IN5080
Sikkerhets- og risikostyring

Del 5b:
ISMS forvaltning

Audun Jøsang
Universitetet i Oslo
Vår 2023

Oversikt: ISMS forvaltning

- Organisasjonsstruktur rundt informasjonssikkerhet
- Program for informasjonssikkerhet
- Måling av sikkerhetstiltak
- Modenhet av sikkerhetsstyring
  - The Capability Maturity Model

Organisasjonsstruktur rundt info-sikkerhet - eksempel

Eiere / Styre

Definere informasjonssikkerhet som en strategisk prioritet.
Sette nivå for risikotoleranse
Etterse at lover, policyer og retningslinjer blir fulgt

Toppledelse

Definere sikkerhetsmålsettinger,
Etablere organisering av informasjonssikkerhet,
Godkjenne sikkerhetspolicyer, risikovurderinger og risikohåndtering

Ledere for IS og PV

CISO Chief Information Security Officer - Leder av ISU (Informasjonssikkerhetsutvalget)
CRO Chief Risk Officer (CRO)
PVO Personvernombud (PVO)
Koordinerer arbeidet med informasjonssikkerhet og personvern

ISU (IS-utvalg)

Representanter for ulike forretningsområder
Samordning og balansering av (IT-)sikkerhetsprogrammet
Utføring av risikovurderinger
Vurdering av personvernkonsekvens (DPIA)

Drift og IS/CERT-team

Planlegging, drift og evaluering av sikkerhetstiltak
Pentesting, hendelseshåndtering, rapportering

ISU - Informasjonssikkerhetsutvalg

- Å etablere et informasjonssikkerhetsutvalg (ISU) er viktig for god styring av informasjonssikkerhet.
- ISU bør ha en bred sammensetning. I tillegg til CISO, bør utvalget ha representanter fra HR, økonomi, internrevisjon, juridisk og administrasjon, og store avdelinger eller forretningsområder.
- Det bør være en formell prosess for oppnevnelse til ISU. Ethvert nytt medlem må godkjennes av adm.dir. eller annen høy leder.
- Definer utvalgets ansvar. Dette er avgjørende for å unngå at kvartalsmøtene ender som informasjonsmøter med CISO som bare forteller om siste cyberhendelser.

Oppgaver for Informasjonssikkerhetsutvalget

- Medlemmer i ISU representerer forretningsinteresser, noe som sikrer at sikkerhetsprosjekter og tiltak er strategisk tilpasset forretningsmålene.
- ISU må identifisere viktige organisatoriske spørsmål og utfordringer knyttet til informasjonssikkerhet.
- ISU lager policyer for informasjonssikkerhetsprogrammet.
- ISU utfører/støtter risikovurderinger og utformer tiltaksplaner.
- ISU initierer sikkerhetsprosjekter.

CISO konsultasjon og kommunisering

Delta på møter med ledelsen for å se forretningsmål fra deres perspektiv. Diskuter og rapporter trusler og risikoeksponering. Ha periodiske møter en-til-en. Få ledelsen til å kommunisere viktigheten av sikkerhet. → **Toppledelsen**

Delta på møter om operativ drift for å forstå utfordringer, krav og avhengigheter. Ha periodiske møter med prosesseiere. Forklar viktigheten av sikkerhet og oppnå støtte for sikkerhetsarbeidet. → **Ledere av forretningsområder**

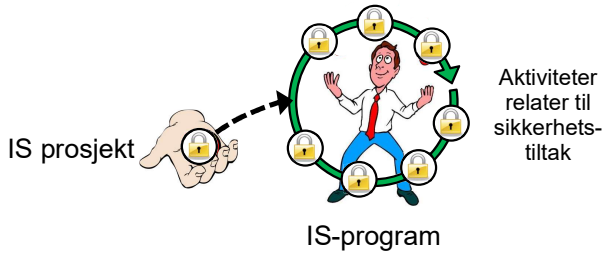
Diskuter behov og ansvar for sikkerhet og oppnå støtte i arbeidet med risikostyring. Rekrutter til informasjonsikkerhetsutvalget. → **Relevante medarbeidere**

