Sikkerhet, risikoanalyse og testing: Begrepsmessig avklaring

Seminar om risikoanalyse og testing innen sikkerhet

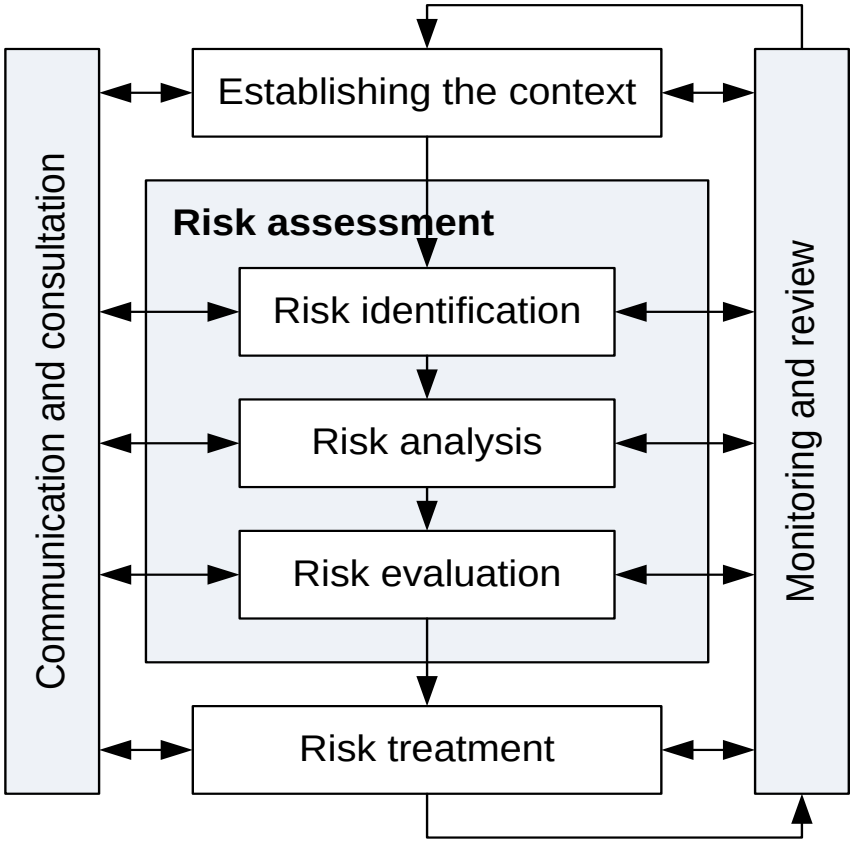
Bjørnar Solhaug

SINTEF, 11. juni, 2013

Oversikt

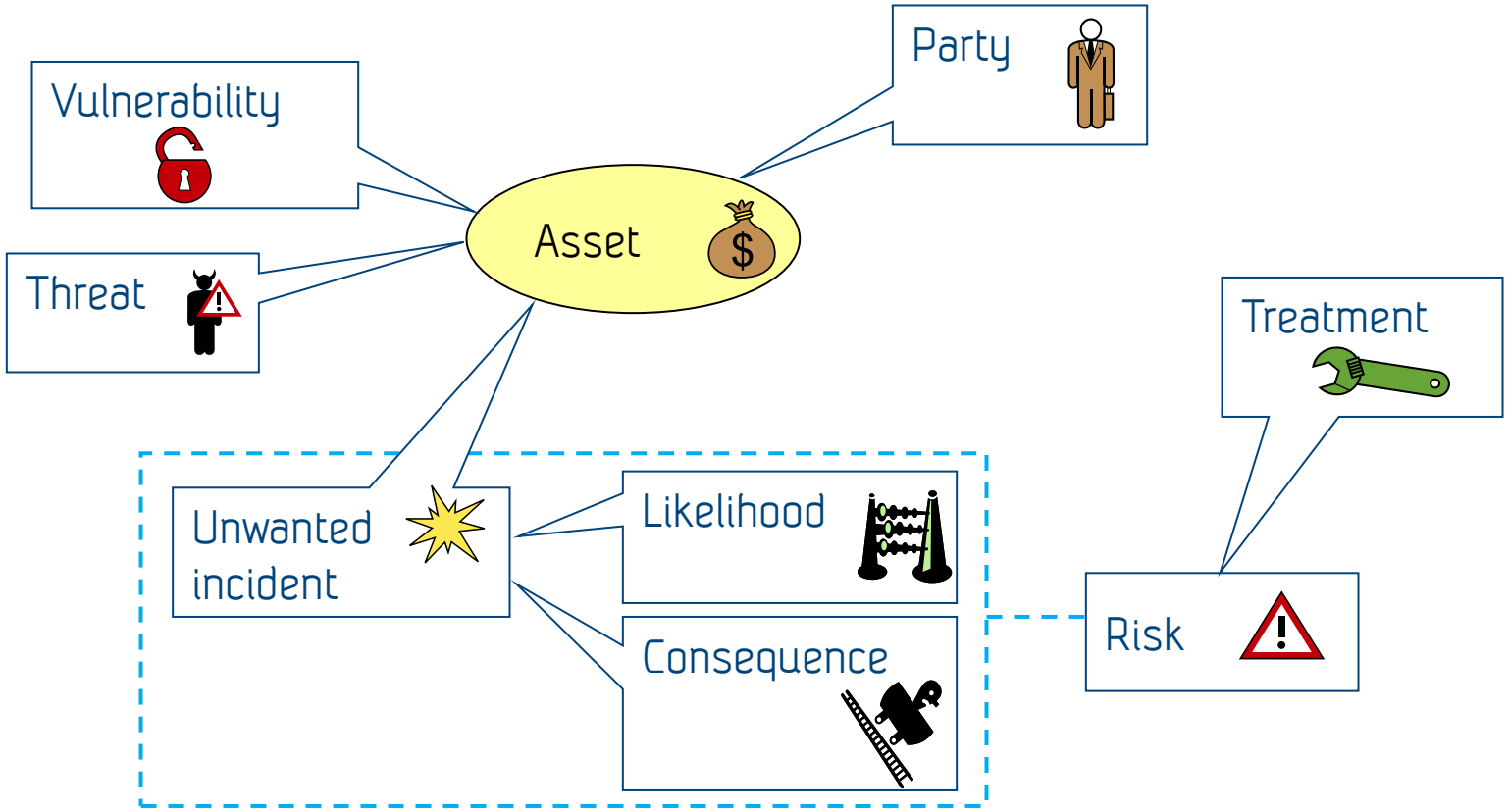
- Risikoanalyse
- Testing
- Sikkerhet som kriterium for risikoanalyse og testing
- Sikkerhet vs. Safety & Security
- Risikoanalyse og testing mht. sikkerhet
- Kombinasjon av risikoanalyse og testing
- Test-drevet risikoanalyse
- Risiko-drevet testing
- Oppsummering
- Videre lesning

Risikoanalyse – Prosess



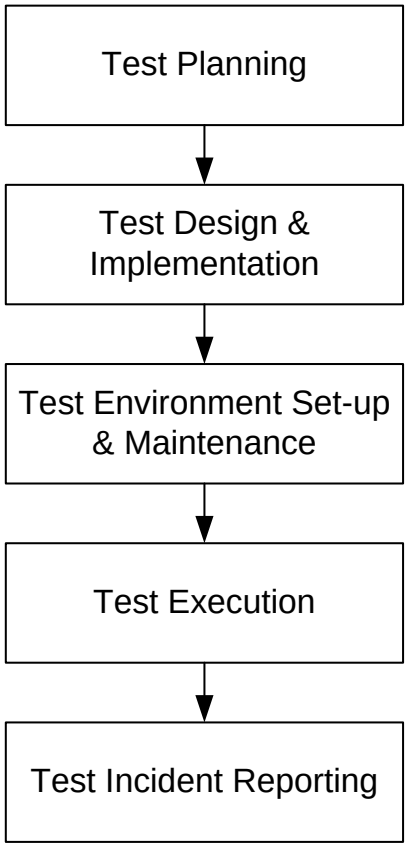
ISO 31000:2009

Risikoanalyse – Begreper



Testing – Prosess

- Testing innebærer å kjøre et system (exercising a system) for å verifisere at den oppfyller gitte krav, og for å avdekke feil
- Systemet er ofte referert til som "system under test" (SUT)



Basert på ISO 29119 (Draft)

Testing - Begreper

- Test planning
  - Planlegge hva det skal testes for (e.g. funksjonalitet, sikkerhet, ytelse) og hvilke deler av systemet som skal testes
- Test design & implementation
  - Utvikle test-caser og test-prosedyrer
- Test environment set-up and maintenance
  - Etablere og vedlikeholde oppsett og omgivelse for testingen
- Test execution
  - Gjennomføre test-caser og –prosedyrer i den etablerte omgivelsen
- Test incident reporting
  - Rapportering av identifiserte feil eller hendelser

