NTNU

Kunnskap for en bedre verden

Risiko og Sårbarhetsanalyse på NTNU

Presentasjons av prosess

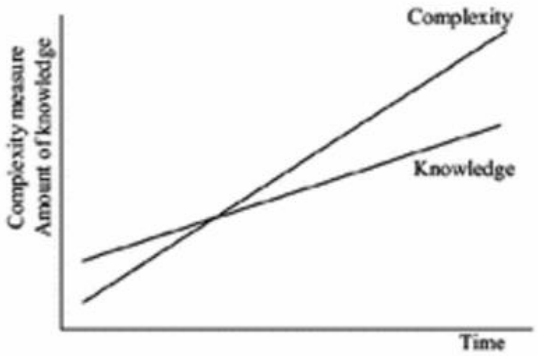
NTNU

(Info)Sikkerhetsrisiko formål

Utfører risikovurderinger for å:

- Redusere usikkerhet og kompleksitet for systemet
- Kartlegge uakseptabel risiko
- Foreslå risikoreduserende tiltak
- Legge til rette for styring og oversikt
- Veie positive og negative aspekter mot hverandre
- Innrette sikkerhet for å oppnå best mulig resultater

- *Ta bedre sikkerhetsbeslutninger!!!*

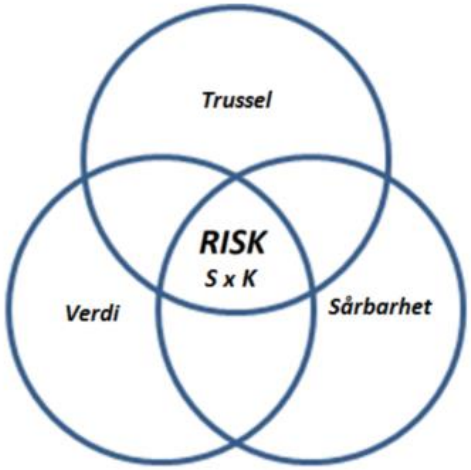


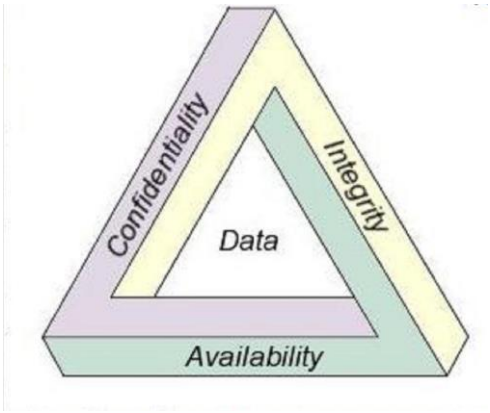
(a) The Complexity-Knowledge gap

NTNU

Hva er Informasjonssikkerhetsrisiko?

- *"The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."*
  - ISO/IEC 27005:2008
- Verdi x Sårbarhet x Trussel -> Utfall (negativt)
- Vurdere brudd på Konfidensialitet, Tilgjengelighet, og Integritet





Nivå 0


Input: System-spesifikasjoner, Intervjuer, Data, Tidligere ROS, osv...
Risikovurdering
Output: Uakseptable Risiko og tiltak for risikohåndtering

