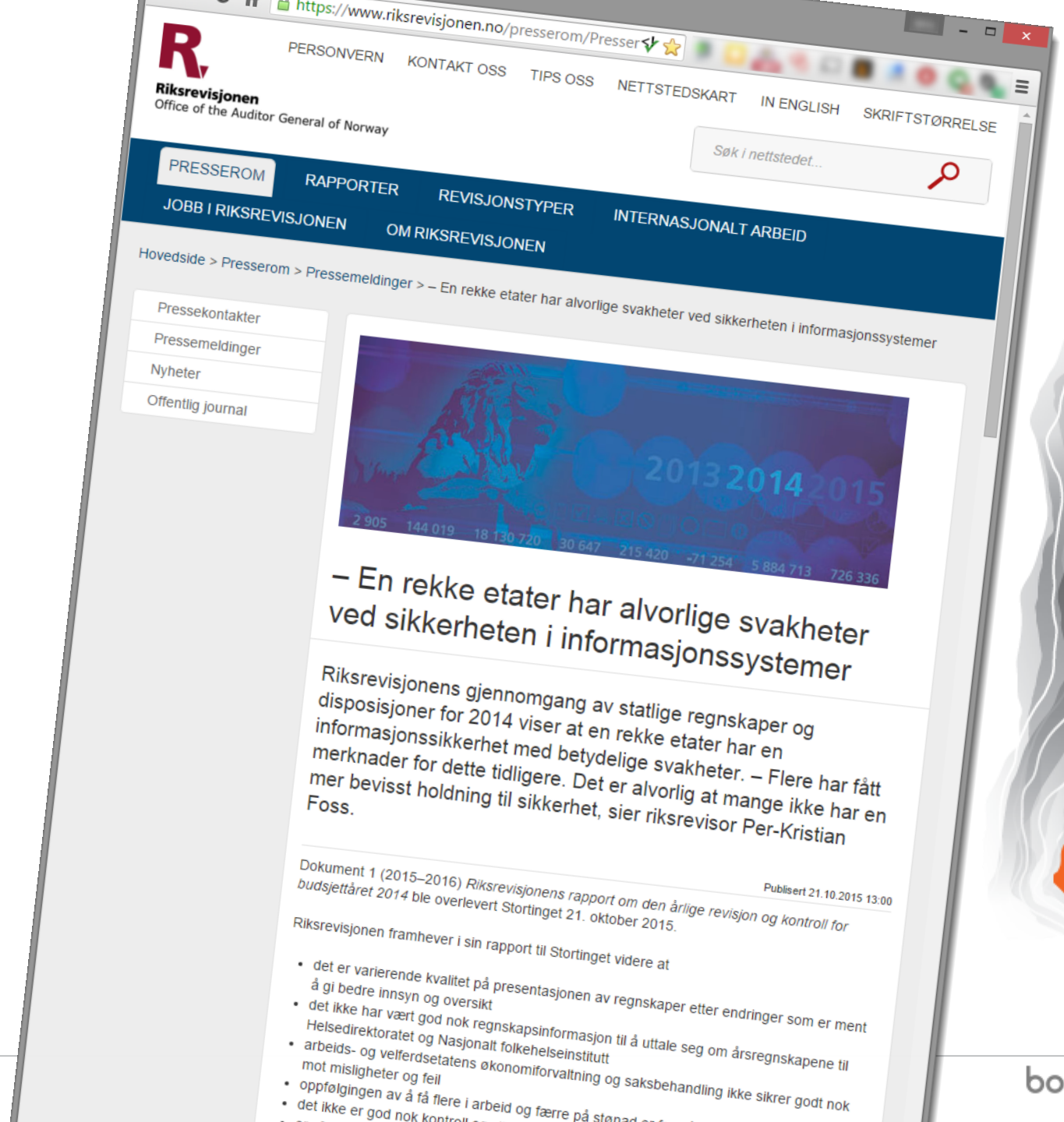
Workshop: Informasjonssikkerhet i digitaliseringsprosjekter

NOKIOS 2015/Jens Lien

- Når man endelig har fått til noe, og lagd noe som er bra, så kommer det ei **«knetakling»** inn fra sikkerhetshold og ødelegger alt!

– Vi ser alvorlig på de svakhetene som er avdekket. Større forbedringer forutsetter kompetanse og systematisk arbeid, men det er også ***mulig å oppnå bedre sikkerhet med tiltak som ikke krever store ressurser****, sier Foss.*



bouvet

IKKE BLI FELT AV SIKKERHETSFEIL

Prosjektveiviseren

- Bidrar til bedre **planlegging** og **prosjekteierstyring**
- Felles modell for offentlig sektor: Erfaring og **læring på tvers**
- Mer effektiv **samarbeid** med leverandør/konsulentmiljøer