Sikkerhet som kvalitetskriterium

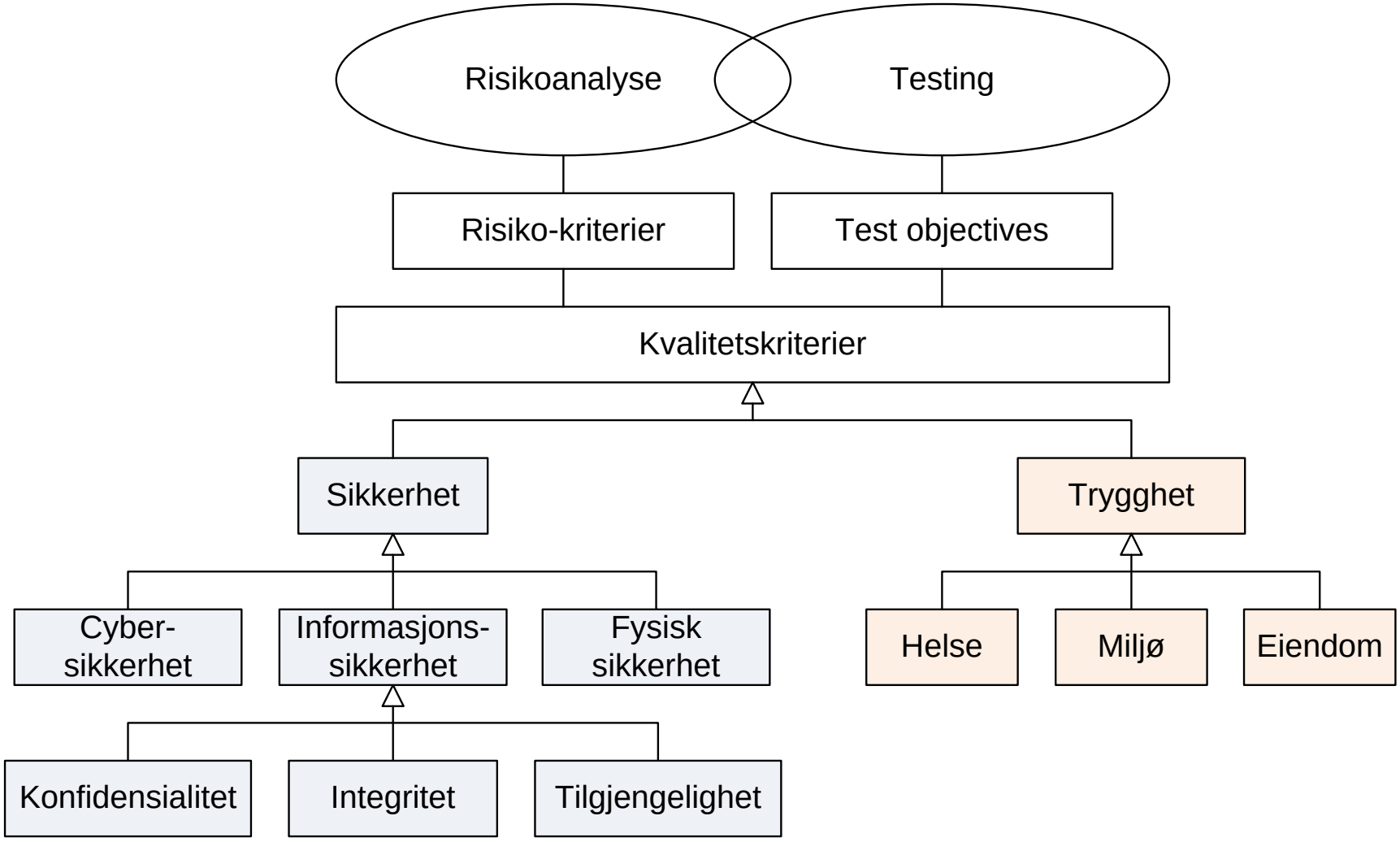
- Både risikoanalyse og testing kan utføres for ulike formål
  - Hva ønsker vi å avdekke?
  - Hva ønsker vi å oppnå?
  - Hva ønsker vi å forstå bedre?
  - Hva er våre **kvalitetskriterier**?
- Sikkerhets-risikoanalyse og sikkerhets-testing
  - Spesialiseringer rettet mot å forstå og forbedre sikkerheten til systemer
- Spesialiseringen av formålet
  - Risikoanalyse: Hva er våre aktiva og risiko-kriterier?
  - Testing: Hva er vår målsetting (test objectives)?
  - Formålet bestemmes av kvalitetskriteriene

Hva betyr "sikkerhet"?

