IN1030
Systemer, krav og konsekvenser

Krav om informasjonssikkerhet

Audun Jøsang
Institutt for Informatikk
Universitetet i Oslo
21. april 2021

Sikkerhet i IT-utdanningen

Krystallklare signaler fra myndighetene

… men det har ikke alltid vært slik

15.08.2014

COMPUTERWORLD

Helse Olje/energi Bygg/anlegg Offentlig it Fintech

COMPUTERWORLD | PC WORLD | MACWORLD | ITBRANSJEN | TELECOM REVY | EVENT | WHITEPAPER | STILLING LEDIG

Senior Architect, Network Services

SOCO Fullstutvikler

Aller Head of UX & Design

Audun Jøsang

Cybersikkerhet starter med it-utdanningen

Endret visjon om IT-sikkerhet i utdanningen

2014

SAK (Samarbeid, Arbeidsdeling og Konsentrasjon)

IT-sikkerhet skal bare undervises ved ett eneste lærested !

2019

Nasjonal strategi for digital sikkerhetskompetanse 2019

Digital sikkerhet skal undervises overalt !

Grunnleggende begreper for informasjonssikkerhet

God og dårlig oversettelse

Engelsk	Norsk	
• Security →	• Sikkerhet	 *God*
• Safety →	• Trygghet	
• Certainty →	• Visshet	
• Security • Safety • Certainty →	• Sikkerhet	 *Dårlig*

Hva er sikkerhet ?

Sikkerhet er beskyttelse av verdier mot skade

eiendom, infrastruktur, demokrati, lov og orden, liv og helse, miljø, informasjon, persondata








- **Fysisk sikkerhet:** hindre innbrudd og tyveri
- **Samfunnssikkerhet:** opprettholde funksjonalitet i kritiske infrastrukturer
- **Nasjonal sikkerhet:** demokrati, politisk stabilitet, territorial integritet
- **Sivil sikkerhet og rettssikkerhet:** opprettholdelse av lov og orden
- **Trygghet (safety) – sikkerhet for liv og helse:** beskyttelse av liv og helse
- **Miljøsikkerhet:** hindre forurensing og fremmede arter
- **Informasjonssikkerhet:** beskyttelse av informasjonsverdier
- **Personvern:** følge prinsipper for innhenting, lagring, behandling og deling av personopplysninger

Hva er *informasjonssikkerhet* ?

- *Informasjonssikkerhet* er å beskytte *informasjonsverdier* mot skade.
- Hvilke informasjonsverdier skal beskyttes?
  - Eksempel: data, programvare, konfigureringer, utstyr og infrastruktur
- Hvordan kan informasjonsverdier skades?
  - Brudd på et eller flere av sikkerhetsmålene Konfidensialitet, Integritet og Integritet (KIT)
- Dekker både tilsiktet og utilsiktet skade
  - Trusselaktører kan være mennesker eller naturlige hendelser
  - Mennesker kan gjøre skade både tilsiktet og utilsiktet
- Definisjon av informasjonssikkerhet:
  - ***Beskyttelse av informasjonens Konfidensialitet, Integritet og Tilgjengelighet.***

    I tillegg kan andre egenskaper, f.eks. autentisitet, sporbarhet, uavviselighet og pålitelighet omfattes. (ISO 27000:2018)

Hva skal barnet hete?

- **Informasjonssikkerhet:** generelt begrep, dekker f.eks. også beskyttelse av informasjon på papir, populært fra 1970-tallet.
- **Datasikkerhet:** kan tolkes som beskyttelse av data, men også systemer, populært fra 1980-tallet.
- **IT-sikkerhet:** tolkes som sikkerhet i IT-systemer, populært fra 1990-tallet.
- **Cybersikkerhet:** tolkes ofte som sikkerhet for alt som har å gjøre med Internett og som er koblet til Internett, populært fra 2010-tallet.
- **Digital sikkerhet:** skapt av norske myndigheter i 2019, med hensikt å være et samlebegrep for alle begrepene ovenfor, rimer godt med «digitalisering» og ser ut til å bli populært fremover.