Prosjektveiviseren

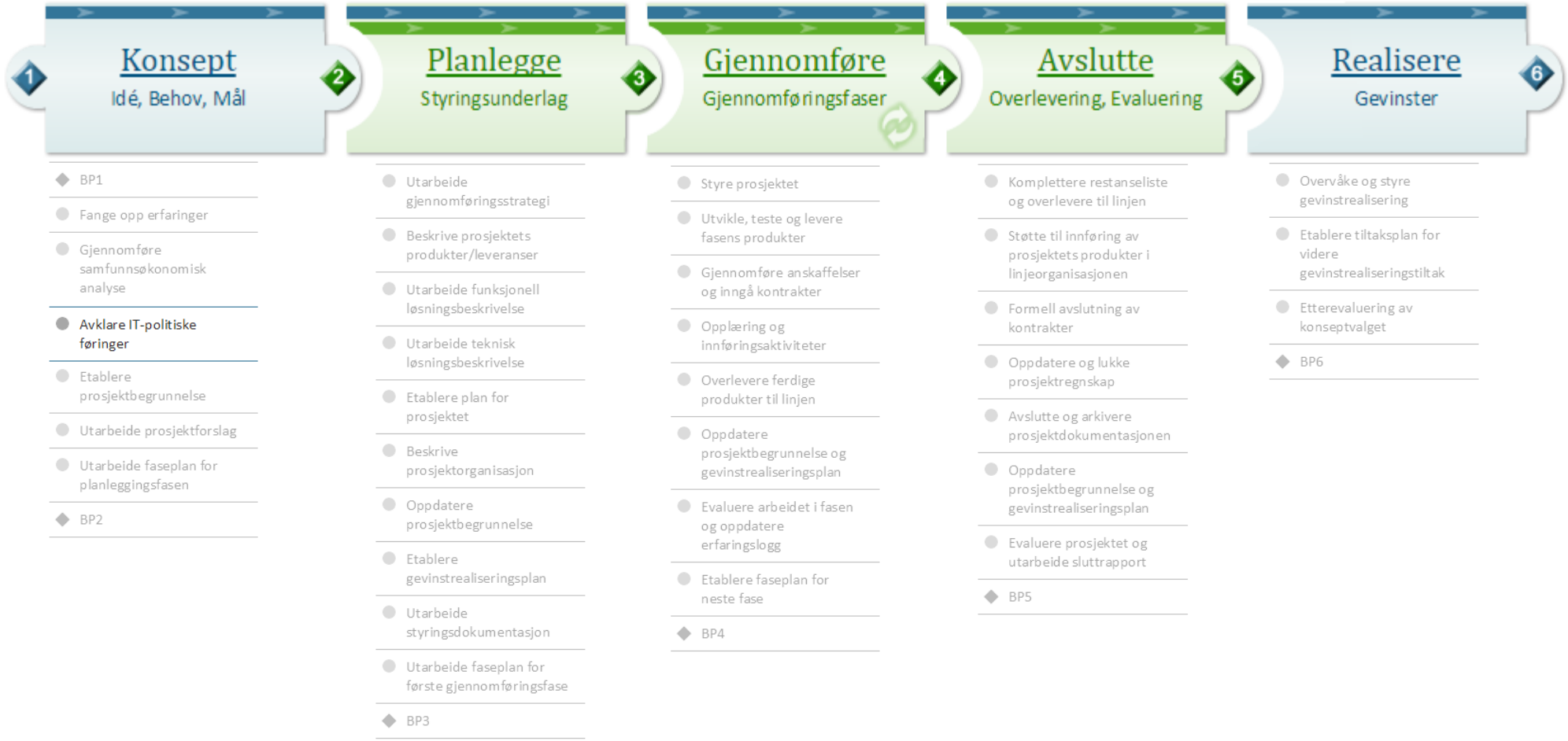
bouvet

Prosjektveiviseren

bouvet

- En svakhet ved veiviseren er imidlertid hvordan arbeid med **sikkerhet** (og person-vern) **bortimot utelates** fra prosjektprosessen.

Prosjektveiviseren og informasjonssikkerhet



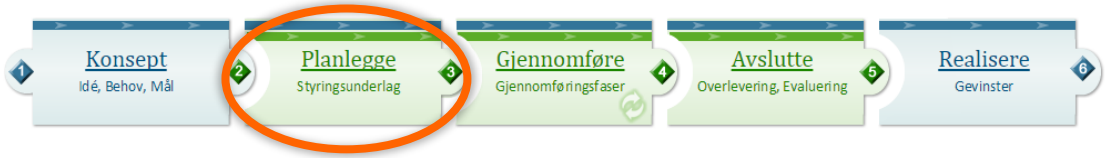
bouvet

Tillegg og utvidelser - **Konsept**

- BP1
- Fange opp erfaringer
- Gjennomføre samfunnsøkonomisk analyse
- Avklare IT-politiske føringer
- Etablere prosjektbegrunnelse
- Utarbeide prosjektforslag
- Utarbeide faseplan for planleggingsfasen
- BP2

- **Fange erfaringer:**
  - Etterspørre erfaringer fra sikkerhetsarbeid. Revisjonsrapporter.
- **IT-politiske føringer:**
  - Eksisterende digitaliserings- eller sikkerhetsstrategier i organisasjonen?
  - Felles sikkerhetskrav (ikke-funksjonelle krav)
  - Nasjonale felleskomponenter (eks. ID-porten, Feide)
  - Nasjonale anbefalinger/føringer (eks. *Normen*, veiledere fra datatilsynet)
- **Utarbeide prosjektforslag**
  - Identifisere ansvarlig for informasjonssikkerhet

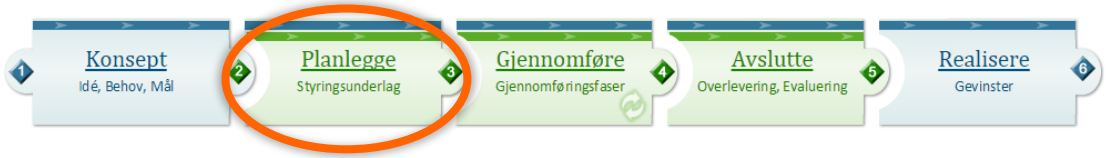
Tillegg og utvidelser - **Planlegge**



- Utarbeide gjennomføringsstrategi
- Beskrive prosjektets produkter/leveranser
- Utarbeide funksjonell løsningsbeskrivelse
- Utarbeide teknisk løsningsbeskrivelse
- Etablere plan for prosjektet
- Beskrive prosjektorganisasjon
- Oppdatere prosjektbegrunnelse
- Etablere gevinstrealiseringsplan
- Utarbeide styringsdokumentasjon
- Utarbeide faseplan for første gjennomføringsfase
- BP3

