiO har kommet lenger enn de fleste innen vår sektor. Vi ble også oppmuntret av dialogen med fagdirektører og dekaner i forbindelse med oppfølgingen av tidligere risikovurderinger på forvaltningsområdet; jfr punkt 1.6 Oppfølging risikovurdering forvaltningsområdet.

EIR har som sin hovedoppgave å se etter om UiO lever opp til Økonomieglementets forventninger. EIR skal vurdere om risikostyringen, internkontroll- og styringssystemene er forsvarlige og fungerer som forutsatt. Dette innebærer at Enhet for intern revisjon skal se etter hvorvidt:

- den økonomiske og operative informasjon er pålitelig og nøyaktig
- policy, planer, retningslinjer lover og forskrifter etterleves
- aktiva/eiendeler er forsvarlig sikret bruken av ressurser er økonomisk og rasjonell
- etablerte formål og målsetninger for driften eller prosjekter oppfylles

Kort sagt innebærer det at EIR skal se etter om man har tilfredstillende kontroll og styring på de områdene vi reviderer, og gi en klar og entydig konklusjon.

For UiO totalt er dette en krevende oppgave, fordi det ikke er mulig for EIR å dekke alle områder og funksjoner i løpet av et år.

Men vi har gjennom det revisjonsarbeidet som ble utført i 2012 kunnet konstatere at:

- Det er økt forståelse for nytten av, og hensiktsmessigheten med risikostyring som et hjelpemiddel for å nå mål
- Der er større bevissthet mht hva som må til for å etterleve lover og regler
- Det er stor bevissthet mht å sikre eiendeler og andre aktiva
- IHR-prosessen har sitt utspring i ønsket om en mer økonomisk og rasjonell drift
- Det er besluttet at mål og formål med IHR-prosessen skal følges grundig

KONKLUSJON pr 31.12.2012

God styring og kontroll skal bidra til at UiO når sine overordnede mål; slik de kommer til uttrykk i SP 2010 – 2020. Dette kommer ikke tydelig fram i alle sammenhenger. Derfor vil det være viktig å rette økt oppmerksomhet mot det å skape forståelse for de styringsprinsippene Økonomireglementet legger opp til. EIR har gjennom vårt revisjons- og rådgivingsarbeid i 2012 kunnet konstatere at UiO er inne i en god utvikling hva gjelder risikohåndtering, økt fokus på fornuftig ressursbruk, måloppnåelse og resultatmåling.

OPPFØLGING AV ÅRSPLAN 2012

Revisjonsplanen for 2012 ble lagt fram for universtetsstyret til orientering, og ble i matriseform presentert slik:

REVISJONSMATRISE FOR EIR 2012

Nr	Område	1 kv	2 kv	3 kv*	4 kv*	
1	Informasjonssikkerhet mobile enheter	X	X			gjernnomført
2	Eksternt finansierte prosjekter - økonomistyring					På vent– arb.gr. IHR
3	Internkontroll i grensesnittet EFP/innkjøp/sidegjm.		X	X		Delvis fulgt opp
4	Midlertidig ansatte					På vent
5	UiOs miljøsatsing – grønt universitet			X	X	Trukket tilbake
6	Strategisk plan 2020 implementering/oppfølging			X	X	Overført 2013
7	SBH-rutiner med hovedvekt på arkivering	X	X			gjennomført
8	Imlementering av helseforskningsloven				X	gjennomført
9	Doble utbetalinger	X				Gjennomført
10	Forskningsbasert utdaning					PÅ VENT
11	Varierte undervisnings- og evalueringsformer					PÅ VENT
12	Tilgangsstyring it-området		X	X		Gjenomført 2013
13	Formidling					PÅ VENT
14	Vortex	X				Des 2011 – feb 2012
15	Oppfølging ririko foraltningsområdet			X	X	

I tillegg kommer EU-revisjoner, Rådgivingsoppgaver (spesielt fasilitering av risikovurderinger).
1 10 og 11 kan slåes sammen, områdene vurderes også i forhold til at NOKUT har signalisert stedlig tilsyn i 2013.
***Det foretas en ny vurdering før sommeren av oppgavene ført opp i 2. halvår – og da vurdert opp mot oppgaver "på vent".**

Revisjonsområdene var noe mer detaljert beskrevet i et eget vedlegg til planen.

Avvik/endringer i årsplanen blir alltid diskutert med universitetsdirektøren. De områdene som står "på vent", ble ikke tatt opp i planen. Når det gjelder område 3 **Eksternt finansierte prosjekter – økonomistyring** så ble dette tatt inn som et nytt element i oppfølgingen av tidligere gjennomførte risikvurderinger av Forvaltningsområdet. Område 5 - **UiO Miljøsatsing – grønt universitet,** ble etter initiativ fra prosjektet, som i utgangspunktet ba om en revisjonsgjennomgang besluttet utsatt, men er nå heller ikke med på planen for 2013.

Område 6 **Strategisk plan - 2020 implementering/oppfølging**, er overført til planen for 2013.

I stedet for de områdene som ikke ble revidert i hht planen ble EIR anmodet om å foreta en ny oppfølging av tidligere års risikovurderinger på "forvaltningsområdet" og da med hovedfokus på å sikre at UiO etterlever lover og retningslinjer. Gjennomgangen omfattet samtlige fakulteter og begge muséene (NHM og KHM). I tillegg ble det gjort en egen revisjon som omfattet samtlige institutter ved Det naturvitenskapelig fakultet..

REVISJONER/OPPGAVER 2012

1.2 Publiseringsverktøyet Vortex - en risikovurdering

Vortex er et egenutviklet produkt i, og av USIT. EIRs arbeid ble igangsatt som et ad hoc oppdrag i desember 2011, og ble avsluttet i februar 2012.

