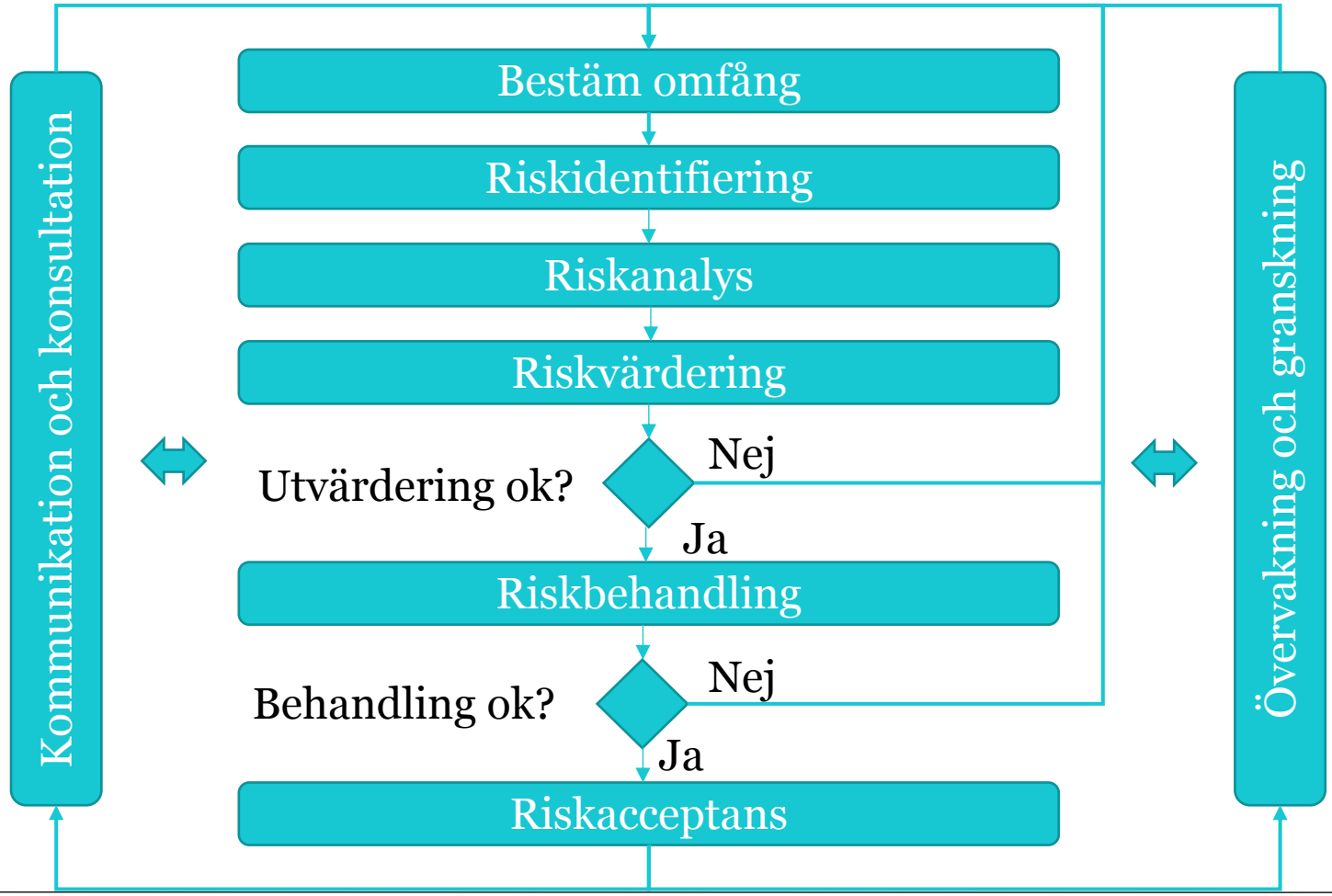
Arbetsflöde för riskhantering

Del av kursen ETE352 Cybersäkerhet – grunder och medvetenhet som ges vid Linköpings universitet

Mikael Asplund

LINKÖPINGS UNIVERSITET

Översikt av flödet (ISO 27005)



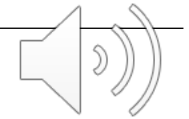
Bestäm omfång

Avgränsa!