Sikkerhet vs. Safety & Security

- "Sikkerhet" brukes gjerne i betydningen til både "safety" og "security"
  - Safety: Beskytte systemets omgivelser mot fare (hazard) for liv, helse, eiendom eller miljø
  - Security: Beskytte systemet mot skade påført av trusler gjennom utnyttelse av sårbarheter
    - Information security: Beskyttelse av konfidensialitet, integritet og tilgjengelighet av informasjon
- På norsk opererer man gjerne tilsvarende begrepsskille mellom sikkerhet og trygghet
  - Sikkerhet = Security
  - Trygghet = Safety
- For mange systemer (f. eks. kritiske infrastrukturer) er kriterier mht. både sikkerhet og trygghet viktig, i tillegg til flere andre kvalitetskriterier

Risikoanalyse og testing mht. sikkerhet



Kombinasjon av risikoanalyse og testing

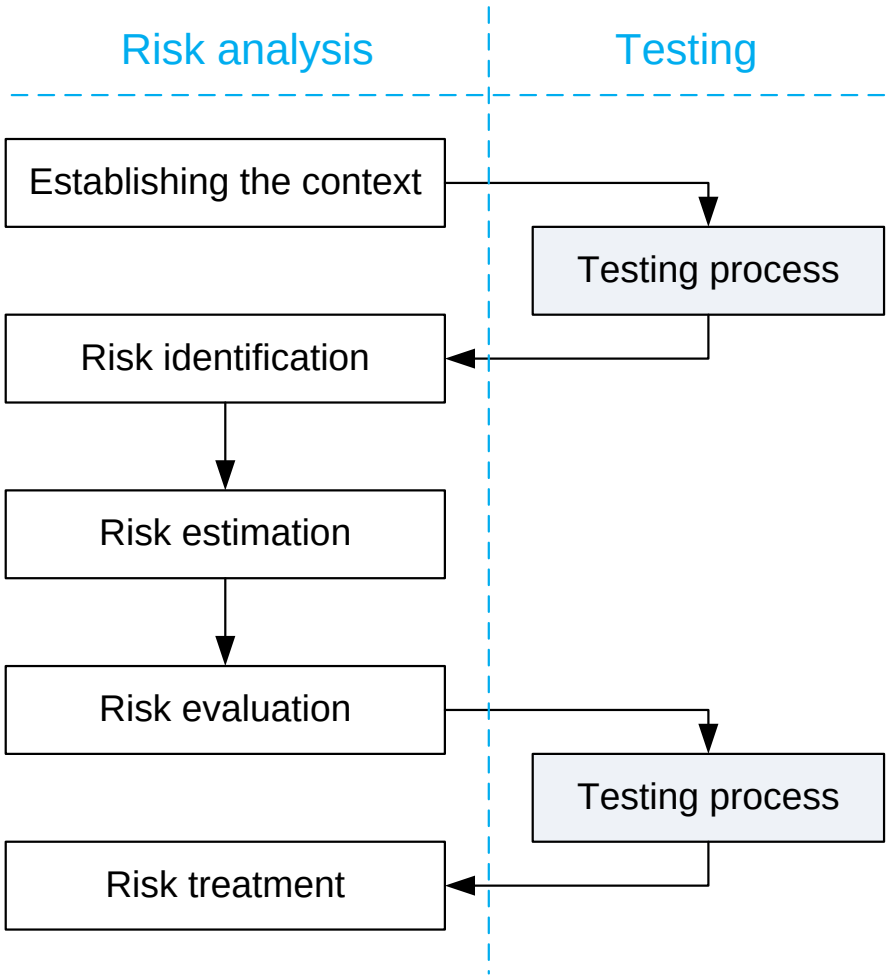
- Risikoanalyse og testing kan kombineres for gjensidig støtte

- Testdrevet risikoanalyse
  - Systematisk bruk av testing som en del av risikoanalysen
  - Testingen styres av aktiva og kriterier fra risikoanalysen

- Risikodrevet testing:
  - Systematisk bruk av risikoanalyse som en del av testingen
  - Risikoanalysen styres av test objectives