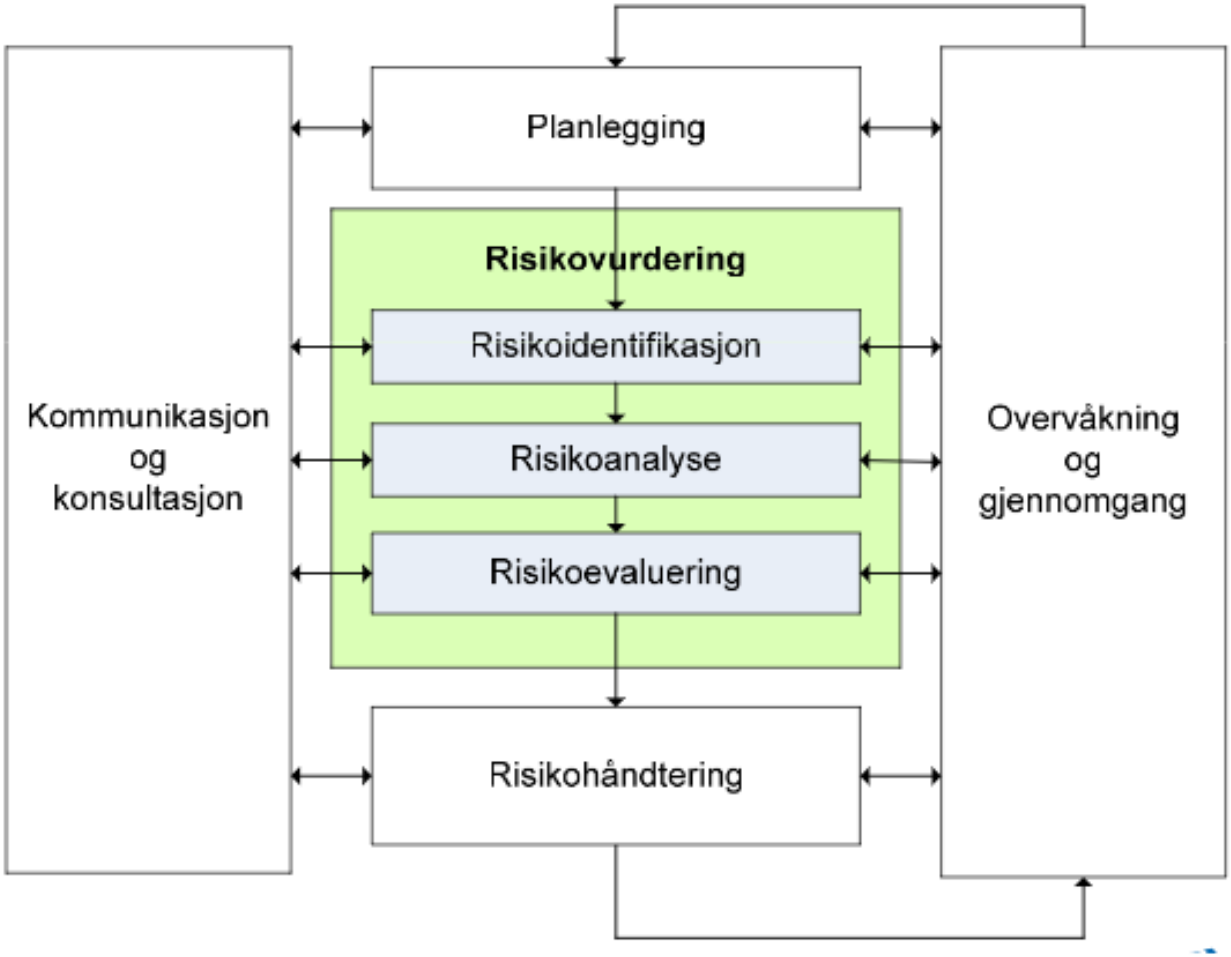
NTNU

Risikostyringsprosessen, Nivå 1

1. Definer kontekst og omfang
2. Identifiser uønskede utfall
3. Estimer konsekvenser og tilhørende sannsynligheter
4. Veie risiko vs gevinst og risikoappetitt
5. Beslutt om risikoen er akseptabel
6. Foreslå og Implementer tiltak (Kost-nytte analyse)
7. Evaluer om tiltak fungerer og om nåværende risikonivå er akseptabelt