- **Beskrive produkt/leveranser**
  - Bedømme *kritikaliteskategori*
  - Tilpasse sikkerhetskrav (ikke-funksjonelle krav) basert på kritikalitetskategori
  - Beskrive kvalitetskontroll/testrutiner mhp. sikkerhet.
  - Krav til kompetanse og ferdigheter innen sikkerhet for utviklere/testere.
- **Teknisk løsningsbeskrivelse**
  - Applikasjonsarkitektur med sikkerhetselementer. Egen sikkerhetsarkitektur?
  - Grensesnittspesifikasjoner
  - Bruk av felleskomponenter for sikkerhet
- **Etablere prosjektplan**
  - Identifisere nødvendig arbeid for godkjenning av leveransen.
  - Allokere sikkerhetsressurser (internt og hos leverandør)
  - Kompetansetiltak?

Tillegg og utvidelser - **Planlegge** *(forts)*



- Utarbeide gjennomføringsstrategi
- Beskrive prosjektets produkter/leveranser
- Utarbeide funksjonell løsningsbeskrivelse
- Utarbeide teknisk løsningsbeskrivelse
- Etablere plan for prosjektet
- Beskrive prosjektorganisasjon
- Oppdatere prosjektbegrunnelse
- Etablere gevinstrealiseringsplan
- Utarbeide styringsdokumentasjon
- Utarbeide faseplan for første gjennomføringsfase
- BP3

- **Beskrive prosjektorganisasjon**
  - Identifiser ansvar for informasjonssikkerhet i prosjektet
- **Utarbeide styringsdokumentasjon**
  - RoS-analyser for informasjonselementer, systemet, komponentene (interne og eksterne). Fokus på virksomhetsmessig risiko.
  - Vurdere personvernkonsekvenser (*Privacy Impact Assessment*, prinsipper for innebygd personvern)
  - Trusselmodellering
- **Faseplan (første) gjennomføringsfase**
  - Utdypende beskrivelse av sikkerhetsarbeid fører til bedre samarbeid med leverandør
- **BP3 - Beslutte gjennomføring**
  - Er prosjektets kartlegging av risiko og tiltak for informasjonssikkerhet tilfredsstillende?

bouvet

Tillegg og utvidelser - **Gjennomføre**

- Styre prosjektet
- Utvikle, teste og levere fasens produkter
- Gjennomføre anskaffelser og inngå kontrakter
- Opplæring og innføringsaktiviteter
- Overlevere ferdige produkter til linjen
- Oppdatere prosjektbegrunnelse og gevinstrealiseringsplan
- Evaluere arbeidet i fasen og oppdatere erfaringslogg
- Etablere faseplan for neste fase
- BP4

- **Utvikle, teste og levere produkter**
  - Analyse av sikkerhetsarkitektur
  - Analyse av angrepsflate (inkl fjerntilganger, utvikler-bakdører etc)
  - Kodegjennomgang
  - Etablere sikret testmiljø (både mhp. testdata og tilgangsstyring)
  - Sikkerhetstest – både knyttet til konkrete krav rundt f.eks. inputvalidering samt inntrengings-tester og analyser av kjente svakheter/angrepsmetoder
- **Gjennomføre anskaffelser og inngå kontrakter**
  - Følge opp forhold rundt sikkerhetsoppdateringer, spesielt tredjepartskomponenter
  - Databehandleravtale
- **Overlevere produkt til linjen**
  - Nødvendige sikkerhetsrelaterte prosedyrer og –miljø er på plass (f.eks. for prosess for sikkerhetsoppdateringer, konfigurasjonskontroll)

Tillegg og utvidelser - **Avslutte**

- Komplettere restanseliste og overlevere til linjen
- Støtte til innføring av prosjektets produkter i linjeorganisasjonen
- Formell avslutning av kontrakter
- Oppdatere og lukke prosjektregnskap
- Avslutte og arkivere prosjektdokumentasjonen
- Oppdatere prosjektbegrunnelse og gevinstrealiseringsplan
- Evaluere prosjektet og utarbeide sluttrapport
- BP5

- **Avslutte og arkivere prosjektdokumentasjon**
  - Formell avslutning av kontrakter med fokus på oppfyllelse av sikkerhetskrav
  - Avslutte prosjektdokumentasjon: oppdatering av sikkerhetsrelevant informasjon.
  - Avsluttende sikkerhetsgjennomgang.
  - Etablere driftsplan for sikkerhet
- **Evaluere prosjektet og utarbeide sluttrapport**
  - Positive og negative erfaringer ifm. sikkerhetsarbeidet dokumentert for erfaringsoverføring

Tillegg og utvidelser - **Realisere**

- Overvåke og styre gevinstrealisering
- Etablere tiltaksplan for videre gevinstrealiseringstiltak
- Etterevaluering av konseptvalget
- BP6

- **Evaluering av konseptvalget**
  - I hvilken grad har sikkerhetsarbeid påvirket gevinstrealiseringen?

bouvet

RIKTIG SIKKERHET ER VINN-VINN

Risiko- og Sårbarhetsanalyser

- I tillegg til eksisterende RoS-arbeid:
  - Gjennomføringsrisiko
  - HMS/fysisk risiko

Fokus på risiko som gjør at **systemet kan medføre negativ innvirkning** på seg selv og omgivelsene, **dersom sårbarheter får ta effekt** eller **bli utnyttet gjennom angrep**.