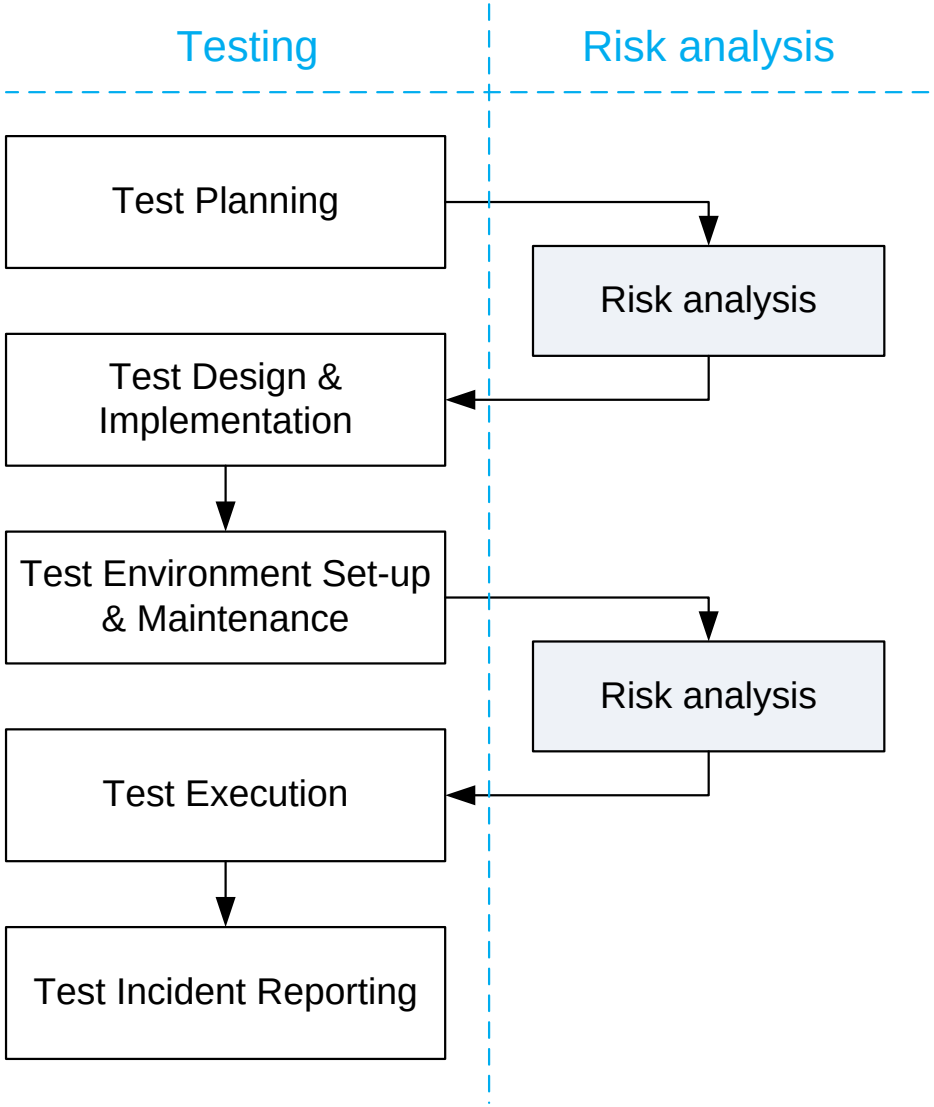
Testdrevet risikoanalyse

- Bruk av testing for å støtte risikoidentifikasjon
  - Sårbarheter, trusler, scenarier og uønskede hendelser, …
- Bruk av testing for å validere/korrigere analysen
  - Sårbarheter, sannsynligheter, konsekvenser, …