Kommuniser og forklar behov og ansvaret for sikkerhet. Skap bevissthet og stimuler til kulturbygging rundt informasjonssikkerhet. Vær et godt eksempel. → **Alle ansatte**

Kommunisere sikkerhet til toppledelse og styre

- Fokus på:
  - Vise sammenfallende målsettinger for sikkerhet og forretningsstrategi
  - Forklare oppdatert trusselbilde og identifiserte risikoer
  - Forklare målsettinger med sikkerhetsarbeidet
  - Spesifisere budsjettposter slik at toppledelsen kan tallfeste kostnadene for sikkerhetsprogrammet
  - Tallfeste kostnader og fordeler med vanlig terminologi for eksempel ROI (Return on Investment) eller TCO (Total Cost of Ownership).
  - Identifisere potensielle konsekvenser av å ikke oppnå sikkerhetsrelaterte mål eller av mangel på samsvar med forskrifter
  - Organisere strategiseminar for informasjonssikkerhet med toppledelsen og styret.

IS-program = et sett med IS-aktiviteter



- Et IS-prosjekt skiller seg ut fra driften av sikkerhetstiltaket.
- Når prosjektet er fullført, er sikkerhetstiltaket operativt.

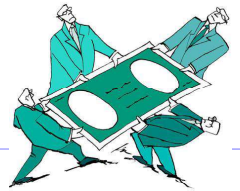
Risikoer for IS-programmet

Vær obs på risikoer i hvert sikkerhetsprosjekt og for hele sikkerhetsprogrammet:

- Uklare mål
- Dårlig motivasjon og instilling
- Mangelfull strategi
- Dårlig planlegging
- Utilstrekkelige ressurser
- Feil eller mangelfulle krav
- Feil eller mangelfull implementering
- Sabotasje

Budsjett for IS-programmet

- CISO (eller tlsv.) må kjenne budsjetteringsprosessen i organisasjonen.
- Forbered saklige argumenter og relevante caser for foreslåtte IS-prosjekter og tiltak.
- Hvert prosjekt i IS-programmet bør spesifiseres med:
  - Tidsbruk
  - Konsulentkostnader
  - Plassbehov (kontorplass, IT-utstyr)
  - Ressursbruk for testing (personell, systemtid)
  - Dokumentasjonsutvikling
  - Behov for drift og vedlikehold
  - Overhead i oppstartfasen
  - Planer ved uforutsette kostnader



Måling av sikkerhet og sikkerhetstiltak

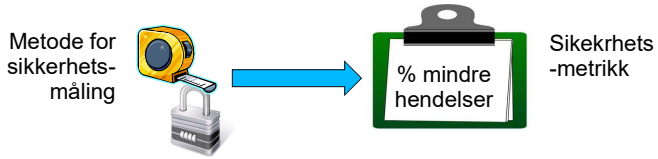
- Hva er effekten av et sikkerhetstiltak?
  - Du må måle det for å vite det.
- Måling av sikkerhet og sikkerhetstiltak gir
  - info om hvor godt sikkerhetstiltakene fungerer
  - grunnlag for å sammenligne effekten av risikostyring
  - referanse for nyttevurdering av sikkerhetsinvesteringer

Hvorfor er dette viktig: Eksempel

- **CEO spør**, *"Er vårt datanett godt nok sikret?"*
- **Uten metrikker:**
  "Vi kjøpte en dyr brannmur, så jeg antar det."
- **Med metrikker:**
  "Ja, sammenligning av statistikk for hendelser før og etter brannmurprosjektet viser dette. Antall hendelser i DMZ er redusert med 90%, og ingen hendelser i driftsnettet. Datanettet er definitivt godt sikret."

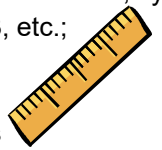
Hva er en sikkerhetsmetrikk?

