UNIVERSITETET I BERGEN

Arkivsaksnr.:	Dokumentdato:
2022/1526	02.03.2022

Styre:	Styresak:	Møtedato:
Universitetsstyret	28/22	10.03.2022

Prosjektplan - Internrevisjon Informasjonssikkerhet og GDPR

Henvisning til bakgrunnsdokumenter

- Styresak 9/22 Årsplan for internrevisjon 2022

Saken gjelder:
I styremøtet 2.februar 2022 vedtok universitetsstyret at revisjonsprosjektet om informasjonssikkerhet skulle legges fram for styret før iverksettelse. KPMG har i etterkant av styremøtet arbeidet fram en prosjektplan i dialog med UiB.

Prosjektplanen

KPMG skriver i sin prosjektplan at formålet med revisjonen er *«å vurdere om UiB er tilstrekkelig sikret mot cybertrusselen gjennom å ha etablert tilstrekkelig grunnsikring, vurdere om de har etablert tilstrekkelige tiltak som gjør UIB i stand til å oppdage og håndtere uønskede hendelser. Internrevisjonen vil også gjøre en vurdering av styring og kontroll med krav til personvern. Videre er formålet å styrke arbeidet med informasjonssikkerheten ved UiB.»*

Med hensyn på det konkrete innholdet sier planen at man *«vil ha særskilt fokus på:*

A. *I hvilken grad operasjonelle tiltak er etablert i UIBs sentrale infrastruktur for å beskytte seg mot uønskede hendelser (grunnsikring)*
B. *I hvilken grad UIB har etablert tekniske og organisatoriske tiltak for å kunne oppdage og respondere på uønskede hendelser*
C. *I hvilken grad UIB har etablert tekniske og organisatoriske tiltak for å respondere på og gjenopprette sentral IT infrastruktur*
D. *Personvern: Fokus på etterlevelse av personvernplikter i forskningsprosjekter, spesifikt hvordan studenter og forskere forholder seg til etablerte rutiner og informasjonsmateriell for innhenting, lagring etc.»*

Med hensyn på avgrensning skriver KPMG videre at «*Revisjonen vil ha mindre fokus på risikostyringsprosessen, organisatoriske forhold og lokale systemer ved fakultetene.»*

Universitetsdirektørens kommentarer:

Den reviderte planen framstår som mer konkret enn den KPMG la fram for styret i sak 9/22. Planen dekker to ulike områder, på den ene siden tekniske og organisatoriske forhold knyttet til beskyttelse, oppdage og gjenopprette av UiBs sentrale infrastruktur (A-C), og på den andre siden etterlevelse av personvernforpliktelser i forskningsprosjekter (D).

I styresak 67/19 og i 70/20 har internrevisjonen tidligere rapportert om lokalt driftet utstyr og systemer på fakultet og institutt, og her er det startet et større omleggingsprosjekt med øremerkede midler slik omtalt i styresak 120/21.

Universitetsdirektøren vil legge til rette for internrevisjonens arbeid på en god måte og bidra til at dette gir merverdi for UiB.

Forslag til vedtak:

Universitetsstyret tar prosjektplanen «Internrevisjon Informasjonssikkerhet og GDPR» til orientering.

Robert Rastad
universitetsdirektør

02.03.2022/Arne R. Ramslien/Tore Burheim(avd.dir)

Vedlegg:
1. Prosjektplan - Internrevisjon Informasjonssikkerhet og GDPR

Universitetet i Bergen

Prosjektplan Internrevisjon
Informasjonssikkerhet og GDPR

Dato 25.02.2022

www.kpmg.no

<table>
<tr>
<td>PROSJEKTNR/NAVN:
P 01/22 Modenhetsvurdering informasjonssikkerhet og GDPR</td>
<td>OVERORDNET RISIKOEIER:
Universitetsdirektør Robert Rastad