- «Informasjonssikkerhet» er brukt jevnlig gjennom hele denne perioden. Dessuten er «informasjonssikkerhet» en direkte oversettelse av det engelske «information security» som samtidig er nedfelt i en rekke internasjonale standarder og rammeverk.

Kilder til krav om informasjonssikkerhet

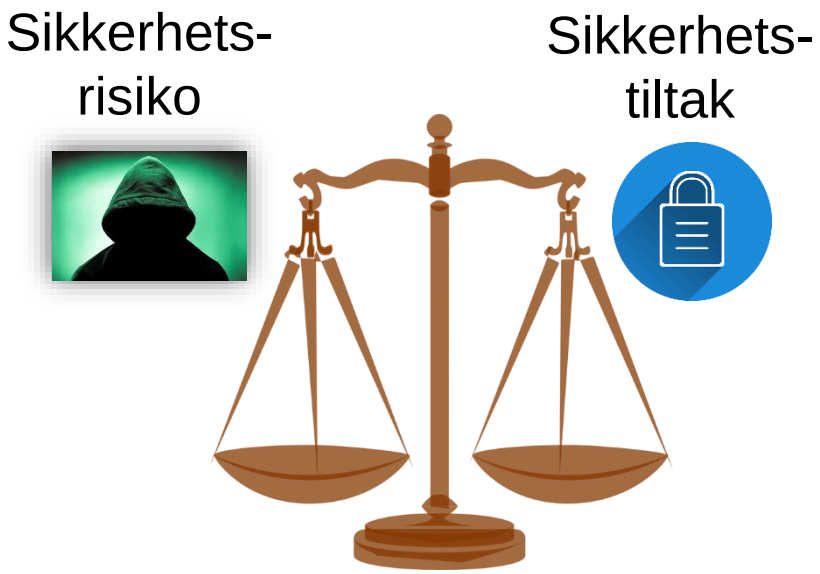
- Juridiske, lovbestemte, regulatoriske og kontraktsmessige krav til informasjonssikkerhet, f.eks,:
  - Sikkerhetsloven setter en rekke krav om sikkerhetstiltak for de som er underlagt loven.
  - GDPR setter krav om beskyttelse av persondata.

- Krav om adekvat sikkerhet i forretningsprosesser i henhold til vanlig praksis og god forvaltning.
  - Vanlig praksis setter f.eks. krav om brukerautentisering og tilgangskontroll.

- Krav om å begrense sikkerhetsrisiko i til et akseptabelt nivå. Tiltak for dette formål identifiseres gjennom sikkerhetsrisikovurdering og risikobehandling.
  - Risikovurdering kan f.eks. sette krav om 2-faktorautentisering