Formålet *med arbeidet var:*

Å risikovurdere Vortex som publiseringsløsning for UiO-web. Vortex har også andre funksjoner og leverer løsninger til andre nettsider enn UiO-web. Denne revisjonen avgrenses til å vurdere Vortex sin, brukervennlighet, funksjonalitet, ytelse og stabilitet, og sikkerhet for UiO-web på kort og lang sikt.

Resultatet av arbeidet ble tatt inn i årsrapporten for 2011. EIRs vurdering var at "miljøet er lite og sårbart og det knytter seg usikkerhet til om man på lengere sikt klarer å hevde seg i konkurransen med andre løsninger."

Strengths **S**	**Weaknesses** **W**
• Brukervennlig ved enkel publisering • Stabilt og tydelig driftsmønster • Blitt bedre over tid • UiO styrer retningen på utvikling av løsningen • Dedikerte tekniske ansatte med god kompetanse • Feil kan bli (og blir) korrigert raskt • Kostnaden for utvikling går til oss selv • Tilpasset universell utforming	• Strategi og langsiktig plan mangler • Tatt i bruk uten en reell vurdering • Alene i verden om å bruke det • Uklare ansvarsforhold • Avhengig av en håndfull personer • Vanskelig rekruttering • Liten fleksibilitet i kapasitet • Mangler i funksjonalitet (ikke utviklet så langt) • Mindre sannsynlig at sikkerhetshull blir oppdaget grunnet få brukere
Opportunities **O**	**Threats** **T**
• UiO kan påvirke utviklingen av løsningen i ønsket retning	• Manglende strategiske beslutninger rundt publiseringsløsning og organisering • Ikke troverdig at utviklingen kan være bedre enn andre løsninger som utvikles av mange • Bortfall av personalressurser • Ukjent økonomisk bilde

Konklusjon
I denne risiko-vurderingen har vi erfart at det ikke foreligger et klart, entydig og kjent formål for UiO's publiseringsløsning. Det er av stor betydning at det kommer på plass slik at best mulige veivalg for løsningen kan gjøres.
Dagens løsning er egenutviklet, og Vortex-miljøet i USIT har gjennom sin kompetanse og sitt store engasjement skapt en god fungerende løsning. Men miljøet er lite og sårbart og det knytter seg usikkerhet til om man på lengre sikt klarer å hevde seg i konkurransen med andre løsninger.

STATUS: Universitetsdirektøren ba USIT sette opp en matrise som inneholdt EIR sine anbefalinger, og rapportere framdriften i arbeidet

1.3 Doble utbetalinger

UiO mottar årlig mer enn 100.000 inngående fakturaer – inkl. alle betalingsoppdrag fra over 10.000 leverandører. I 2011 ble det registrert 107.436 utførte betalingsoppdrag. Dette tallet omfatter også fakturaer som av forskjellige grunner har blitt registrert flere ganger. Det vil alltid være en risiko for at fakturaer kan bli registrert mer enn en gang og bli betalt dobbelt.

FORMÅLET med revisjonen var å se etter at fakturaer ikke blir betalt flere ganger, og at UiO har gode kontrollrutiner for å hindre at dette skjer.

Avgrensing - framgangsmåte
Revisjonen ble avgrenset til rutinene for fakturamottak, scanning og betaling.

Rutinene ble gjennomgått i flere intervjurunder med ledere for to av seksjonene ved Regnskapsseksjonen (RS), og i møter med andre ansatte. Det ble deretter gjennomført en omfattende test på omtrent halvparten av alle inngående fakturaer i 2011. Utvalgskriterier var fakturanummer, leverandørinformasjon, fakturadato og beløp.
I løpet av revisjonen ble vi kjent med at Riksrevisjonen hadde gjennomført en bilagskontroll ved UiO. Riksrevisjonen konstaterte at: "En kontroll av enkelte poster i hovedboken viser at universitetet har betalt samme faktura to ganger til forskjellige leverandører" .

Hovedfunn
Fakturaer registrert på feil leverandør har vært den hyppigste årsaken til feil- og dobbelutbetalinger. RS har jobbet med å fremskaffe en oversikt over fakturaer som er registrert på feil leverandør. Totalt viser oversikten 4,5 MNOK, men en del av EIR sine funn var ikke med. Vi har derfor grunn til å tro at oversikten ikke er komplett.
Typiske funn var:

- Dobbeltregistrering av samme faktura på samme leverandør.
- Dobbeltregistrering av samme faktura på samme leverandør, men til forskjellige divisjoner/avdelinger innenfor selskapet.
- Dobbeltregistrering av samme faktura, en gang på feil leverandør og andre gang på riktig leverandør.
- En stor kreditnota var registrert som faktura (168.478 NOK).
- 2 forskjellige fakturaer fra en leverandør, med 2 forskjellige ordrenummer inneholdt samme timeliste for samme person (46.894 NOK).
- Samme faktura registrert 2 ganger. Fakturabeløp =0, men fakturaen registrert med beløp (30.370 SEK)
- Fakturaer registrert med feil valuta.

KONKLUSJON
Revisjonen viser at det er et betydelig antall fakturaer som er registrert feil og/eller dobbelt, og at UiO ikke har hatt god nok kontroll på rutinene sine i 2011. Vår gjennomgang viser at den størst svakheten i 2011 har ligget i den manuelle verifiseringen av fakturaer, og som skal luke bort feil ved den elektroniske registreringen.

Risikoen for at en faktura som kun er registrert én gang skal bli dobbelt utbetalt anser vi som liten. På dette området vurderer vi rutinene som tilfredsstillende.

Noen av funnene våre var allerede oppdaget av RS og lå i en oversikt de selv har laget over feilutbetalinger. Vi har grunn til å tro at listen ikke er komplett i forhold til å dekke alle varianter av feil- og dobbeltutbetalinger, men RS jobber systematisk videre for å avdekke

mest mulig. Tapet for UiO ligger både i for mye utbetalte beløp og i ressursene som kreves for å rette opp feil.