RoS-analyser gir **grunnlag for riktig sikkerhet** basert på **verdier** og **risiko**

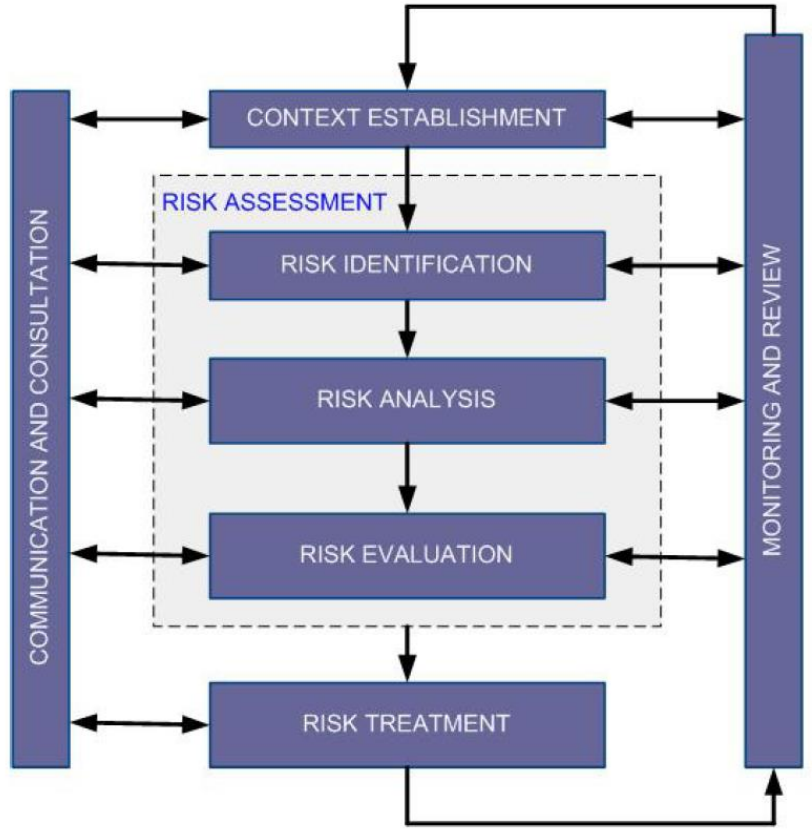
Risiko- og Sårbarhetsanalyser

- Planlegge:
  - Krav og systemskisse → **RoS** → Reviderte krav
- Gjennomføre:
  - Teknisk implementasjon → **RoS** → Forbedret løsning
- Avslutte:
  - Realisert system → **RoS** → Herdet drift

Mål for RoS-analysene

- Holde risiko på akseptabelt nivå
- Prioritere innsats

Hva kan gå galt?	Konsekvenser?	Sannsynligheter?
• Verdier • Uønskede hendelser • Sårbarheter • Trusler	• Direkte • Indirekte	• Frekvens • Evne/Kapasitet • Motivasjon/Vinning