Målsetting for styring av informasjonssikkerhet

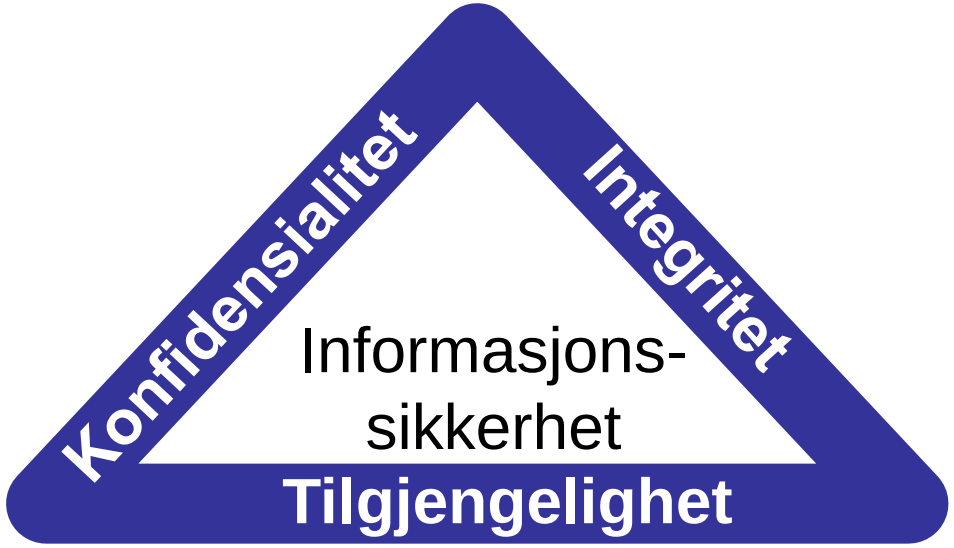
- Ville det være mulig å løse alle sikkerhetsproblemer?
- Nei, fordi:
  - Det oppdages stadig nye sårbarheter i gamle systemer
  - Nye digitale tjenester, ofte med sårbarheter, eksponeres online
  - Trusselaktører er flinke til å finne sårbarheter som kan utnyttes
  - Det utvikles stadig mer effektive angrepsverktøy
  - Økende antall og alvorlighet av trusler
- Konklusjon: Informasjonssikkerhet er en kontinuerlig prosess for å stoppe trusler og fjerne sårbarheter
- Målsetting for styring av informasjonssikkerhet er å oppnå god balanse mellom sikkerhetsrisiko og sikkerhetstiltak.



Generelle sikkerhetsmål: KIT+P

- Informasjonssikkerhet er tradisjonelt definert som opprettholdelse av KIT:

- Engelsk: CIA
  - **Confidentiality**
  - **Integrity**
  - **Availability:**



- Person(opplysnings)vern (data protection) er et tilleggsmål som bl.a. forutsetter KIT. GDPR (General Data Protection Regulation) definerer krav til personvern.

Personvern

Konfidensialitet

- Egenskapen av at informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.
  (ISO/IEC 27000)
- Trusler:
  - Datatyveri (ekstern trussel)
  - Datalekkasje (intern trussel).
- Sikkerhetstiltak eksempler:
  - Kryptering,
  - Kryptografiske kommunikasjonsprotokoller, f.eks. TLS
  - Autentisering og tilgangskontroll,
  - Anonymisering, f.eks. gjennom pseudonym eller VPN
  - Skallsikring
  - Sikkerhetskultur, bevissthet
  - …