STATUS: EIR har mottatt et tilfredsstillende svar på revisjonen, og det er holdt et møte med RS som dokumenterte at man har grepet fatt i problemene på en god måte.

1.4 Arkiv - SAKSBEHANDLING

Universitetet i Oslo gikk for 4 år siden over fra fysisk til elektronisk arkivering, noe som har ført til at flere arkivoppgaver har en flytende overgang til saksbehandling. Selve arkiveringen har endret seg fra å bli utført av arkivmedarbeidere, til å bli utført av andre ansatte; i første rekke saksbehandlere. Det er i den forbindelse blitt stilt spørsmål om vi har god nok kontroll på arkivet til UiO.

I henhold til Forskrift om offentlige arkiver av 11.desember 1998 §2-2, er alle offentlige organ pålagt å ha en arkivplan. Arkivplanen ved UiO dokumenterer arkivorganisasjonen, oppbyggingen av arkivet og den gir regler for hvordan dette skal forvaltes. Personer som forvalter arkivet skal arbeide etter følgende målsetting:

- Arkivet skal være en oppdatert og tilgjengelig informasjonsbase for saksbehandling og offentlig innsyn.
- Arkivet skal være godt registrert og sikkert lagret. Arbeidsrutiner, arkivsystem og informasjonsbærere skal være mål for kvalitetssikring.
- Arkivet skal på en trygg måte ivareta rettslig og historisk dokumentasjon for ettertiden.

FORMÅLET med revisjonen ble beskrevet slik:
å vurdere om det interne kontrollsystemet som er etablert, er tilstrekkelig og hensiktsmessig, og om det gir en rimelig sikkerhet for at ARKIVFUNKSJONEN ved UiO når sine målsettinger. Organisering, roller, ansvar og myndighet er sentrale elementer også i den sammenheng.

Revisjonen ble gjennomført med intervjurunder hos OPA, e-Sak og arkivledere. I tillegg laget vi en spørreundersøkelse som ble sendt ut til 492 saksbehandlere, hvorav 47 % svarte. Dette er en svarprosent vi er godt fornøyd med.

KONKLUSJON:
ePhorte har ikke blitt det tjenlige verktøy for hele UiO som man hadde håpet på da systemet ble tatt i bruk. Hovedårsaken til det er at brukerterskelen er høy, og at systemet er lite intuitivt. Dermed blir en del dokumenter lagret/arkivert i andre systemer, og i noen tilfeller lagret fysisk hos den enkelte medarbeider. Dette medfører risiko for at saker kommer på avveie, og/eller at de ikke blir gjennfunnet når det er behov. F.eks. når det kreves innsyn i saksbehandlingen.

Arkivpersonalet er imidlertid fornøyd med at det er enkelt å finne saker som ER lagt inn i systemet, og det er ikke konstatert at REGISTRERTE saker har kommet på avveie.

Når det gjelder organiseringen av arkivledelsen og arkivfunksjonen ved UiO, er det ikke sammenheng mellom ansvar og myndighet. En følge av dette er at eSaks rolle oppfattes som uklar av mange arkivmedarbeidere, og at møter i felles fora ikke blir så effektive og klargjørende som de burde være.
Misforholdet mellom ansvar og myndighet står i sterk kontrast til målsettingen med IHR-prosjektet.

Vi regner med at problemet vil bli adressert og løst i prosjektet.

1.5 Sikkerhet mobile enheter

Formålet med revisjonen var «å se etter om informasjonssikkerheten er tilstrekkelig ivaretatt ved bruk av mobile enheter ved UiO». Mobile enheter er definert som: Bærbar PC, smarttelefon, mobiltelefon, nettbrett og minnepinner.

Et viktig utviklingstrekk er det som navnes BYOD – Bring Your Own Device, som medfører at arbeidstakere vil benytte privat utstyr som en del av jobbutførelsen. Et annet er skytjenester.

Vurderinger
Utviklingen med økt bruk av mobile enheter gir nye utfordringer og nye risikoeksponeringer. Særlig bruk av private enheter setter informasjonssikkerheten under press. Et særtrekk er at informasjonen som blir behandlet ikke har en entydig systemeier og dermed ikke er underlagt et tydelig forvaltningsregime (herunder ansvar for kompetansetiltak for brukere).

Det er utarbeidet en prosedyre til IT-sikkerhetshåndboka (prosedyre 7.1) som beskriver klassifisering av informasjon i 3 klasser, UiO-åpen, UiO-begrenset og UiO-konfidensiell. All informasjon som behandles ved UiO skal klassifiseres, og det skal foreligge rutiner og prosedyrer for behandling og sikring av de ulike klassene av informasjon.
Denne prosedyren er imidlertid ikke implementert i organisasjonen.

Disse to forholdene, at informasjonen ikke er underlagt et tydelig forvaltningsregime og at prosedyre for klassifisering av informasjon ikke er implementert, medfører at det er vanskelig å sikre tilstrekkelig informasjonssikkerhet.

Den enkelte bruker har et ansvar for å holde sin mobile enhet tilfredsstillende oppdatert og med tilstrekkelig sikkerhetsprogramvare. Selv om det er den enkeltes ansvar trengs det mer støtte for å sikre tilfredsstillende informasjonssikkerhet.

Det er ikke laget en samlet risikoanalyse av området, men flere risikoer ble nevnt i de samtaler som ble gjennomført. En samlet risikoanalyse må lages, den må dokumenteres og fornyes med jevne mellomrom, og den må inneholde tiltak for å redusere risikoene

Konklusjon
Informasjonssikkerheten er **ikke tilfredsstillende** ivaretatt ved bruk av mobile enheter ved UiO.

EIR peker 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.