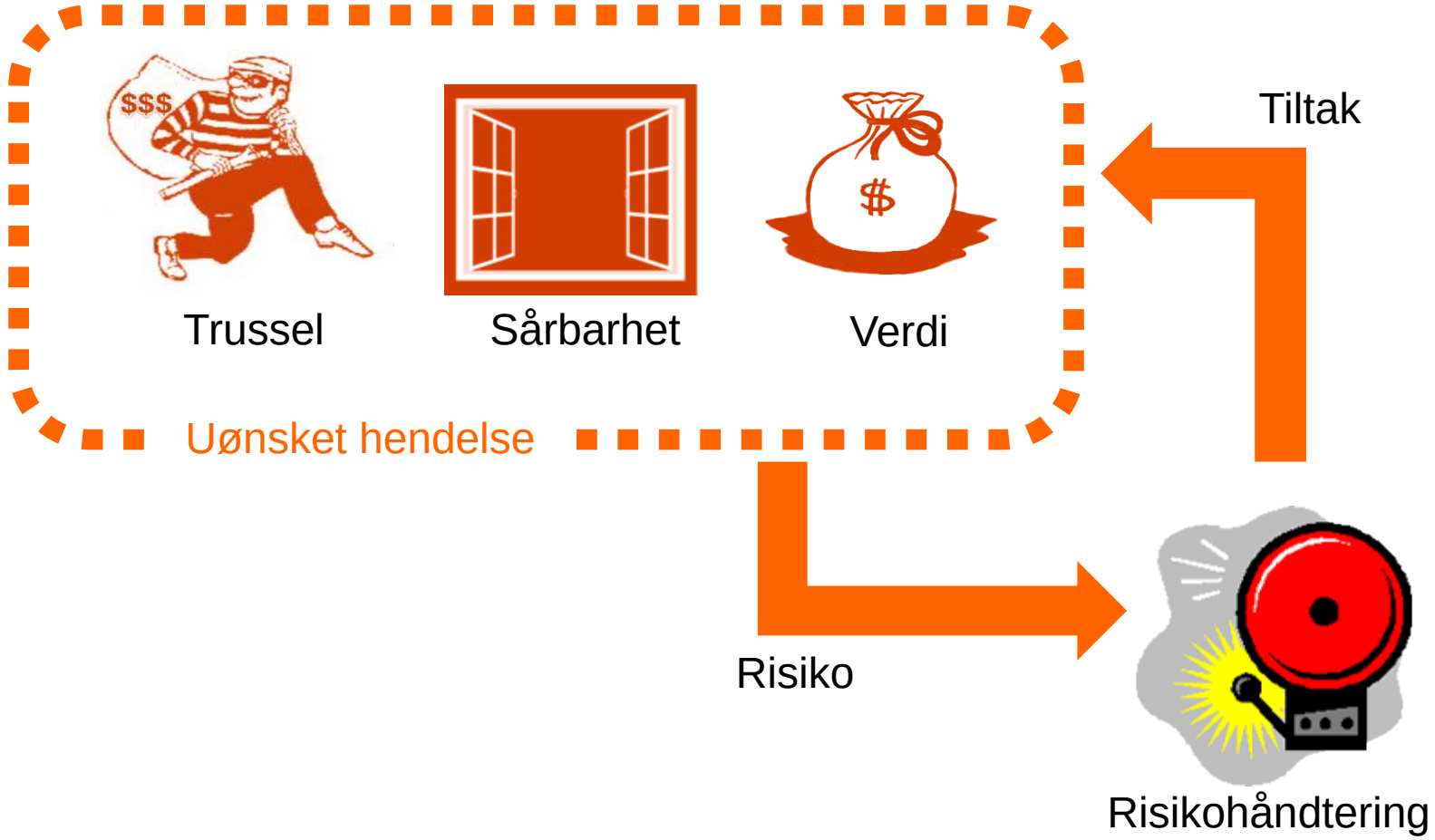
bouvet

RoS i planleggingsfasen

- Krav og systemskisse gir **tidlig oversikt over risikobildet**
  - Hvilke verdier skal beskyttes
  - Konsekvenser ved tap/skade på verdiene
  - Mulige trusler og uønskede hendelser
  - Hva er akseptabel risiko?

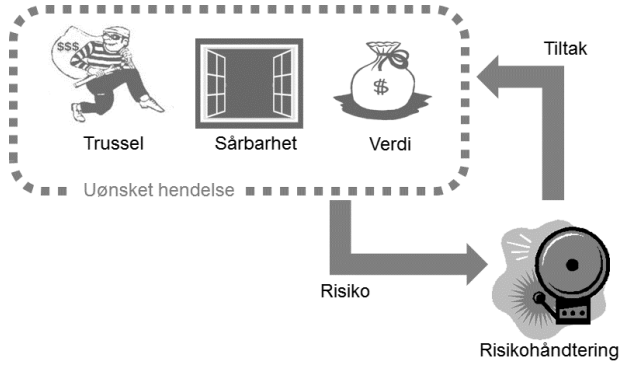
- **Styrende** for videre **arbeid med sikkerhet** i prosjektet
  - Definere sikkerhetskrav og tiltak
  - Dimensjonering av sikkerhetsmekanismer (f.eks. autentiseringsnivå)
  - Krav til sikkerhet i utviklingsprosjektet

Begreper


$$$
$
Trussel
Sårbarhet
Verdi
Uønsket hendelse
Tiltak
Risiko
Risikohåndtering

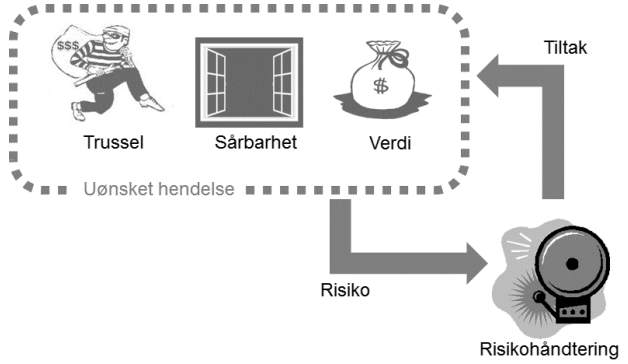
Verdier

- **Primære verdier**
  - Klassifisert basert på type (personopplysninger, sensitive personopplysninger, informasjon omfattet av sikkerhetsinstruksen, forretningshemmeligheter osv.)
  - Fra informasjonsmodelleringen
- **Sekundære verdier**
  - Autentiseringsdata, styring av tilgang, logger
  - Tjenester
  - Nødvendige for drift og operasjon
- **Indirekte verdier**
  - Økonomiske tap og tap av anseelse