NTNU

Risikostyringsprosessen, Nivå 1



ISO/IEC 27005:2011

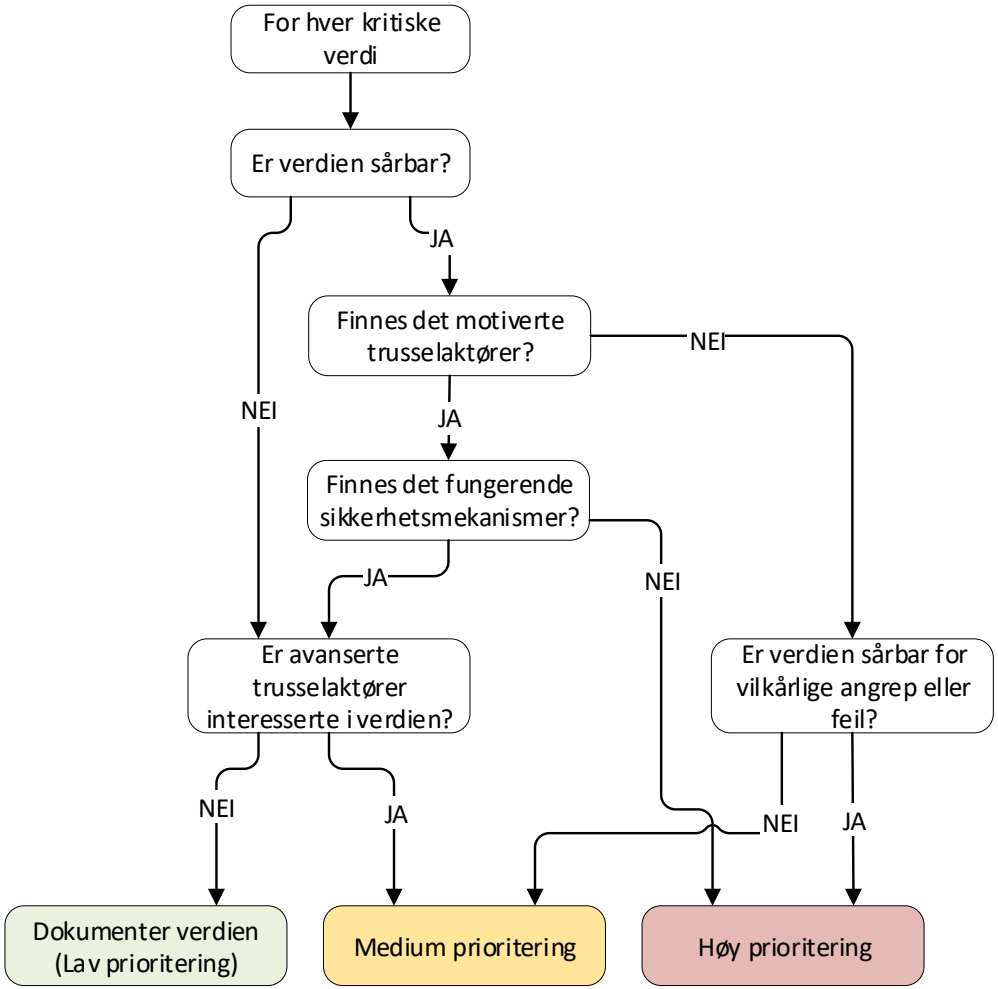
Forventet produkt 1

- Produktet av risikoidentifiseringen er:
  - Oversikt med verdier og kritikalitet som systemet håndterer/lagrer
  - Oversikt over mest sannsynlige trusler mot systemet
  - Oversikt over sårbarheter samt vurdering av alvorlighet
  - Oversikt over eksisterende kontroller i systemet
  - *Risikoscenarier med negativt utfall utledet av punktene over*