EIR mener de tiltak som er beskrevet i høringsnotat om IT-virksomheten angir en god retning, men at de påpekte forholdene i denne rapporten tas med i det videre arbeidet med notatet.**bakemelding fra USIT**

USIT ga tilbakemelding på revisjonsrapporten tidlig i januar 2013. De er enige i konklusjonene som rapporten har. Tiltak vil bli iverksatt i løpet av 2013.

USIT hadde i tillegg noen kommentarer med overskriftene;

- Tekniske tiltak løser kun en liten del av problemet
- Elektronisk post som spesiell utfordring
- Standardisering
    - Ref vedtak i styret fra 22.oktober 2012 om «Organisering og standardisering av universitetets IT-virksomhet
    - Gode innkjøpsavtaler, og lojalitet til disse
- Driftsløsninger for mobile enheter
- Klassifisering av informasjon
    - For å få innført og informert om nye regler og rutiner vil også Kommunikasjonsavdelingen og Organisasjons- og personalavdelingen bli involvert
- Kompetanseheving
- Risikovurdering

EIR er fornøyd med mottatt tilbakemelding fra USIT, og vil følge opp framdrift på tiltak per 1.halvår 2013

1.6 Oppfølging risikovurdering forvaltningsområdet

I 2008 ble det i regi av Ernst&Young gjennomført en risikoanalyse av forvaltningsområdet.

I 2010 fikk EIR i oppdrag av universitetsdirektøren å følge opp den delen av risikogjennomgangen som gjaldt overholdelse av lover og regler (orienteringssak i styremøte 7/2010).
Konkusjonen var at risikobildet hadde endret seg til det bedre på de fleste områdene.

EIR ble anmodet om å foreta en ny oppfølging i 2012, og arbeidet ble utført i oktober og november.

Mens risikovurderingene i de foregående år hadde involvert kun fagavdelingene i SA, ble det i 2012 gjort en endring ved at også alle åtte fakulteter og Naturhistorisk museum og Kulturhistorisk museum ble involvert arbeidet. Hensikten var å få en noe bredere vurdering, samt å se om det var forskjeller mellom de vurderingene som ble gjort i sentral-administrasjonen og ute i organisasjonen.

Ved samtlige fakulteter hadde vi samtaler med dekan og/eller fakultetsdirektør. Ved museene hadde vi samtaler med underdirektørene.

Det ble som en del av oppfølgingen også gjennomført samtaler med instituttnivået på MatNat-fakultetet, for å se om risikobildet var annerledes fra det ståstedet.

KONKLUSJON
Den entydige oppfatningen er at risikoen på de tolv forskjellige områdene som er vurdert er redusert eller at den er uforandret i forhold til hva den var i 2010

Vi har ikke kunnet registrere noen forskjell mellom svarene fra fakultetene og fra fagavdelingene i SA (inklusive USIT og Teknisk Avdeling).

Kun ved to enheter påpekte man lokale forhold som medførte økt sannsynlighet for at man ikke ville være i stand til å etterleve lover og regler. Og i begge tilfellene dreide det seg om midlertidige forhold som skyldtes ombyggings-/rehabiliteringsarbeider som skapte vanskelige arbeidsforhold for personalet.

Det var ikke klare forskjeller i hvordan risikobildet ble vurdert av hhv fakultet/fagavdeling og instituttene ved MatNat-fakultetet. Se for øvrig kort oppsummering av risikogjennomgangen ved instituttene ved MatNat i nste punkt (1.7)

Generelle betraktninger - videre oppfølging av risiko på forvaltningsområdet
Som nevnt var "panelet" denne gangen utvidet fra å omfatte fagdirektører til også å involvere de åtte fakultetene og de to muséene.
Samtalene fikk også et annet innhold denne gangen, man var i større grad enn tidligere opptatt av å diskutere relevansen ved de valgte risikoområdene, presisjonen i risikoformuleringene (eller mangelen på presisjon)

Vi fikk et klar oppfatning av at bevistheten og kompetansen på risikoområdet har fått et løft siden EIR gjorde sin forrige oppfølging.

1. Det ble stilt kritiske spørsmål til om man risikovurderer de riktige (eller viktigste) områdene.
2. Det ble påpekt at risikoformuleringene var lite presise.
3. Det ble stilt spørsmål til resultatene av de tidligere vurderingene, fordi konsekvensene neppe er så høye som risikobildene viser. Det innebar at mange vurderte det nivået som ble satt for konsekvens i 2008 som altfor høyt.
4. Tidligere vurderinger har ikke vært nok bevisst på hvordan økt sannsynlighet påvirker konsekvensen.
5. Man har hatt forslag til andre områder som bør risikovurderes i tillegg til, eller istedenfor eksisterende områder.
6. EIR har fått innspill til områder som kan være med på revisjonsplanen for 2013.

Ad 1) Områdene har vært de samme helt siden Ernst & Young ledet prosessen i 2008. Dette for å kunne se utviklingen over tid. Formuleringene fra 20098 er beholdt av samme grunn.
EIR anbefaler at man i neste omgang gjør en generell risikovurdering av hele forvaltningsområdet; og ikke bare mot den delen som gjelder overholdelse av lover og regler.

1.7 Risikovurdering ved Matematisk-naturvitenskapelige fakultet

EIR gjennomførte intervjuer med ledelsen ved alle institutter (9) og 2 sentre ved fakultetet, for å få en vurdering av risikotilstanden på instituttnivå.

Et risikoområde ble av alle pekt ut til å ha høy risiko, EFP (eksternt finansierte prosjekter). Risikoeksponeringen ble begrunnet med at økonomistyring var svært vanskelig på instituttnivå. BOA (Bidrags- og oppdragsfinansiert aktivitet) har endret situasjonen til det verre. Det er ikke adekvat støtte fra økonomisystemene, og enheten vet ikke eksakt økonomisk status i et prosjekt. Det brukes store ressurser lokalt for å holde noenlunde økonomisk kontroll.