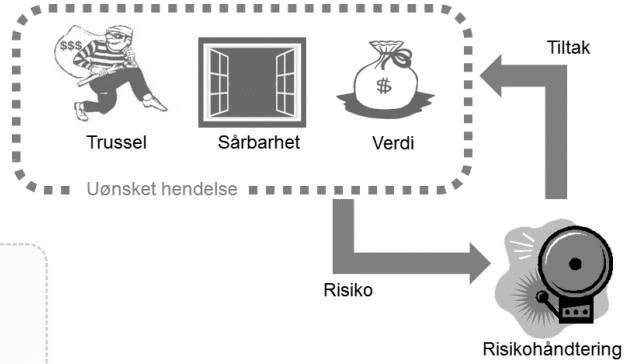


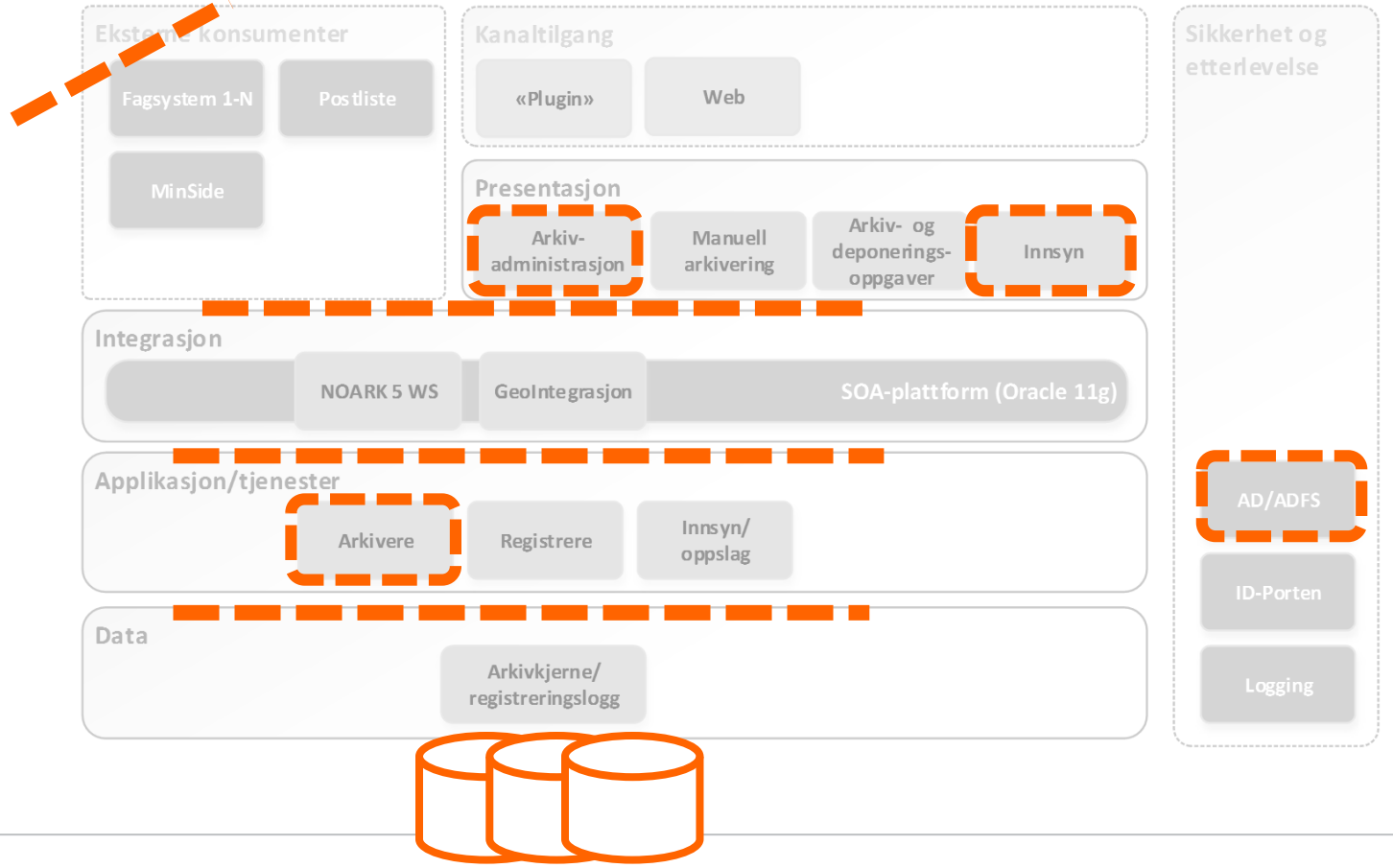
Trusler

- **Tilsiktede** handlinger (angrep/misbruk)
- **Ikke tilsiktede** handlinger (uhell/feil bruk)
- **Ikke-menneskelige feil** og hendelser (systemfeil som gir tap av integritet eller tilgjengelighet)



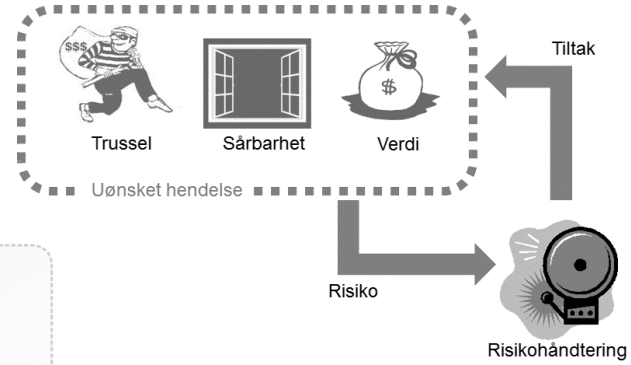
Sårbarheter





bouvet

Mulige sårbarheter



Sårbarheter i tilknyttede fagsystemer

Sårbarheter for tilsiktede uønskede hendelser fra ansatte/lovlige brukere (misbruk / utro tjenere)

Sårbarhet for utilsiktede uønskede handlinger

Sårbarheter i applikasjoner for publikumsbrukere

Sårbarheter i omkringliggende prosesser knyttet til arkivfunksjonen

Sårbarheter i omkringliggende systemer og infrastruktur

Sårbarheter i arkivsystemet

Sårbarheter i eksterne systemer for administrasjon av brukeridentitet, autentiseringsinformasjon, roller og rettigheter

Sårbarheter i sikkerhets-administrasjon

Sårbarheter i omkringliggende prosesser for drift og adminstrasjon

Sårbarheter i sikkerhets-vedlikehold

Eksterne konsumenter
- Fagsystem 1-N
- Postliste
- MinSide

Kanaltilgang
- «Plugin»
- Web

Presentasjon
- Arkiv-administrasjon
- Manuell arkivering
- Arkiv- og deponerings-oppgaver
- Innsyn

Integrasjon
- NOARK 5 WS
- GeoIntegrasjon
- m (Oracle 11g)

