1: Identificér enhedens aktiver

- Hvilke aktiver er enheden ansvarlig for? (overblik)
- Har ledelsen en dækkende fortegnelse over de vigtige aktiver, den er ansvarlig for? (dokumenteret oversigt)
- Hvem er den respektive ejer af hvert aktiv? (ejerskab skal dokumenteres, og ejer skal være bekendt med sin rolle og sit ansvar)

2: Vurdér aktivernes kritikalitet og konsekvenser

- Hvilken dataklassifikation tilhører enhedens informationer og aktiver? (afgør kritikalitet og grad af beskyttelse)
- Hvad er mængden og koncentrationen af informationer? (påvirker kritikalitet)
- Hvilken forretningsprocessen understøtter informationen? (strategisk værdi) – herunder forretningsmæssig vigtighed af *fortrolighed*, *integritet* og *tilgængelighed*
- Hvilke forventninger har interessenterne?
- Hvordan stemmer det overens med AU's risikokriterier/risikotolerancer?
- Hvilken konsekvens kan læk/tab af informationer have?
  - Dødsfald/skade på enkeltpersoner/gruppe
  - Tab af frihed, værdighed/retten til privatliv
  - Tab af medarbejdere/viden
  - Skade på forretningsfunktion/–proces
  - Indvirkning på planer og deadlines
  - Tab af forretningsmæssig og økonomisk værdi
  - Skade på tillid fra offentligheden og omdømme
  - Brud på juridiske, lovmæssige/regulatoriske krav
  - Brud på kontrakter eller serviceniveauer
  - Negativ indvirkning på interessenter
  - Negativ påvirkning på miljøet

3: Prioritér enhedens mest kritiske og/eller sensitive aktiver

- Hvilke er enhedens mest kritiske og/eller sensitive aktiver? (i prioriteret rækkefølge)