Utgå ifrån systemmodellen

Bestäm konsekvens- och sannolikhetssnivåer

Definiera roller och ansvar



Riskidentifiering

Identifiera tillgångar

Huvudsakliga tillgångar

Tillgångar som kan möjliggöra åtkomst till andra tillgångar

Identifiera hot

Hotanalys (se kapitel 4)

Skapa riskscenarion

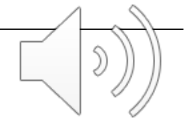
Riskscenarion

Attack/incident
Tillgång
Sårbarhet
Konsekvens

- En angripare utför en SQL-injection attack genom att skriva in databas-frågor i ett webbformulär som saknar indatavalidering vilket möjliggör dataläckage från databasen.

- En angripare skickar ett phishingmejl som ser ut som ett helpdesk-ärende till en oaktsam användare som klickar på länken och loggar in med sina uppgifter vilket resulterar i läckta inloggningsuppgifter.

- Ett utpressningsvirus tar sig in på utrustning för styrning av en vattenpump med default-inloggning och slår därmed ut vattenförsörjningen i en hel stadsdel.



Riskanalys

- Bestäm sannolikhet (frekvens)
  - Enligt förbestämd skala

- Bestäm konsekvens
  - Enligt förbestämd skala

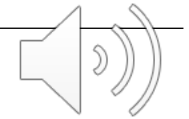
Utvärdera risker

Placera in risker i riskmatrisen

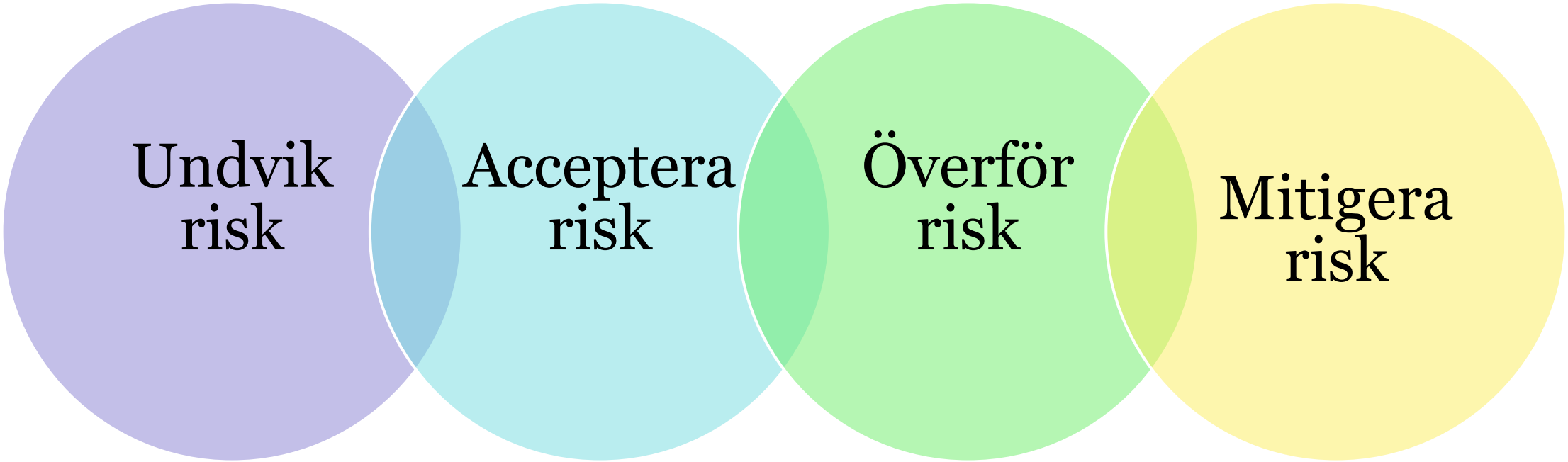
Avgör om riskerna är acceptabla

Prioritera de risker som behöver åtgärdas

Dokumentera



Behandla risker



Gör om processen…

- Är de vidtagna åtgärderna tillräckliga?
- Skapar åtgärderna nya sårbarheter?
- Skapar åtgärderna andra problem för verksamheten?
- **Riskanalyser är färskvara!**

https://cybersakerhet-grund.ida.liu.se

LINKÖPINGS UNIVERSITET