- En sikkerhetsmetrikk er en parameter for en spesifikk type sikkerhetsmåling
- Å måle sikkerhet er å benytte en spesifikk metode for å innhente informasjon om effektiviteten til en tiltak eller aspekter ved ISMS
- Selv om det finnes standard sikkerhetsmetrikker, bør hver organisasjon ideelt sett tilpasse metrikker etter eget behov.



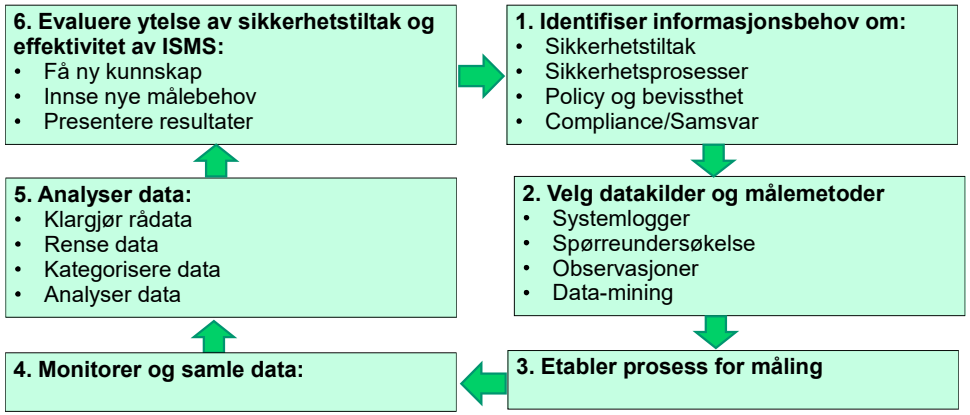
Data typer

- Kvantitative data
  - Data-parametre: f.eks. IP porter og addresser, systemnavn.
  - Ordnede data: Rekkefølge nr. 1,2,3, etc.;
  - Mengde: Hvor mye, hvor mange
  - Intervaller: Avstand, område
  - Statistisk: Prosent, avvik, konfidens