Verdivurdering

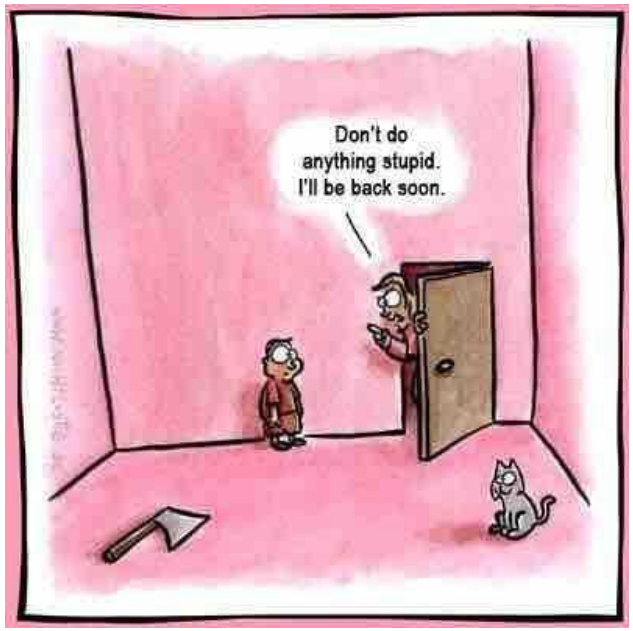
Klasse	Konfidensialitet	Integritet	Tilgjengelighet
Nivå 1	**Åpen** informasjon som er tilgjengelig for alle uten særskilte tilgangsrettigheter. Informasjon som ikke kan skade noe eller noen, og alle kan få se.	Arbeidsdokumenter, notater og tilsvarende informasjon hvor feil i informasjonen ikke får negativ konsekvens i beslutningsprosesser hos den/de som benytter informasjonen.	Nedsatt ytelse eller utilgjengelighet til informasjon eller tjeneste har liten eller ingen betydning for produksjon eller omdømme ved NTNU. Begrenset tilgang kan oppleves som kritisk for enkeltperson(er), men har liten betydning for NTNUs totale produksjon eller omdømme. Feilretting skjer kun innenfor normal arbeidstid.
Nivå 2	**Intern** benyttes om informasjon som er begrenset til å være tilgjengelig for medarbeidere for å gjennomføre pålagte oppgaver. Informasjonen kan være tilgjengelig for eksterne med kontrollerte tilgangsrettigheter. Informasjon på avveie kan gi moderate økonomiske skader og/eller svekket omdømme for NTNU, enkeltindivider eller samarbeidspartnere.	Den som benytter informasjonen forventer at den er autentisk og gyldig. Feil i informasjonen kan gi moderate økonomiske skader og/eller svekket omdømme for NTNU, enkeltindivider eller samarbeidspartnere.	Nedsatt ytelse eller utilgjengelighet kan føre til noe etterslep i produksjon og redusert servicenivå for store deler av NTNU. Systemet og dataene kan være utilgjengelig i 2 virkedager uten at det medfører vesentlig fare for økonomisk- eller omdømmetap for NTNU. Feilretting skjer kun innenfor normal arbeidstid.
Nivå 3	**Fortrolig** benyttes dersom det vil kunne skade offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at dokumentets innhold blir kjent for uvedkommende. Informasjon skal kun være tilgjengelig for medarbeidere med kontrollerte rettigheter og med behov for denne informasjonen. Informasjon på avveie som kan medføre alvorlig skade for NTNUs formål, samarbeidspartnere, enkeltpersoner og/eller samfunnet om den kommer uautoriserte i hende.	Den som benytter informasjonen er avhengig av at den er autentisk og gyldig. Utilsiktet eller tilsiktet feilinformasjon vil kunne føre til feilvurderinger eller beslutninger slik at det kan medføre betydelig økonomisk tap, omdømmetap eller annen skade for NTNU, enkeltindivider eller samarbeidspartnere. Grunndata, forskningsdata og publikasjoner hvor autentisitet er svært viktig	Benyttes der nedsatt ytelse eller utilgjengelighet kan føre til store etterslep eller stans i vesentlige tjenesteleveranser. Systemet kan maksimalt være utilgjengelig i 4 timer uten at det medfører vesentlig fare for økonomisk- eller omdømmetap for NTNU. Feilretting starter umiddelbart og fortsetter inntil feilen er løst.
Nivå 4	**STRENGT FORTROLIG** benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende. Informasjon skal kun være tilgjengelig for medarbeidere med strengt kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. I spesielle tilfeller kan strengt fortrolig informasjon også gjøres tilgjengelig for eksterne under samme strengt kontrollerte tilgangsrettigheter. Brudd kan medføre katastrofal skade på NTNUs interesser, samarbeidspartnere, enkeltpersoner og samfunnet om den kommer uautoriserte i hende.	Det er av kritisk betydning at det avleveres autentisk og gyldig informasjon. Utilsiktet eller tilsiktet feilinformasjon vil kunne føre til feilvurderinger eller beslutninger med fatale konsekvenser. Brudd kan medføre tap av liv for eksempel ved feilbehandling av pasienter, eller feilkonstruksjoner i bygg. Brudd kan medføre korrupte data i sentrale systemer som fører til omfattende følgefeil og påfølgende stort tap av produsert materiale ved NTNU.	Benyttes der nedsatt ytelse eller utilgjengelig kan være katastrofalt. Dvs. selv korte avbrudd vil føre til kritiske situasjoner. Systemet er virksomhetskritisk og vil ved utilgjengelighet umiddelbart medføre vesentlig fare for økonomisk- eller omdømmetap for NTNU. Systemet har høyeste prioritet, feilretting starter umiddelbart og fortsetter inntil feilen er løst.

Utsiling og seleksjon av risiko



Risikoestimering

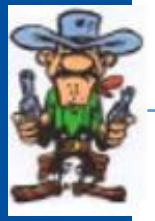
Identifiserte scenarioer estimeres med sannsynlighet og konsekvens.