Krevende samarbeid med Teknisk avdeling ble også pekt på som en risiko.

De andre områdene ble vurdert til å ha lav til moderat risiko.

1.8 Varslinger

I 2012 mottok EIR kun to meldinger fra fakultetene om varslinger, og vi mottok én varsling direkte.

At det kun har vært to varslinger ved UiO (utenom EIR) anser vi for å være usannsynlig, og der kan tyde på at denne delen av varslingsregimet ikke fungerer som det skal.

EIR har derfor anmodet OPA om å innskjerpe reglene slik at EIR kan ivareta sin oppgave med å følge opp varslingsbehandlingen.

Et nytt system vil fra 2.halvår 2013 sikre at EIR blir bedre informert om mottatte varsler, både fra studenter og fra ansatte.

1.9 REVISJON IMPLEMENTERING KVALITETSSYSTEM HELSEFORSKNING

Ny lov om medisinsk og helsefaglig forskning (helseforskningsloven, heretter forkortet HFL) trådte i kraft 1. juli 2009. Forskningsadministrativ avdeling har utarbeidet et kvalitetssystem med rutiner for hvordan roller, oppgaver og ansvar skal ivaretas ved UiO slik at lovens krav blir fulgt. Kvalitetssystemet for medisinsk og helsefaglig forskning (heretter omtalt som «kvalitetssystemet») ble gjort gjeldende 1.7.2012.

Formålet med revisjonen er å se etter at kvalitetssystemet ved UiO er tilfredsstillende implementert, og at det er hensiktsmessig i forhold til målsettingen om at UiO skal etterleve HFL.
Revisjonen avgrenser seg til fakultetene, dvs. at museer, sentre og tverrfakultært satsningsområde som også har fått delegert oppgaver ihht. HFL ikke har vært gjenstand for revisjon. I tillegg er revisjonen avgrenset til rutiner og prosesser i forbindelse med etterlevelse av kvalitetssystemet og HFL, og ikke en kontroll for alle elementer som må være oppfylt i de forskjellige prosjektene.

Revisjonen er basert på samtaler strukturert etter elementene i kvalitetssystemet. Vi har snakket med samtlige fakultetsledelser og flere instituttledere. I tillegg har vi hatt samtaler med 24 prosjektledere på til sammen åtte aktuelle institutter.

ROLLER – ANSVAR - OPPGAVER
Konklusjon:
Roller og ansvar i kvalitetssystemet er formalisert og forstått, men hva oppgaven går ut på, blant annet å sikre at prosjektledere er satt in stand til å bruke kvalitetssystemet, er ikke utført. Tidligere IS-direktør sin rolle er ikke formelt ivaretatt eller videreført. Det er i dette avsnittet pekt på forhold og oppgaver hvor ansvaret bør ligge sentralt.

Anbefaling:
- Oppgavene til IS-direktør bør delegeres formelt og gjøres kjent i organisasjonen.
- Et felles IT-system som støtter kvalitetssystemet, bør implementeres.
- Kartlegge behovet for opplæring og støttefunksjon.
- Tilstrekkelig finansiering for fremdrift av forskningsserveren TSD 2.0.

LØPENDE OVERSIKT OVER HELSEFORSKNINGSPROSJEKTER OG BIOBANKER
Konklusjon:
Uten et felles system for registrering av prosjekter, vil det være tidkrevende å ha en løpende oversikt slik HFL krever. Også her er det risiko for at ressursbruken ikke er effektiv, ved at enhetene hver for seg utvikler egne løsninger. Ved tilsyn fra henholdsvis

Helsetilsynet eller Datatilsynet vil UiO ikke kunne fremskaffe en samlet løpende oversikt over egne prosjekter som faller inn under HLF

Anbefaling:

- EIR anbefaler at UiO søker å få på plass et felles system for å håndtere løpende oversikt over prosjekter og biobanker

INFORMASJONSSIKKERHET PÅ PROSJEKTNIVÅ

Konklusjon:

Revisjonen viser at kravene fra kvalitetssystemet i stor grad blir fulgt. Det er likevel uheldig at det er opp til hver enkelt medarbeider hvor bevisst man er på sikker lagring i praksis.

Anbefaling:

- All data fra helseforskning legges over på felles forskningsserver når denne er klar.

INTERNKONTROLL PÅ PROSJEKTNIVÅ

Konklusjon:

De formelle kontrollmekanismene som skal ivareta den interne kontrollen for et prosjekt er ikke gode nok. Likevel ser vi at uformell sparring mellom kollegaer, sammen med visse rutiner er positivt for kontrollmiljøet.

Anbefaling:

- Rutinene i kvalitetssystemet er tilfredsstillende med tanke på å sikre god internkontroll i prosjektene. Instituttledere må følge opp at disse er implementert og etterlevd.

KVALITETSSYSTEMETS HENSIKTSMESSIGHET

Konklusjon:

Ved bruk av kvalitetssystemet vil HFLs krav ivaretas og internkontrollen i prosjektene bli bedre. For å sikre bruken, øke mulighetene for å oppdage avvik, samt effektivisere hverdagen for prosjektleder og instituttleder, mener vi et tilhørende felles IT-system er en nødvendighet.

Anbefaling:

- Vi viser til tidligere punkt vedrørende felles IT-system.
- Engelsk versjon av kvalitetssystemet bør utarbeides sentralt. Enhetene må få beskjed når dette vil skje, slik at dobbeltarbeid unngås.

HOVEDKONKLUSJON

Kvalitetssystemet for medisinsk og helsefaglig forskning er et godt verktøy for prosjektledere, men det er i liten grad kjent. Det er heller ingen tidligere formelle strukturer som ivaretar en interkontrollfunksjon på dette området.