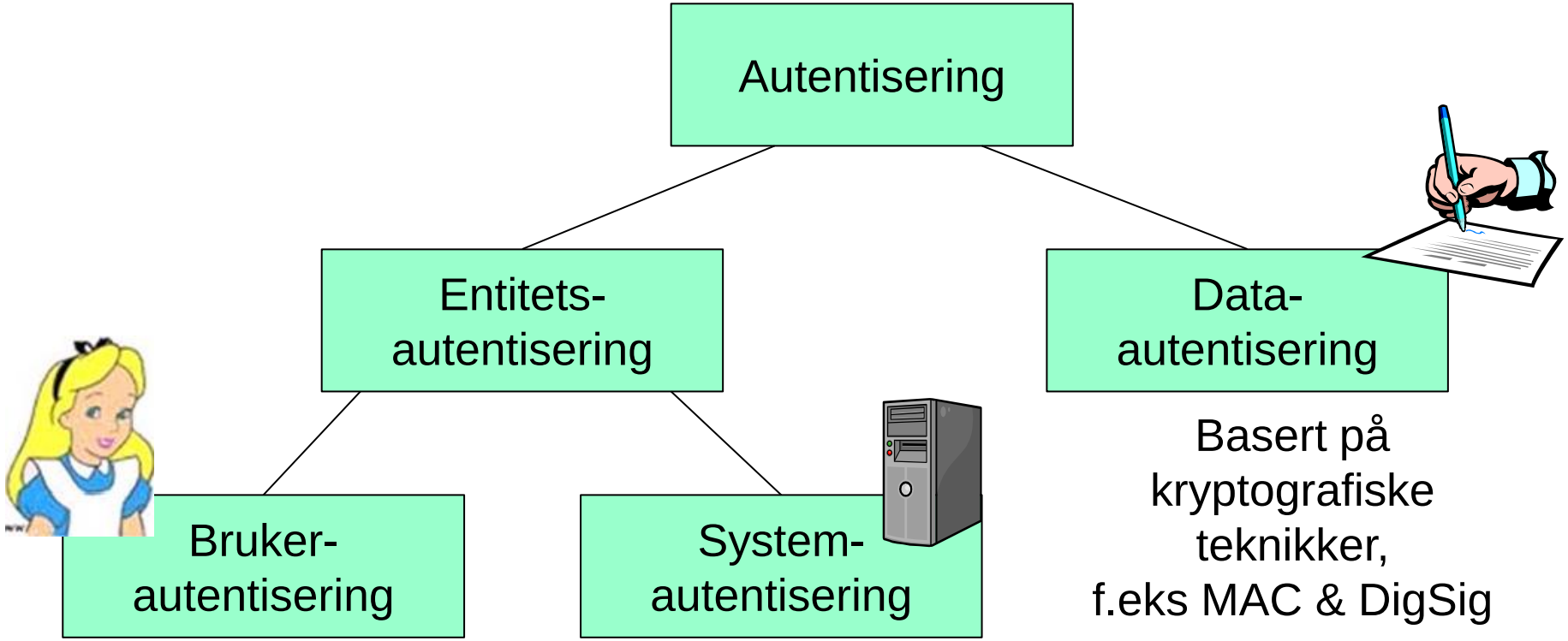
Integritet

- **Dataintegritet:** Egenskapen av at data ikke har blitt endret eller slettet på en uautorisert måte. (X.800)
- **Systemintegritet:** Egenskapen av å opprettholde korrekthet og kompletthet av dataressurser (ISO/IEC 27000)
- Trusler: Ødelagte data og miskonfigurerte systemer
- Sikkerhetstiltak eksempler:
  - Hashing, MAC, kryptering
  - Konfigurasjonsstyring
  - Endringsledelse
  - Autentisering
  - Tilgangskontroll
  - Sertifisert programvare
  - Sikkerhetskultur, bevissthet
  - …