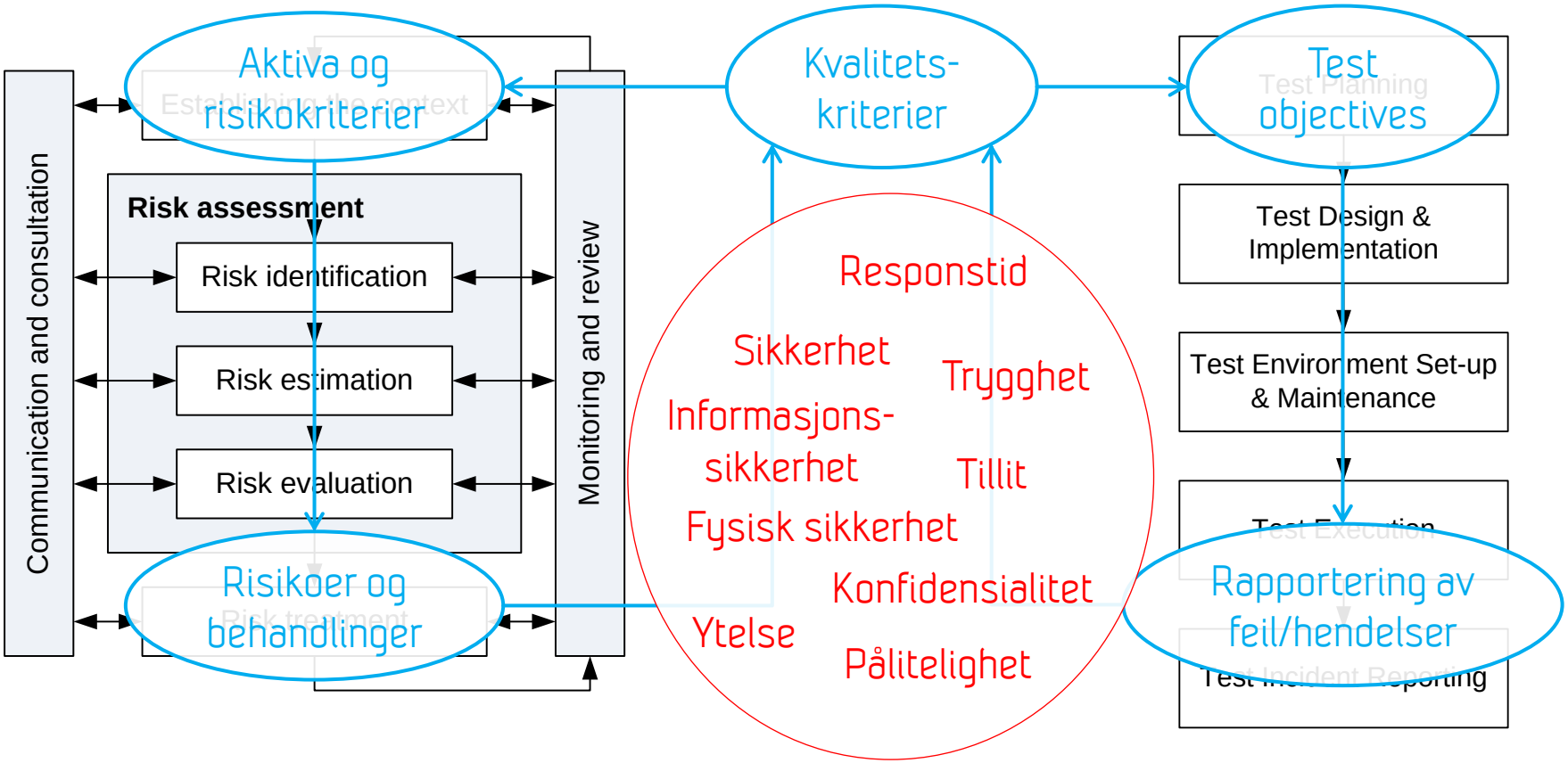


Risikodrevet testing

- Risikoanalyse for å identifisere hvilke deler av systemet som bør testes
  - Prioriterte risikoer for å optimalisere testdesign
  - Identifisere test-caser
- Risikoanalyse for å prioritere test-caser



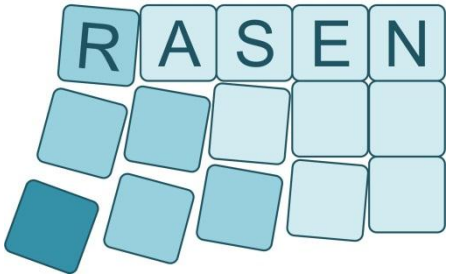
Oppsummering



Videre lesning

- Gencer Erdogan, Yan Li, Ragnhild Kobro Runde, Fredrik Seehusen, Ketil Stølen: Conceptual framework for the DIAMONDS project. Technical report, SINTEF A22798, SINTEF ICT, 2012
- International Organization for Standardization: ISO 31000 – Risk management – Principles and guidelines, 2009
- International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27001 – Information technology – Security techniques – Information security management systems, 2005
- International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management, 2011
- International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 9126 – Software engineering – Product quality – Part 1-4, 2001-2004.
- International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers: ISO/IEC/IEEE 29119 – Software and systems engineering – Software testing (under development)

Relaterte prosjekter



www.rasen-project.eu

www.itea2-diamonds.org

www.nessos-project.eu