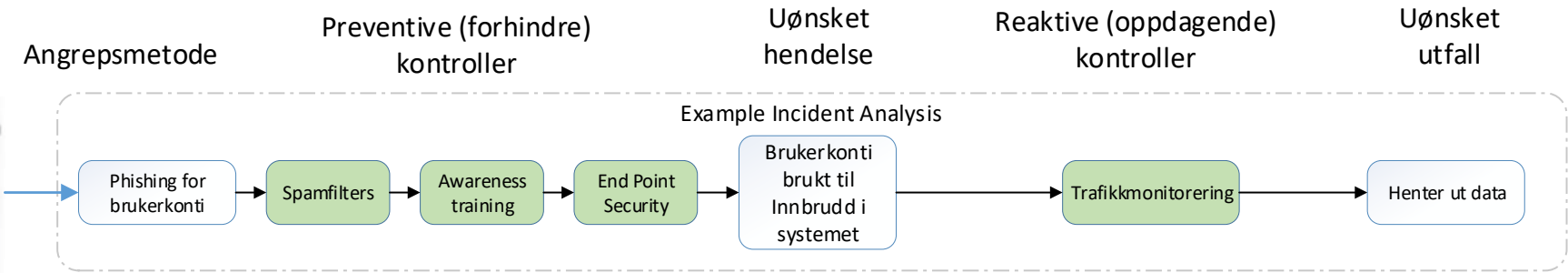
Forventet produkt 2

- Produktet av risikoestimeringen
  - Risikoanalyse basert på sannsynlighet og konsekvens for risikoscenariene
  - Prioritert liste med risikoer
- Tiltaksplan
  - Forslag til tiltak basert på Kost/nytte analyse
  - Prioriterte tiltak
  - Eier av risiko og tiltak
  - Tidsfrist for implementasjon (opp til beslutningstager)

Enkel risikomodell



Industri-spion



- Fra venstre er trusselaktøren som har intensjon om å bryte seg inn i systemet
- Aktøren velger angrepsmetode
- Mellom aktøren og den den uønskede hendelsen er det preventive sikkerhetsmekanismer (kontroller) som er på plass for å redusere sannsynligheten for at angrepet lykkes
- Hvis angriperen kommer seg forbi de preventive mekanismene, så har vi reaktive (oppdagende eller gjenopprettende) sikkerhetsmekanismer som er på plass for å redusere konsekvensen av et vellykket angrep.
- Hvis alle mekanismer feiler så vil angriperen lykkes og vi vil ha et uønsket utfall (eller en incident)
- Da må vi estimere konsekvenser og sannsynligheter

Konsekvenstabeller for estimering

KONSEKVENS						
Konsekvens	Minimum	Maximum	**Økonomi**	Personsikkerhet	Omdømme	Personvern
4 KRITISK	NOK	NOK	Tap av eller uopprettelig skade på store forskningsdata. Alvorlige bøter og/eller sanksjoner fra offentlige myndigheter.	Ett eller flere dødsfall. Flere personskader med varige men.	Straffereaksjoner fra offentlig myndighet Tap av forskningsprosjekter og/eller oppdragsforskning. Negativ omtale i riksdekkende media, sosiale media og/eller fagmiljøer Fare for stort frafall søkere på ett eller flere studie	Alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi (kompromittering av opplysninger av registrerte som kritisk krenkende).
3 ALVORLIG	NOK	NOK	Tap av eller uopprettelig skade på betydelig forskningsdata. Moderate bøter og/eller sanksjoner fra offentlige myndigheter.	Alvorlig personskade på en eller flere personer. Mén eller fare for varig mén. Personskade med fravær over 16 dg.	Tap av forskningsprosjekter og/eller oppdragsforskning. Negativ omtale i sosiale media og fagmiljøer	Tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatter som krenkende, eller som andre kan gjøre nytte av)
2 LITEN	NOK	NOK	Tap av eller uopprettelig skade på forskningsdata tilknyttet en enkeltforsker	Få/små personskader. Fravær opp til 16 dager.	Flere misfornøyde studenter/ansatte Negativ omtale i interne kanaler	Tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger den registrerte oppfatter som følsomme)
1 UBETYDELIG	NOK	NOK	Kostnader/tap opptil XXX* NOK Ikke tap av eller uopprettelig skade på forskningsdata	Personskade uten fravær	Ingen negative skadevirkninger	Ingen tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger som den enkelte ikke oppfatter som følsomme).
	*Fylles ut av linjeleder	*Fylles ut av linjeleder				

Sannsynlighetsvurdering for estimering

SANNSYNLIGHET			
Grad av sannsynlighet	**Skriftlig beskrivelse**	Beskrivelse sannsynlighet	Frekvens intervall (P)
4	SVÆRT SANNSYNLIG	Oftere enn en gang i måneden	P>13/365
3	SANNSYNLIG	En til tolv ganger i året	1/365 til 12/365
2	MINDRE SANNSYNLIG	En gang annenhvert år	0,9/365 til 0,5/365
1	USANNSYNLIG	Sjeldnere enn annenhvert år	P<0,5/365

Dagens oppgaver:
ROS Nivå 2