For at kvalitetssystemet også skal bli et godt verktøy for UiO som institusjon, må en felles IT infrastruktur på plass, og god opplæring må tilbys. Videre er det et savn at UiO p.t. ikke har en felles forskningsserver, samt at kvalitetssystemet ikke foreligger på engelsk. Disse forholdene skaper en betydelig frustrasjon ute i organisasjonen.

Bedre tilrettelegging fra sentralt hold må til for at fakultetene på en kostnadseffektiv måte skal kunne utføre det ansvaret som er gitt gjennom kvalitetssystemet.

1.10 Personvernombud

EIR ivaretar funksjonen som personvernombud (PVO) for administrative behandlinger ved UiO, estimert til ca ¼ stilling. Den ivaretas av 1 medarbeider, godkjent av Datatilsynet.

Opplegg med stedlige kontroller av behandling av personopplysninger har fortsatt i 2012. De stedlige kontrollene gjennomføres i et samarbeid mellom PVO og daglig behandlingsansvarlig, som et team. Det er gunstig å være flere til å ivareta gjennomføringene, og samarbeidet med daglig behandlingsansvarlig er svært godt. Imidlertid har framdriften vært redusert i 2012 pga en del fravær hos daglig behandlingsansvarlig.

Effektene av stedlige kontroller er at bevissthet og kompetanse hos besøkt enhet øker. Samtidig er teamet svært fornøyd med tilstanden ved de besøkte enheter, og også den vilje som vises for å bedre på 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.

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. De stedlige kontrollene er i stor grad med på å sikre at registeret inneholder alle aktuelle behandlinger og at det er á jour.

Personvernombudet har i tillegg blitt rådspurt i flere konkrete saker gjennom året.

1.11 EU-revisjoner

EIR reviderte 17 EU prosjekter i 2012, en nedgang fra 22 i 2011. Det er flest prosjekter fra 7.rammeprogram, og ingen fra 6.rammeprogram etter sommeren 2012.
Vi regner med at antall revisjoner vil fortsette å falle i 2013.
Vi konstaterer at kompetansen på innrapporteringen er varierende, men i hovedsak tilfredsstillende.

Andre oppgaver

I innstruksen som ligger til grunn for enhetens arbeid, er det slått fast EIR skal ha en kontrollerende, informerende og rådgivende funksjon.

Universitetsledelsen har signalisert at den rådgivende funksjonen skal gis god plass, og vi opplever i stadig økende grad å bli rådspurt i spørsmål som dreier seg om kontroll og styring.

Varslingssystemet

I Årsrapporten for 2011 skrev vi at: «EIR mottok kun to meldinger fra fakultetene om varslinger, og vi mottok én varsling direkte.
At det kun har vært to varslinger ved UiO (utenom EIR) anser vi for å være usannsynlig, og der kan tyde på at denne delen av varslingsregimet ikke fungerer som det skal.»

Det var heller ingen økning i 2012, og hele Varslingsregimet vil bli lagt om høsten 2013. En av sakene fra 2012 har imidlertid vært svært ressurskrevende. Den var av en slik art at EIR har arbeidet med den selv.

Administrative forhold

Èn medarbeider har hatt foreldrepermisjon siden 1. august, men stillingen har vært dekket opp ved vikar.

Sykefraværet er tilbake på normalt (lavt) nivå.

Kompetansen ved enheten vurderes som tilfredsstillende.

Universitetet i Oslo

ENHET FOR INTERN REVISJON

ÅRSPLAN FOR 2013

OSLO, 28.02.2013

Sveinung Svanberg

Revisjonssjef

1. INNLEDNING

Revisjonsplanen for 2013 er et produkt av innspill og signaler EIR har mottatt gjennom det siste året. I forbindelse med en oppfølging av en tidligere risikoanalyse, hadde EIR møte med ledelsen ved samtlige fakulteter, begge muséene og de fleste fagavdelingene i SA. En del av møteopplegget var at enhetene ble anmodet om å komme med forslag til revisjonsområder for 2013, og fikk gode forslag gjennom de møtene. I tillegg bygger planen på enhetens egne vurderinger av risiko og vesentlighet, og den har vært gjenstand for diskusjoner med universitetsdirektør og assisterende universitetsdirektør.

Den tar også opp i seg viktige styringssignaler som er gitt fra Kunnskapsdepartementet, spesielt hva gjelder styringsprinsipper - herunder risikohåndtering.

Videre er det en målsetting med planen at den skal reflektere de utfordringene som preger UiOs strategiplan.

2. STRATEGIER/ARBEIDSMÅL

I Intern revisjons Mål og strategidokument er enhetens mål formulert slik:
Intern Revisjon skal bidra til målbare kvalitetsforbedringer i rutiner, systemer og den administrative drift slik at universitetets overordnede strategier og mål kan oppfylles på en effektiv og rasjonell måte.

Videre heter det at EIR skal

- ✓ *ha fokus på måloppnåelse ut fra visjon, strategier, verdigrunnlag, kommunikasjonsplattform og ledelseskrav som er fastlagt for UiO*
- ✓ *gi bidrag/råd i utviklingsprosjekter for å skape forbedringer*
- ✓ *øke forståelsen for betydningen av helhetlig og integrert risikostyring i organisasjonen*[1]

Intern revisjons arbeid tar utgangspunkt i vurderinger av risiko og vesentlighet. Risiko kan defineres som *"en samling av alle interne og eksterne faktorer som påvirker vår evne til å nå mål eller å oppfylle formålet. Risiko oppstår like mye ut fra faren for at noe fordelaktig ikke vil skje (tapte muligheter), som trusselen for at noe galt vil inntreffe, eller avvik fra forventet resultat."*

UiOs ledelse er pålagt å sørge for at det er etablert en forsvarlig risikostyring og intern kontroll, og påse at den fungerer på en tilfredsstillende måte. Intern Revisjon vil fokusere på dette i sitt arbeid, og det er satt av egne ressurser for å bistå organisasjonen i å etablere intern kontroll i tråd med Økonomireglementets krav til virksomhetsstyring.