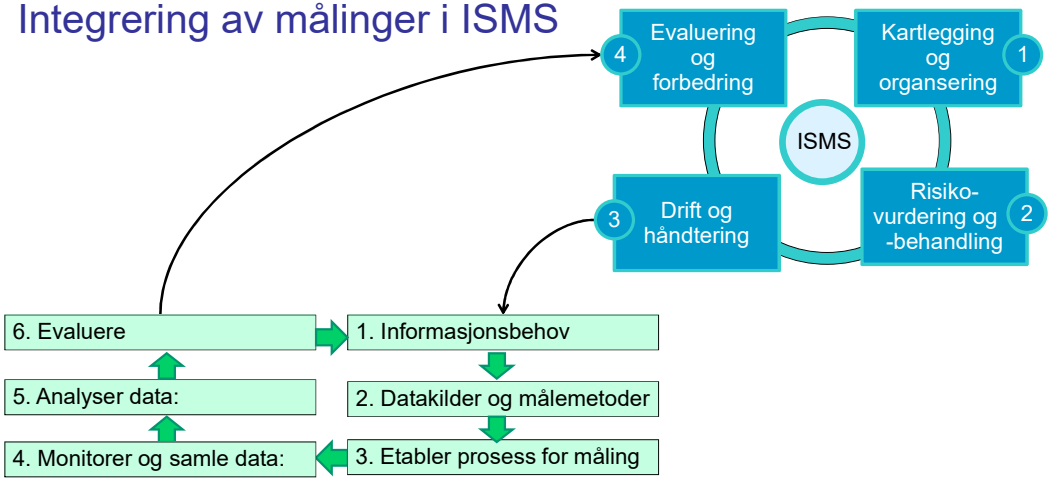


- Kvalitative data
  - Tekst
  - Utsagn
  - Kategorier
  - Multimedia

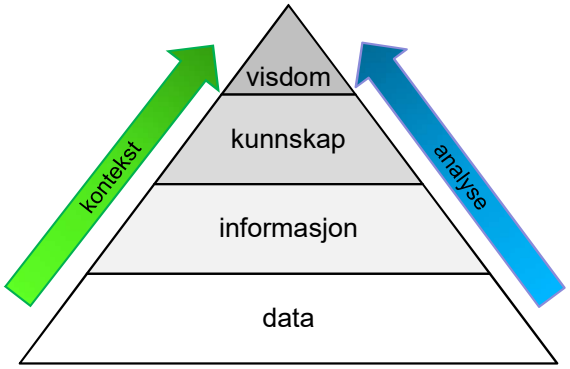
Modell for sikkerhetsmåling (ISO/IEC 27004)



Integrering av målinger i ISMS

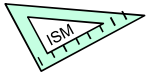


Semantiske målingsnivåer



ISM: Informasjonssikkerhetsmetrikker

- Sikkerhetsmåling deles i enkle oppgaver
- Begrenser informasjonsbehov, håndterbart i omfang
- Definerer innsats for å samle inn og analysere data
  - Personalet som trengs
  - Ressurser som trengs
  - Tid som trengs



- Få autorisasjon til å samle inn og bruke data
- Sikkerhetsmålinger kan bli gjenstand for revisjon
  - Dokumentasjon for datainnsamling og analyse
- Oppbevar data og målinger med tilstrekkelig beskyttelse

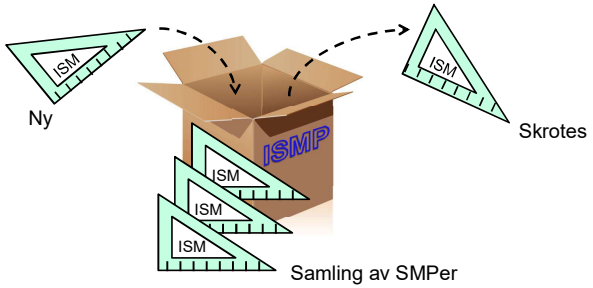
ISMP: Information Security Measurement Program

- Samling av informasjonsikkerhetsmetrikker (ISM-er)
- ISM-er er ofte relatert
  - Samme/relaterte datakilder
  - Samme/relaterte innsamlingsmetoder
  - Samme/relaterte analysemodeller
  - Resultater fra en ISM kan brukes som input til en annen ISM

- ISMP-elementer
  - Planlegging av hvert ISM
  - Katalog over ISM-er
  - Rapportering av sikkerhetstiltak og resultater
  - Vurdering av hver ISM
  - Opprettelse av nye ISM-er
  - Skroting av foreldede ISM-er

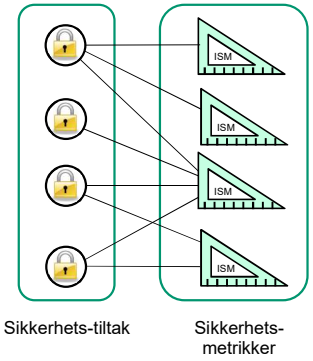
ISMP - drift

- En samling av ISM-er driftes over lange perioder
  - Gir grunnlag for trender, sammenligninger og objektiv risiko
- Utdaterte ISM-er skrotes, nye ISM-er legges til



Kartlegging mellom sikkerhetstiltak og metrikker

- Mange-til-mange-relasjoner
- Kostnadsbesparelse når en enkelt sikkerhetsmetrikk kan belyse flere sikkerhetstiltak og aspekter



Mal for sikkerhetsmetrikker

- ISO 27004 gir forslag til mal for sikkerhetsmetrikker:
  - Metrikk-ID
  - Datakilder
  - Grunnleggende datatyper
  - Avledede målinger
  - Indikator for sikkerhetstiltak
  - Beslutningskriterier
  - Måleresultater
  - Interessenter
  - Målehyppighet
- Se eksempler i ISO 27004