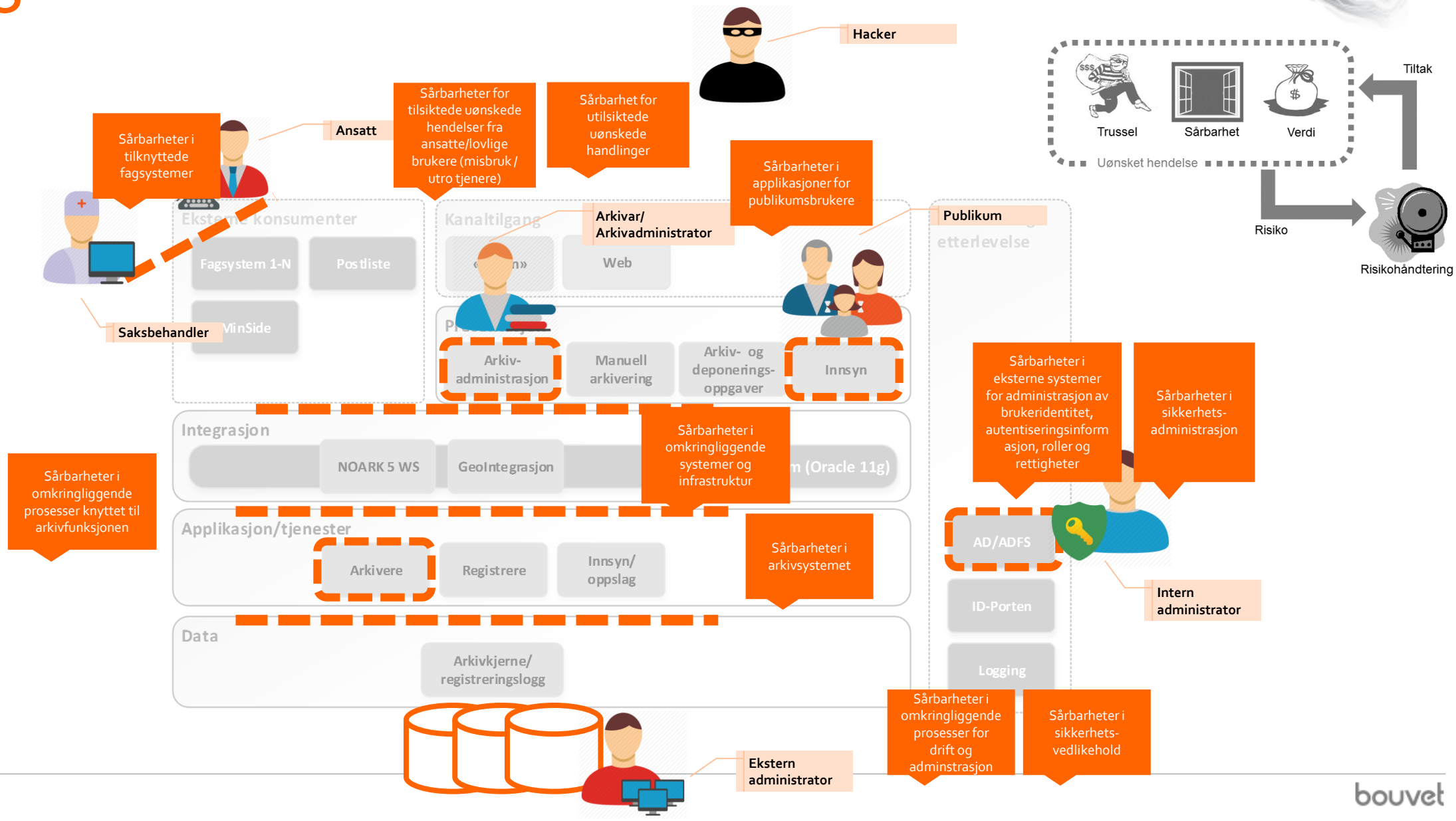
Applikasjon/tjenester
- Arkivere
- Registrere
- Innsyn/ oppslag

Data
- Arkivkjerne/ registreringslogg

Sikkerhet og etterlevelse
- AD/ADFS
- ID-Porten
- Logging

bouvet

Mulige sårbarheter



bouvet

Trusselaktører

eksempel for tilsiktede handlinger

Trusselaktør	Mål for angrep	Motivasjon	Intensjon/Vilje	Kapasitet / Evne	Historikk	Trussel-vurdering
Saksbehandlere, Arkivar Administratorer	• Konfidensiell informasjon	• Snoking	2	5	2	2
Saksbehandlere, Arkivar Administratorer	• Endre arkivinformasjon	• Personlig vinning • Hevn	1	5	1	1
Publikumsbruker	• Konfidensiell informasjon • Endring av data	• Snoking • Personlig vinning • Tilgang til skjermet informasjon	1	1	1	1
Hackere (målrettet angrep)	• Konfidensiell informasjon • Personinformasjon • Endring av data • Ødeleggelse/kidnapping av data	• Salg av informasjon, • Utpressing • Industrispionasje • Identitetstyveri, • Spredning av skadevare (malware) • Publisitet/nyhetsoppslag	3	4	2	3
Hackere (ikke målrettet)	• Installasjon av skadevare • Spredning av skadevare • Kidnapping av data • Tilgjengelighet	• Benytte kommunens maskiner som angrepsplattform (f.eks. DDoS) • Spredning av malware • Utpressing: Kidnapping/kryptering av data som frigis mot løsepenger	4	2	2	3
Terrorister	• Konfidensiell informasjon • Tilgang til systemer og nettverk	• Tilgang til informasjon som kan benyttes til terrorangrep (bygningstegninger, informasjon om kritisk infrastruktur, beredskapsplaner etc.) • Spredning av skadevare for målrettet angrep mot personer/roller i kommunen.	1	4	1	1
Fremmede stater/etterretning	• Konfidensiell/Gradert informasjon, personinformasjon	• Tilgang til gradert informasjon, bygningstegninger, personinformasjon etc. som kan være interessant for etterretning, • Industrispionasje	1	5	1	1