---

[1] En av enhetens medarbeidere skal gjennomføre BIs managementprogram «Intern revisjon; Governance - Risikostyring - Intern styring og kontroll», og skal i den forbindelse skrive en prosjektoppgave om helhetlig risikostyring ved UiO.. Medarbeideren og EIR har etablert god kontakt med ØPA slik at oppgaven skal få størst mulig nytteverdi for UiO.

EIR ønsker å bidra til økt kvalitet ved å fokusere på et bevisst forhold til risiko, samt å støtte opp under ønskede endringsprosesser som skal sette organisasjonen enda bedre i stand til å gripe og utnytte nye muligheter.

Gjennom sitt arbeid i store deler av organisasjonen vil Intern Revisjon være i en god posisjon til å spre "best practice" og bidra til intern læring og samhandling mellom fag- og funksjons-områder.

For at vi skal lykkes, er vi avhengig av en god dialog med universitetsledelsen, fakulteter, institutter og de tekniske og administrative enhetene både i planleggingsarbeidet og i gjennomføringen av revisjons-arbeidet.

3. ENHET FOR INTERN REVISJON – BEMANNING - ARBEIDSUTFØRELSE

Enhet for Intern revisjon disponerer fire stillinger, og samtlige stillinger er pr. dato besatt; én med vikar som følge av at en medarbeider har foreldrepermisjon.

EIRs oppgaver er knyttet til utførelsen av operasjonell revisjon. Revisjonsmetodikk velges ut fra det enkelte oppdrags formål og omfang, samt etter tilgjengelige ressurser. I enhetens instruks er det slått fast at "revisjonsarbeidet skal være kontrollerende, informerende og rådgivende". Videre er Intern Revisjon pålagt å *"drive utstrakt veiledningsvirksomhet og yte bistand og gi råd innenfor internrevisjonens saksområder og kompetanse. Enheten skal drive forebyggende virksomhet og sikre at rutiner omkring kontroll av sikringssystemer blir tilfredsstillende fulgt opp i organisasjonen."*

Revisjonene utføres ved bruk av kartleggings-, evaluerings- og testingsverktøy som gir grunnlag for evalueringer og forbedringsforslag. EIR har utarbeidet et nettbasert verktøy for kartlegging, risiko-vurderinger og egenevalueringer. Dette verktøyet vil bli benyttet i en viss utstrekning, men stedlige revisjonsbesøk vil være den viktigste arbeidsmetoden.

Revisjon av EU-prosjekter innebærer en bekreftelse på at kostnadene i prosjektene er i samsvar med kontrakten med EU, og at de er tilfredsstillende dokumentert. Det forventes færre EU-revisjonsoppdrag i 2013 enn foregående år.

Intern revisjons virksomhet blir utført i samsvar med de standarder som er utarbeidet av *The Institute of Internal Auditors (IIA).* EIRs medarbeidere er medlem av Norges Interne Revisorers Forening (IIA's norske organisasjon). En medarbeider er også medlem av ISACA, internasjonal organisasjon spesielt for interne revisorer innen IT.

4. BUDSJETT

Det er viktig at enheten tilføres midler som sikrer faglig utvikling, og som medfører at medarbeiderne kan delta på vedlikeholdsaktiviteter som er nødvendige for å kunne opprettholde sertifiseringer. Den budsjettrammen enheten er tildelt for 2013 legger til rette for det.

Således tas det sikte på aktiv deltagelse i IIAs[2], ISACAs[3] og NIRFs[4] kurs- og seminartilbud. Det avsettes to dager både vår og høst for evaluering av egen virksomhet mot planer, instruks, UiOs "Visjon og verdier", EIRs eget visjons- og verdidokument, samt til planlegging av kommende halvår. Videre ser vi det som verdifullt å delta i nettverksarbeid med internrevisjonsavdelinger ved universitets- og høgskoler i Norden.

5. REVISJONSPLAN 2013

Vi har som **vedlegg** til planen en beskrivelse av de enkelte revisjonsområdene med angivelse av formål og omfang. Omfanget vil bli vurdert og konkretisert når vi starter planleggingen av de enkelte revisjonene. Dette vil skje i samarbeid med de enhetene som skal revideres, og de avdelingene som har et ansvar i forhold til revisjonsområdet.

Aktivitetene dekker hele 2013. Det er ikke reservert tid til ad hoc-oppdrag, men de vil bli utført fortløpende ved at det foretas omprioriteringer i samråd med universitetsdirektøren.

Oppgaven som **personvernombud** for administrative behandlinger tilligger fremdeles en stilling i EIR og beslaglegger ca. 20 % av denne stillingen.

Enhet for intern revisjon er tildelt rollen som **varslings- og rapporteringsinstans** for UiO. Det er ikke mulig å tidfeste ressursbruken til dette arbeidet i 2013. Men dette er et arbeid som MÅ prioriteres.

Følgende hovedområder (1-10) planlegges revidert i 2013. Nummereringen innebærer ingen prioritering, men er henvisninger til beskrivelsen av områdene i vedlegget.

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 butikkutsalgene KHM/NHM			X	
9	EU-revisjoner	X	X	X	X
11	AD HOC	X	X	X	X
10	Risikogjennomganger (fasilitering)	X	X	X	X

[2] The Institute of Internal Auditors
[3] Information Systems Audit and Control Association
[4] Norges interne revisorers forening

6. OPPFØLGINGSREVISJONER

I henhold til instruksen, er det pålagt Intern Revisjon å følge opp og se etter at det blir tatt behørig hensyn til revisjonsrapportene. På bakgrunn av endelig revisjonsrapport, har revidert enhet ansvar for at det blir utarbeidet en handlingsplan. Handlingsplanen, som skal inneholde så vel tidsfrister som opplysning om hvem som har ansvar for gjennomføring av tiltak, skal være grunnlaget for oppfølgingsarbeidet.