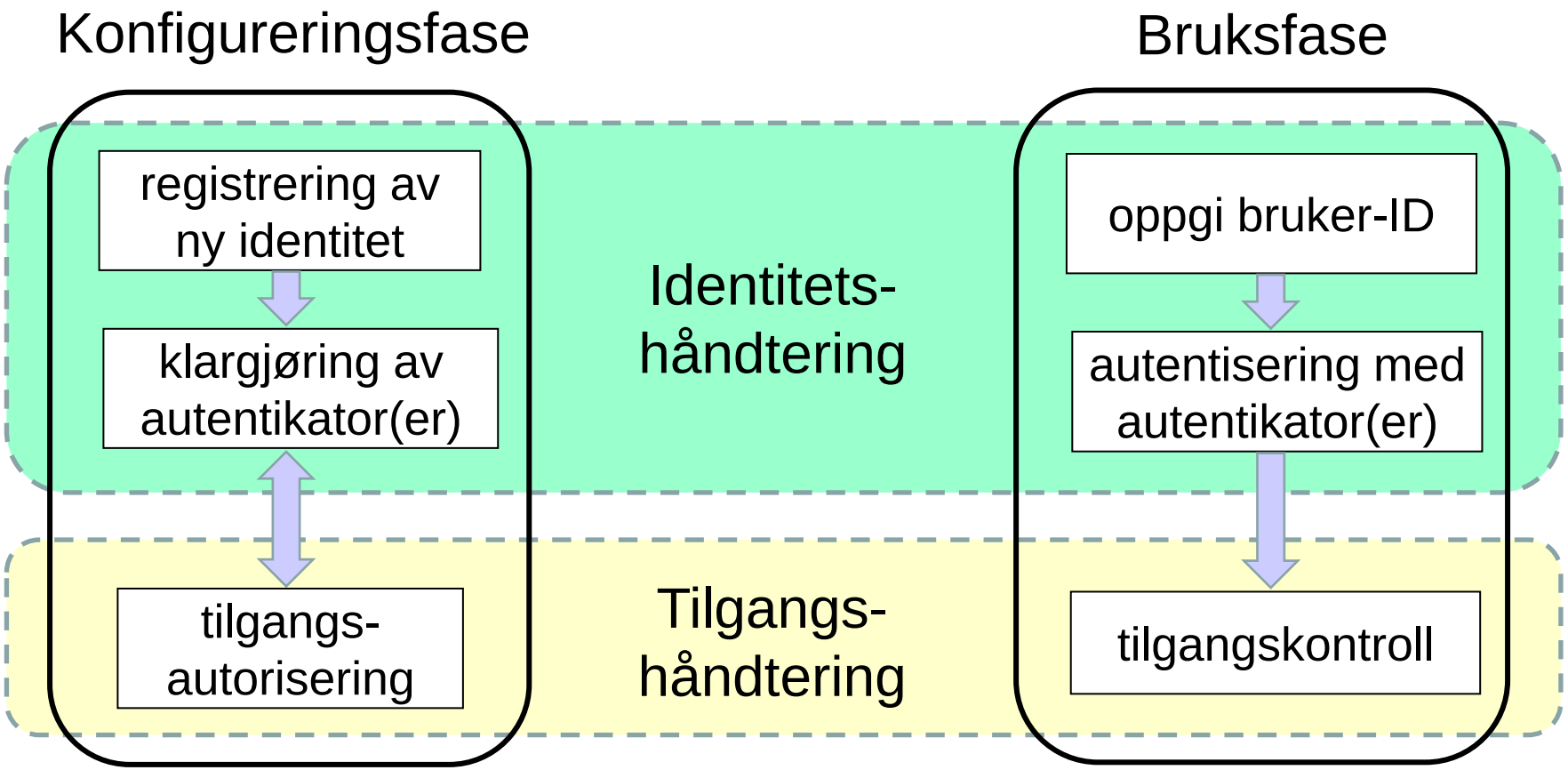
Tilgjengelighet

- Egenskapen av at data og tjenester er tilgjengelige og anvendbare ved forespørsel fra en autorisert entitet. (ISO/IEC 27000)
- Trusler:
  - Tjenestenekt (DoS / DDoS)
  - Løsepengevirus
  - Forsinkelse av tidskritiske funksjoner.
- Sikkerhetstiltak eksempler:
  - Redundans av ressurser,
  - Failover-konfigurasjon
  - Brannmur
  - Sikkerhetskopiering (backup)
  - Hendelsesrespons og beredskap,