OPERASJONELL RISIKOEIER/KONTAKTPERSON:
IT-direktør Tore Burheim</td>
<td>OPPDRAGSANSVARLIG KPMG: Kine Kjærnet
KUNDEANSVARLIG: Kenneth Hansen
PROSJEKTLEDER: Mette Remø
TEAMDELTAKERE: Nils Harald Børve, Aleksandra Endresen</td>
</tr>
<tr>
<td>OMRÅDE SOM SKAL REVIDERES:

Revisjonen retter seg mot informasjonssikkerhet og personvern.</td>
<td>FORMÅL MED REVISJONEN:
Formålet med revisjonen er å vurdere om UiB er tilstrekkelig sikret mot cybertrusselen gjennom å ha etablert tilstrekkelig grunnsikring, vurdere om de har etablert tilstrekkelige tiltak som gjør UIB i stand til å oppdage og håndtere uønskede hendelser.

Internrevisjonen vil også gjøre en vurdering av styring og kontroll med krav til personvern. Videre er formålet å styrke arbeidet med informasjonssikkerheten ved UiB.</td>
<td>MÅLSETTINGER FOR OMRÅDET:
• Overholdelse av NSMs grunnprinsipper for IKT-sikkerhet og Nasjonal strategi for digital sikkerhet
• Styringsstruktur på et overordnet nivå er hensiktsmessig samt mellom administrasjon og fakulteter
• Overholdelse av regulatoriske krav til personvern og etterlevelse av UIBs internkontroll for personvern.
• Få en oversikt over:
- Hvor modne og effektive er eksisterende forsvarsmekanismer
- Hvordan sårbarheter påvirker virksomhetens risikoprofil
- Om eksisterende sikkerhetskontroller er tilpasset trussel-landskapet UiB opererer i.</td>
</tr>
<tr>
<td>FOKUSOMRÅDER
Internrevisjonen vil generelt se på helhetlig styring av personvern, cyber- og informasjonssikkerhet, men vil ha særskilt fokus på:
A. I hvilke grad operasjonelle tiltak er etablert i UIBs sentrale infrastruktur for å beskytte seg mot uønskede hendelser (grunnsikring)
B. I hvilke grad UIB har etablert tekniske og organisatoriske tiltak for å kunne oppdage og respondere på uønskede hendelser
C. I hvilke grad UIB har etablert tekniske og organisatoriske tiltak for å respondere på og gjenopprette sentral IT infrastruktur
D. Personvern: Fokus på etterlevelse av personvernplikter i forskningsprosjekter, spesifikt hvordan studenter og forskere forholder seg til etablerte rutiner og informasjonsmateriell for innhenting, lagring etc.

