120.

RIKSREVISIONEN

Datum: 2023-01-17

# Möte KTH7

Datum: 2023-01-17

Plats: KTH

**Deltagande**

KTH

Internrevisionschef och internrevisorer

RiR:

- Sara, Ludvig

- Internrevisionsrapport 2010 visade på brister. Granskning gjordes igen 2014, och samma problem framkom. Sen ny granskning 2020, föranledd av MSB:s nya föreskrifter.
- Konsulter gjorde penetrationstester.
- Finns en mer utförlig bilaga till 2020-rapporten, mer teknisk. Kanske intressanta för Josefine att ta del av
- Nuvarande styrelsen är väldigt intresserade av informationssäkerhet. Stort intresse och kunskap
- Internrevisionens egna riskanalys föranleder granskningar, och man lämnar sedan förslag till styrelsen
- Åtgärderna i svar på internrevisionens rekommendationer kommer inte med i verksamhetsplanen för verksamhetsstödet
- Internrevisionen gör sedan en årsrapport med uppföljningar
- Anna Dahlström gör riskanalys för hela KTH, på central nivå
- Stora problemet senaste åren har varit var i organisationen frågan om infosäk ska ligga. Om det ska ligga under säkerhet överlag t.ex. Inte haft en strategisk höjd.
- Även bekymmer att informationssäkerhetsansvarig nu ligger på IT-avdelningen. Inga tydliga roller. Har försvårat situationen för att se att det behöver lyftas till en mer strategisk fråga. Men samtidigt fördel att infosäk ligger på IT-avdelningen, rent operativt.

- En risk är det här med klassningen. Det finns en modell för det. Men verkar inte göras, ingen systematisk metod. Men kompetensen för att göra det finns nog.
- Externa finansiärer: ibland kräver de ett visst skydd.
- Man har gjort ansatser att kartlägga den information/data som finns på lärosätet. Arkivfunktionen. Utifrån informationshanteringsplanen. (CISO) har även försökt lite från sitt håll.
- Man har även gjort en ansats att samla alla projekt och avtal i en databas som heter CASE. Forskningsdatan ska inte samlas där utan mer dokumentation om projekten. CASE ska vara ett undersystem till diariesystem.
- Kan begära ut projektregister, antingen per skola eller institution. Man får unikt projektnummer, skola/institution, belopp, period, finansiär. Agresso. Prata med ekonomiavdelningen. Boka in möte?
- Infosäkarbetet är väldigt personberoende
- Internrevisorerna tycker att CISO:n borde vara tydligt kravställande mot IT-avdelningen
- Rollen som CISO har är inte tydligt definierad. Rapporteringen är inte fastställd eller beslutad, utan mer på behovsbasis eller när ledningen/styrelsen efterfrågar det
- Öppenheten på lärosäten är inte bara naivitet, utan något man aktivt strävat efter
- Hur doktorander sparar och lagrar sin data är en riskfaktor
- Skalskydd och behörighetshantering har det gjorts internrevision på
- Inga krav på att byta lösenord på sina konton
- Finns ingen anpassad utbildning i infosäk för anställda. Nyanställda får ingen utbildning i infosäk.
- Man mejlar vissa uppgifter helt fritt.
- Vissa forskare har nog däremot mer säkerhetstänk, en medvetenhet som kommer från deras forskningsområde (flyg och fartyg)
- Gästforskare och vad de får tillgång till