Enhedsledelsen: har ansvaret for informationssikkerhed på instituttet/fakultetet - og i den funktion også har det overordnede risikoejerskab.
Enhedslederen er ansvarlig for at fastlægge og dokumentere ejerskab af aktiver, herunder projekter og systemer, risici, foranstaltninger og krav/lovgivning.
Hvor ejerskabet er delt, bør der foreligge forvaltningsaftaler, som dokumenterer ansvarsfordelingen.

Risikoejer: kan, som det fremgår af rollerne Enhedsledelse og System-/aktivejer, tildeles på flere niveauer. Det vigtigste er, at en risikoejer har ansvaret for og beføjelsen til at forvalte de risici, de er ansvarlige for, herunder at træffe informerede beslutninger om håndtering af risici.

Hvilket ledelseslag en risikoejer skal findes på afhænger ofte af konsekvensen af den konkrete risiko - hvor risici med højkonsekvens ofte placeres højere oppe i hierarkiet end risici med lav konsekvens.

System-/aktivejer: forvaltning omkring et væsentlig aktiv kan tildeles system-/aktivejer, som oftest er en person med ledelsesansvar og med kendskab til selve brugen og værdien af aktivet for at sikre forretningens daglige virke.

System-/aktivejer kan også være risikoejer, men her kan der være behov for at sætte kriterier internt for, hvornår og hvilke risici og scenarier der *skal eskaleres* til enhedsledelsen og hvordan.

Organisering informationssikkerhed

Lokal Informationssikkerhedskorrdinator: har enten et institut eller fakultet, hvor de er udførende i forhold til informationssikkerhedsaktiviteter i den pågældende enhed.

Systemforvalter: har et dybdegående kendskab til aktivet, her et it-systemet; hvordan det benyttes og indgår som et vigtigt redskab i en kritisk forretningsproces. Systemforvalter forvalter it-systemet rent praktisk i det daglige.

Placering af risikoejerskab eller eskalering af risici kan identificeres gennem:

- hændelse der har en negativ påvirkning på AU/enhedens omdømme
- hændelse til stor gene for forretningen/bred brugergruppe
- kompromittering af kritiske/sensitive informationer eller stort omfang af berørte personer
- økonomi ud over Systemejers budget
- utilgængeligt centralt system/aktiv
- behov for kontakt til Datatilsynet