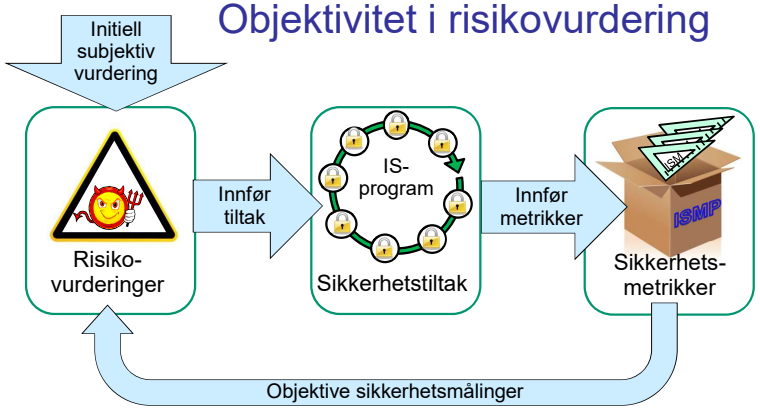
Fokusområder for sikkerhetsmetrikker

- Plattform
  - Andel webservere med kritiske sårbarheter etter skanning
- Nettverk
  - Mengde og type DMZ-portskanninger
- Hendelse
  - Antall systemer infisert med skadelig programvare XYZ
- Mennesker
  - Antall tidligere ansatte med systemtilgang
- Industri
  - Antall sikkerhetshendelser i sektoren med alvorlighetsgrad Z
- Politisk
  - Hacktivisme, antall trusselaktører som utpeker sektor / selskap ABC som potensielt angrepsmål

Målinger ⇒ Forpliktelser

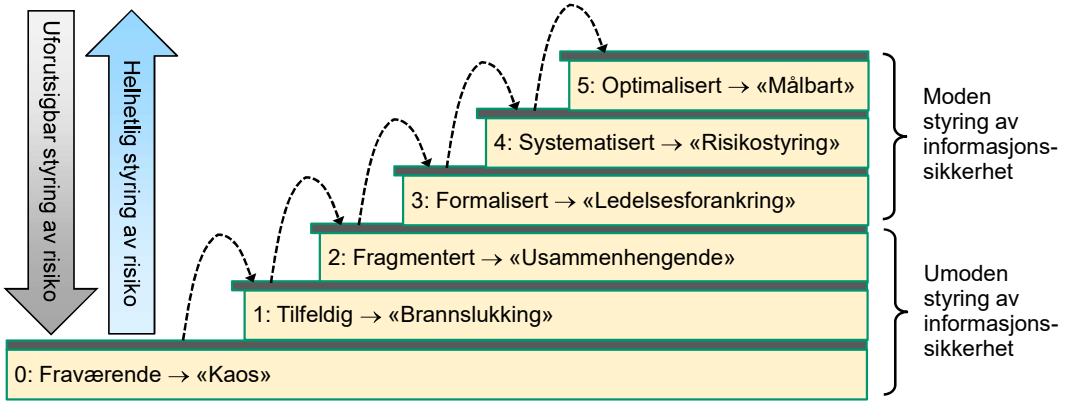
- Sikkerhetsmåling kan bli en forpliktelse
  - Kunnskap om mangler i sikkerhetstiltak skaper en forpliktelse til å gjøre noe med det.
  - Hendelser som følge av kjent – men forsømt – svakhet har ansvar
  - "Due care" -prinsippet, dvs. handle som forventet i situasjonen
- Måling uten oppfølging = sløsing med penger!
  - Bruk av sikkerhetsbudsjett i stedet for å redusere risikoen.
- Vær forberedt på oppfølging før du starter en SMP

Objektivitet i risikovurdering



- Initielle risikovurderinger er subjektive
- Risikovurderinger blir objektive når de er basert på objektive sikkerhetsmålinger.

Modenhet i styring og ledelse av informasjonssikkerhet
CMMI – Capability Maturity Model Integration



Slutt på presentasjonen