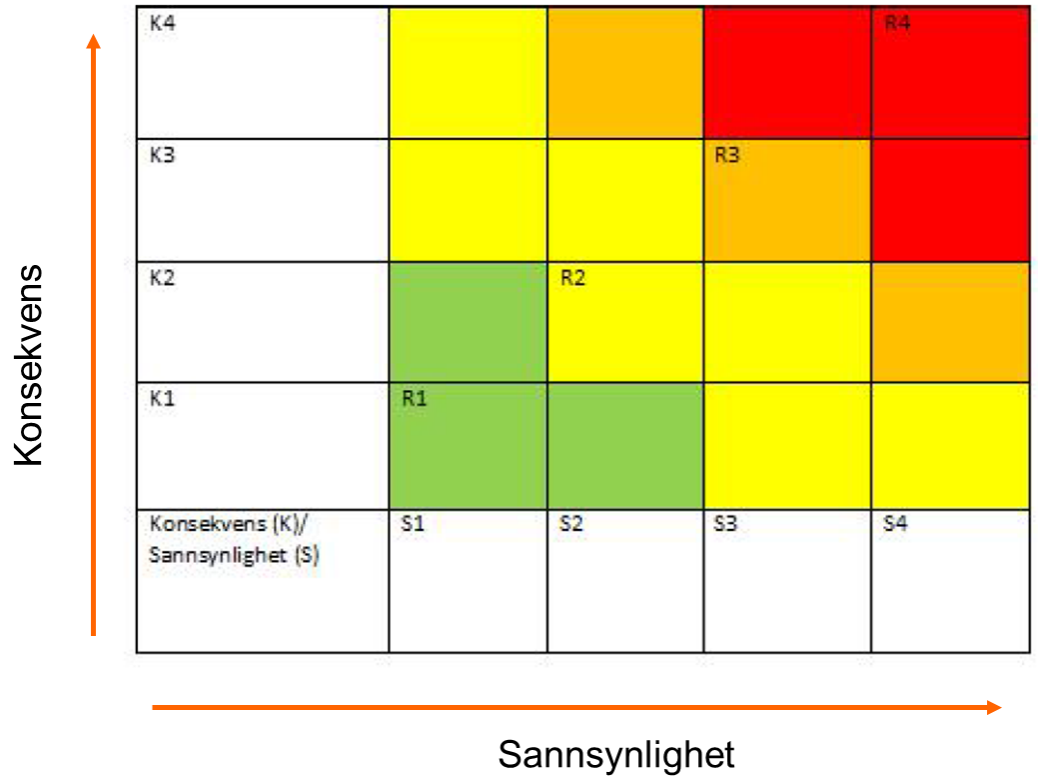
Sannsynlighet og konsekvens

	S1 Lav sannsynlighet	S2 Moderat sannsynlighet	S3 Høy sannsynlighet	S4 Svært høy sannsynlighet
Frekvens	Hendelsen inntreffer 1 gang pr. 50 år eller sjeldnere.	Hendelsen inntreffer 1 gang pr. 10 år eller sjeldnere.	Hendelsen inntreffer årlig eller sjeldnere.	Hendelsen inntreffer flere ganger pr. år.
Letthetsvurdering	Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten. Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene. Eksternt personell kan ikke omgå/bryte tiltakene.	Sikkerhetstiltak er etablert i	Sikkerhetstiltak er ikke fullt	Sikkerhetstiltak er ikke etablert
Motivasjon	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.			

	K1 Liten konsekvens	K2 Moderat konsekvens	K3 Stor konsekvens	K4 Katastrofal konsekvens
Konsekvenser for liv eller helse	Det kan ikke forekomme fare for tap av liv og/ eller helseskader	Det kan forekomme mindre helseskader	Det kan forekomme mindre helseskader	Det kan forekomme tap av liv og/ eller store helseskader
Økonomisk tap/ merarbeid/ økte kostnader	Intet økonomiske tap/ merarbeid/ økte kostnader	Det kan føre til et mindre økonomisk tap/ merarbeid/ økte kostnader	Brudd kan føre til moderat økonomisk tap/ merarbeid/ økte kostnader	Brudd kan medføre store økonomiske tap/ merarbeid/ økte kostnader
Tap av renommé (anseelse, tillit og integritet)	Ingen skade på renommé	Eventuelle skader på renommé anses bagatellmessige	Renommé kan bli noe svekket i et kortere tidsrom	Renommé kan bli svekket i et lengre tidsrom, eventuelt varig
Hindring i straffe-forfølgelse	Ingen bidrag til hindring av straffe-forfølgning	Minimalt bidrag til hindring av straffe-forfølgning	Moderat bidrag til hindring av straffe-forfølgning	Det kan forekomme hindringer i straffe-forfølgning
Uaktsomt bidrag til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Brudd kan bidra til uaktsom bistand til lovbrudd
Bryderi/ ulempe	Ingen ulempe eller bryderi	Det kan forekomme noe ulempe eller bryderi	Ikke relevant	Ikke relevant

Risikomatrisen

- Grunnlag for:
  - Definering av sikkerhetskrav og tiltak
  - Dimensjonering av sikkerhetsmekanismer (f.eks. autentiseringsnivå)
  - Krav til sikkerhet i utviklingsprosjektet



TRONDHEIM
KOMMUNE

DIGITALT
FØRSTEVALG

Trondheim Kommune – bruk av prosjektveiviseren med utvidelser

- Utarbeidet og benytter oppdaterte kvalitetskrav (ikke-funksjonelle krav) i prosjektene
  - Sikkerhetskrav (med veiledning og testbeskrivelser)
  - Sikkerhetselementer i krav for brukskvalitet, arkiv etc.
- Veiledere for kritikalitetsvurdering
- Veiledere for RoS-analyser (sikkerhetsfokus)
- Systemstøtte gjennom open-source-prosjektet «Prosjektportal for Sharepoint»

Jens Lien

jens.lien@bouvet.no

twitter.com/jenslien