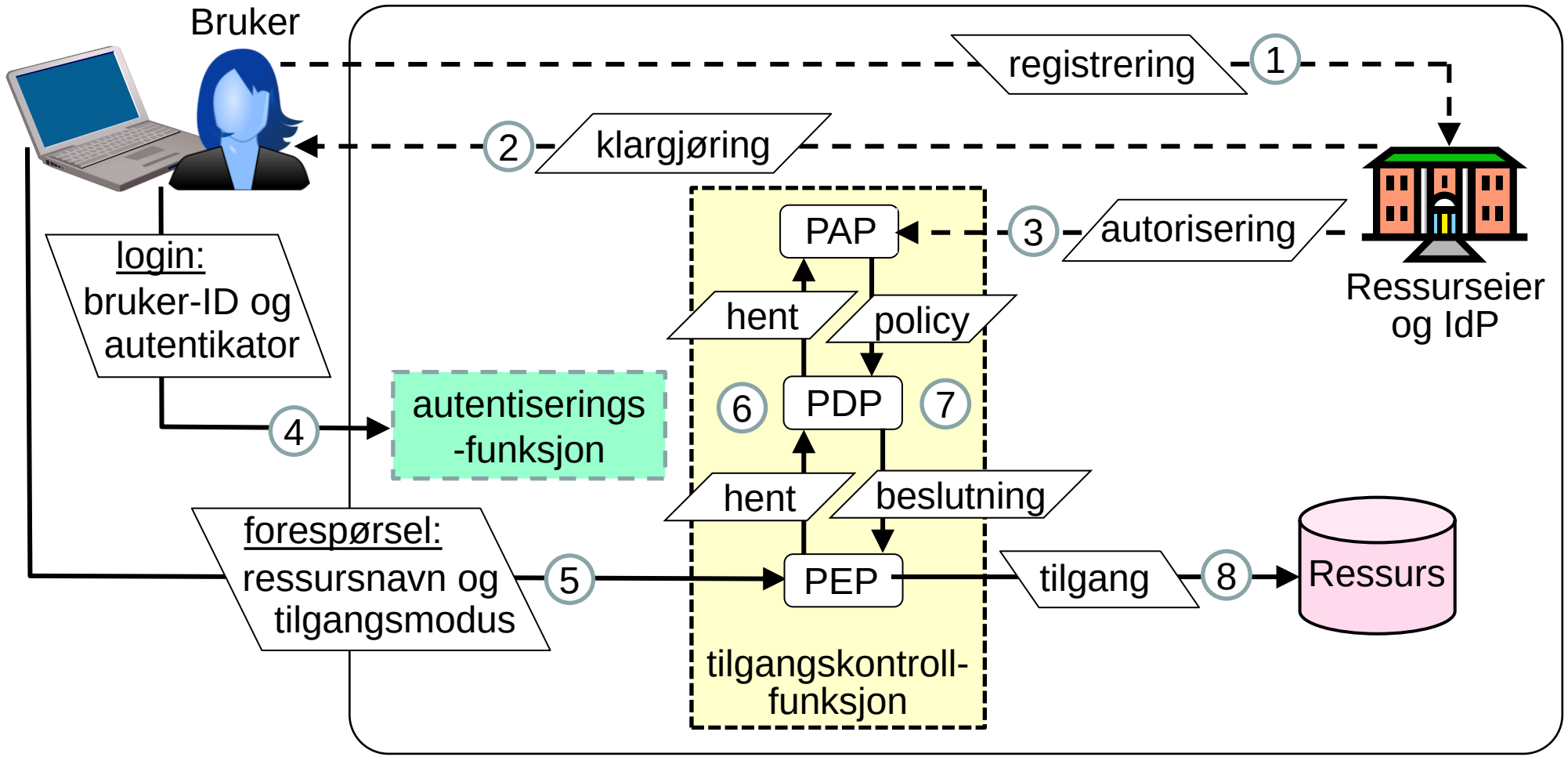
Typer av autentisering



Identitets- og tilgangshåndtering
IAM
Identity and Access Management



IAM scenario



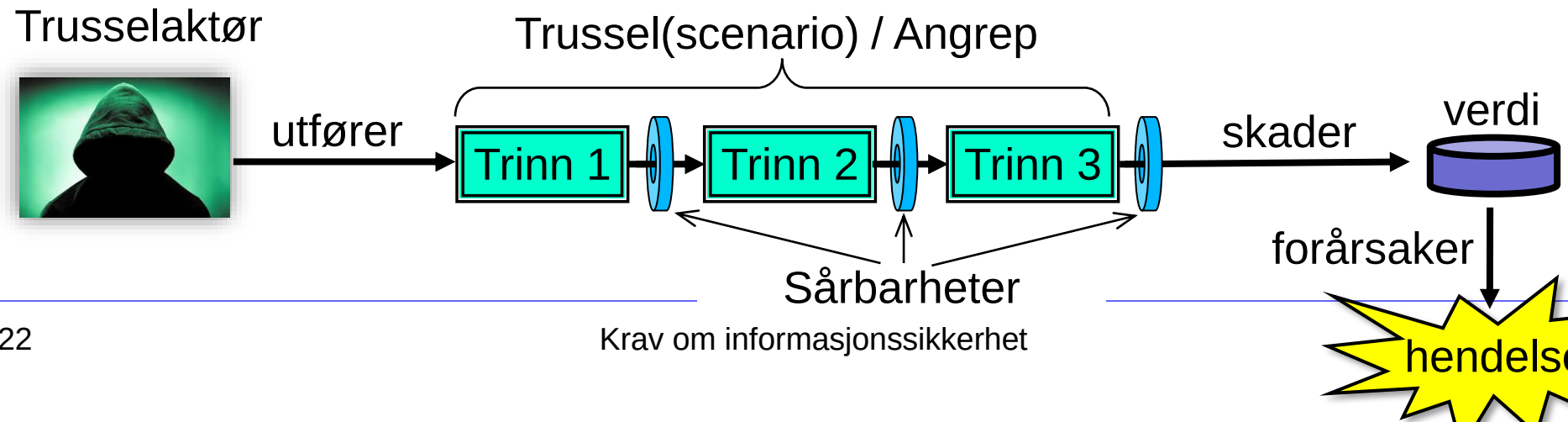
PAP: Policy Administration Point
PDP: Policy Decision Point
PEP: Policy Enforcement Point
IdP: Identity Provider
konfigureringsfase
bruksfase

Trusler, sårbarheter, risiko og sikkerhetstiltak

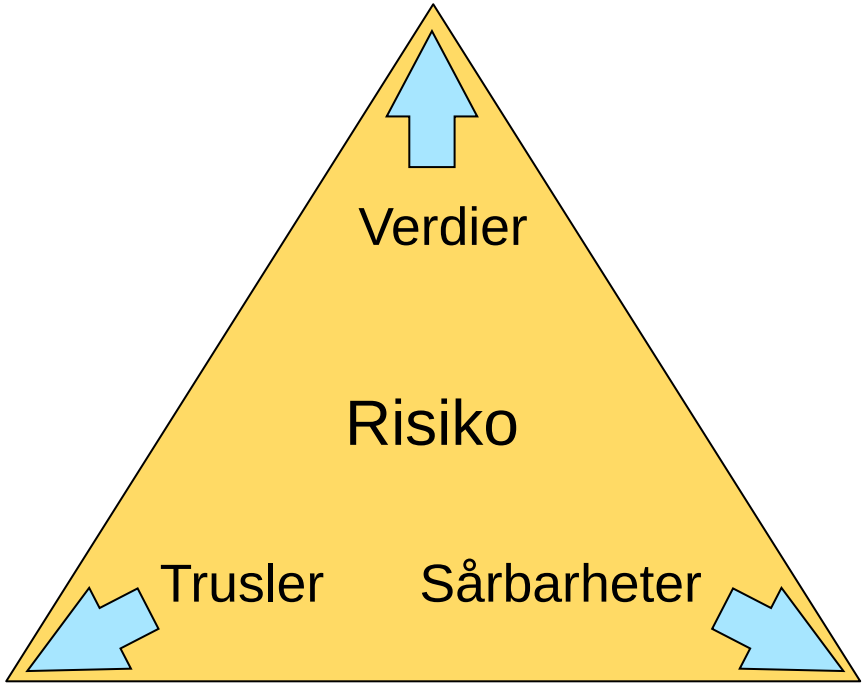
Verdier, Trusler, Sårbarheter og Tiltak

- **Verdier:** (Informasjons)ressurser som er av verdi for organisasjonen.
  - Data, systemer, applikasjoner, nettverk, enheter, tjenester, mennesker

    Mål for informasjonssikkerhet er å beskytte verdienes KIT, avhengig av behov.
  - Person(opplysnings)vern
- **Trussel:** Et potensielt angrepsscenario som kontrolleres av en trusselaktør, som kan skade organisasjonens verdier
- **Sårbarhet:** Mangel på sikkerhetstiltak mot trusler.
- **Sikkerhetstiltak** (Security Control): Metode for å forhindre trusler eller redusere konsekvenser