7. RAPPORTERING

Det vil bli utarbeidet rapporter etter alle revisjoner. Rapport sendes revidert enhet med gjenpart til overordnet enhet. Rapportformen vil kunne variere alt etter hva som anses som hensiktsmessig.

I henhold til Intern revisjons instruks skal det utarbeides halvårlige rapporter som også skal framlegges for Styret ved UiO.

FORSLAG REVISJONSOMRÅDER/ARBEIDSOPPGAVER EIR 2013[i]

NR	Revisjonsområde	Bakgrunn for valg av revisjonsområde	Gjennomføres
1.	Oppfølging av IHR	Det er satt mål for IHR-prosjektet, som nå går inn i en avsluttende fase. Tre arbeidsgrupper har avsluttet sitt arbeid, en del arbeid gjenstår i de øvrige arbeidsgruppene. Hva gjelder å dokumenter måloppnåelse, er prosjektet nå inne i en kritisk fase. Arbeidet vil bestå i å følge opp at de vedtak som er gjort i forhold til de arbeidsgruppene som har lagt fram sine forslag, blir gjennomført og å vurdere om de har/kan ventes å få de planlagte gevinster. Videre vil EIR følge resten av prosjektet for å bidra til å sikre framdrift, videreføring i linjen, og en vellykket gjennomføring av vedtatte tiltak.	**Påbegynnes i 2. halvår. Avsluttes i 2014**
2.	Oppfølging av styrevedtak	Blir Universitetsstyrets vedtak gjennomført som forutsatt? I revisjonsarbeidet vil EIR ta for seg vedtak i hht styreprotokoller for en nærmere definert periode, og se etter om vedtakene er gjennomført som forutsatt. Det vil også bli vurdert om vedtakene har hatt den tenkte/planlagte effekten. Det vil være aktuelt også å se på noe "eldre vedtak" for å kunne fastslå det siste; altså at tiltakene har den planlagte effekt.	**Påbegynnes 2. kvartal, avsluttes 4. kvartal**
3.	Strategi2020	Ved utarbeidelse av SP 2010 – 2020 ble det lagt vekt på at Målsettingene skulle være konkrete og målbare. Det er viktig at det sikres at strategiplanen implementeres nedover i organisasjonen. Det må være sammenheng mellom sentrale og desentrale styringsdokumenter. Hvem skal strategiplanen være et dokument for? Hele organisasjonen? Ledere? Er SP et levende dokument? Måloppnåelse - milepæler – gjennomføringsevne vil være sentrale begreper.	**Påbegynnes 2. kvartal, avsluttes 4.kvartal**

NR	Revisjonsområde	Bakgrunn for valg av revisjonsområde	Gjennomføres
4.	Sentral-administrasjonen koordinering	Det fremføres ofte kritikk mot SA fra fakulteter og muséer fordi man oppfatter virksomheten som lite koordinert. Det har blitt nevnt: styringssignaler fra samme avdeling trekker i forskjellige retninger, flere avdelinger spør (tilsynelatende) om samme /beslektet informasjon. EIR innhentet enkelte konkrete eksempler i forbindelse med utarbeidelsen av årsplanen. Disse vil trukket inn i/vurdert i revisjonsarbeidet	**Knyttes opp mot IHR-prosjektet – ikke eget revisjonsområde hvs EIR skal følge IHR-innspurten**
5.	Risiko vedr. systemer som delvis forvaltes av USIT, med styrere som ligger utenfor.	Noen nasjonale systemer har et styre som prioriterer utviklingen av systemet, mens selve utviklingen kjøpes som en tjeneste hos USIT. Er det risiko som kan ramme UiO sitt omdømme ved en alvorlig hendelse, selv om ansvaret formelt sett ligger hos systemets styre.?	**Påbegynnes 2. kvartal**
6.	Tilganger til IT-systemer/avslutning arbeidsforhold	Videreføres fra 2012: Tilgang til både fagsystemer og andre ressurser, og særlig koblet til intern flytting og avslutning av arbeidsforhold. Er det tilstrekkelige rutiner som sikrer konfidensialitet? (konfidensialitet = at kun autorisert personale får tilgang til tilgangsbegrenset informasjon, og at det på forhånd er foretatt en gyldig identifisering og autentisering av personen)	**Er igang** **Avsluttes 1. kvartal (mars/april)**
7.	Implementering av kvalitetssystem helseforskning	Videreføres fra 2012: Foreløpig revisjonsrapport sendt 8.2.2013; Noer oppfølging og etterarbeid i form av aktiviteter mot desentrale enheter må påregnes.	**1. kvartal**
8.	Oppfølging butikkutsalgene ved NHM og KHM	Sviktende rutiner ved utsalgsstedene ved NHM og KHM var medvirkende årsaker til at UiO fikk merknader i Riksrevisjonenens Dokument 1 til Stortinget. Universitetsdirektøren har en uttalt målsetting om at UiO IKKE skal ha slik omtale.	**3. kvartal**
9.	EU-revisjoner	Antall revisjoner forventes å bli noe mindre enn i 2013 som følge av at EU har endret revisjonskravene. Men det vil fortsatt være behov for at EIR utsteder Revisjonssertifikater.	**Hele året**
10.	RISIKO-gjennomganger	Jfr. bl.a epost til/fra Universitetsdirektøren.	**Ved behov hele året**
11.	Ad HOC	Evt. Ad hoc-oppdrag vurderes og avklares med universitetsdirektøren, og gjennomføres ved omprioriteringer hvis nødvendig	**Hele året - ett oppdrag påbegynt og avsluttet**

[i] For alle revisjonsområdene vil det bli utarbeidet mer omfattende oppdragsbeskrivelser