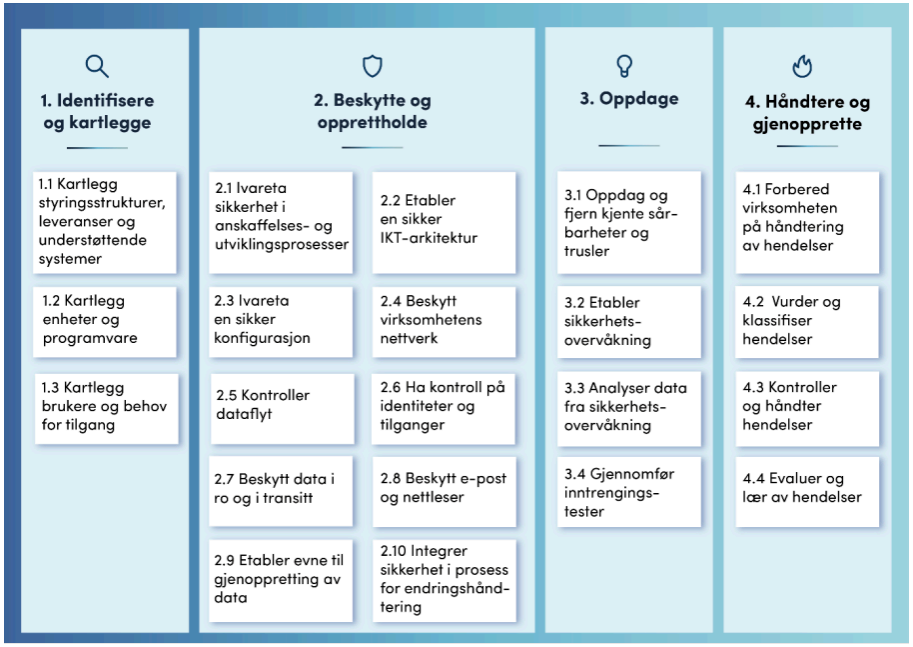
Avgrensning:
Revisjonen vil ha mindre fokus på risikostyringsprosessen, organisatoriske forhold og lokale systemer ved fakultetene.</td>
<td>METODE/FREMGANGSMÅTE:
• Oppstartsmøte for å diskutere omfang og gjennomføring av prosjektet
• Datainnsamling: Dokumentasjon, intervjuer og egenvurdering
• Analysere innsamlede data
• Oppsummeringsmøte, gjennomgang av våre observasjoner med risikoeier og ledelsen</td>
<td>FREMDRIFTSPLAN:
• Uke 12: Oppstartsmøte
• Uke 12-13: Datainnhenting, prosessgjennomgang og innledende dokumentanalyser
• Uke 14-17: Intervjuer og dokumentanalyse
• Uke 18-19: Analyse
• Uke 20-22: Rapportskriving
• Uke 23: Eventuelle oppfølingsintervjuer
• Uke 24: Valideringsmøte
• Uke 32: Rapporteringsmøte
• Uke 33: Endelig rapport sendes til styret

TIMER / BUDSJETT: 300 timer</td>
</tr>
<tr>
<td>Prosjektplanen er tatt til orientering
Sted/dato: Bergen, dd.mm.20åå</td>
<td colspan="2">Risikoeier:</td>
</tr>
</table>

Evalueringskriterier

UiB har utarbeidet en plan som er lagt opp etter NSMs grunnprinsipper for IKT-sikkerhet, se figur. Revisjonen vil derfor ta utgangspunkt i denne, og tilhørende skala for måling av modenhetsnivå. På personvernområdet vil internrevisor ha særskilt fokus på etterlevelse av personvernplikter i forskningsprosjekter, spesifikt hvordan studenter og forskere forholder seg til etablerte rutiner og informasjonsmateriell for innhenting, lagring og annen behandling av personopplysninger. Disse pliktene er illustrert i figuren under.

NSMs grunnprinsipper for IKT-sikkerhet



Virksomhetens plikter etter personvernregelverket

Modenhetsnivå

Initiell 0
Ad-hoc, uforutsigbar, dårlig kontrollert, reaktiv

Repeterbar 1
Grunnleggende prosesser, repeterbare oppgaver

Definert 2
Definerte og dokumenterte prosesser, proaktivt

Styrt 3
Integrerte prosesser, målbare og kontrollerte

Optimal 4
Kontinuerlig forbedring, tilpasning til organisasjonen

Modenhetsnivå vurderes for hvert domene og for hvert fokusområde innenfor domenene og angis på en skala fra 0 til 4.

Dokumentasjon

Relevante dokumenter (listen er ikke uttømmende):

- Styringssystem for IT- sikkerhet inkludert underliggende dokumenter
- Personverndokumentasjon
- Risikostyringsprosesser og risikovurderinger
- Hendelseslogg
- Rapporter fra tidligere sikkerhetstester
- Avtaler med tjenesteleverandører
- IT-infrastruktur og systemoversikt
- Risiko og sårbarhetsanalyser

Kontakt oss

Kine Kjærnet

Partner

T +47 905 69 124

E kine.kjaernet@kpmg.no

Kenneth Hansen

Director

T +47 907 37 682

E kenneth.hansen@kpmg.no

kpmg.no