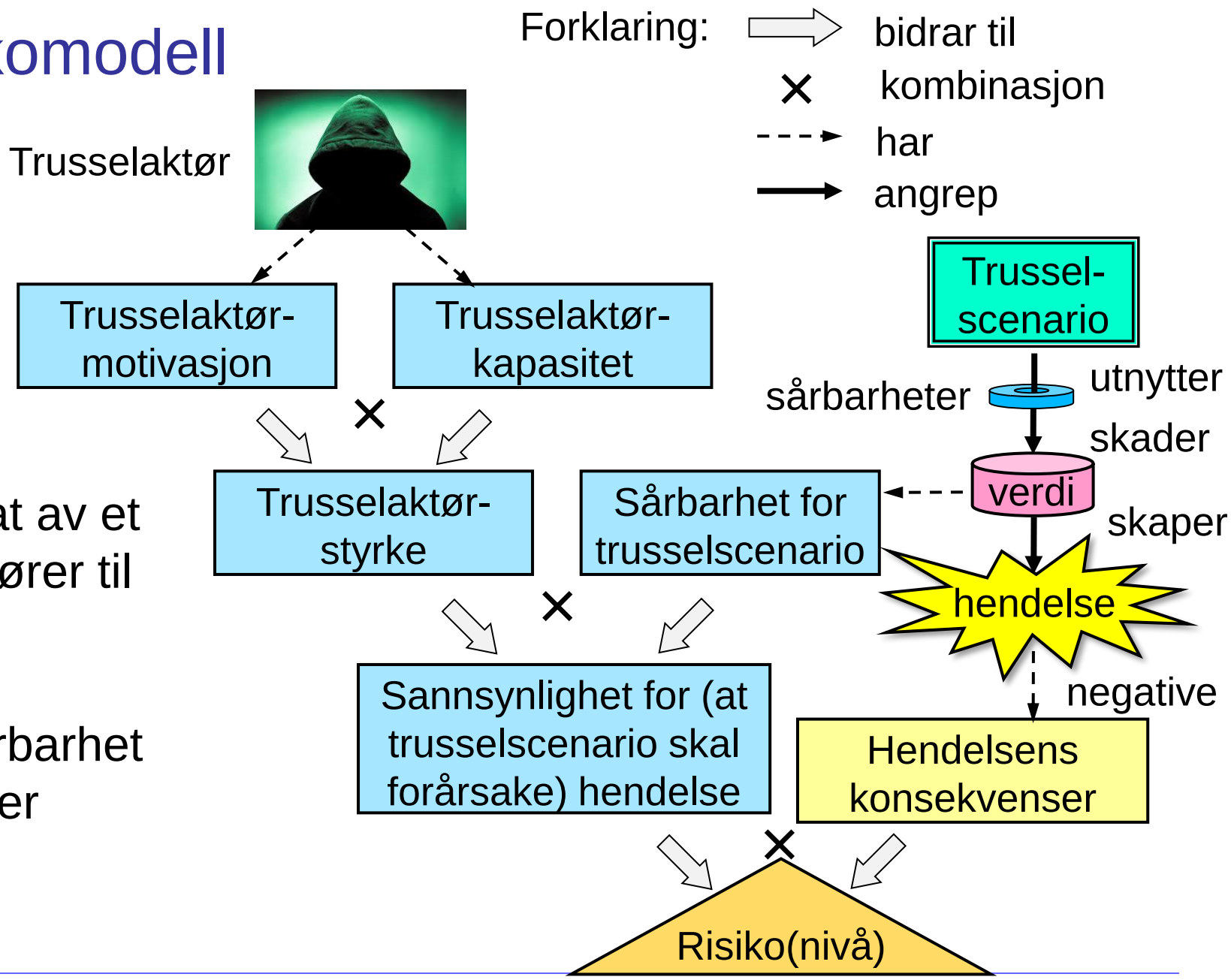


Generell risikomodell for IT-sikkerhet



- Generell modell for risiko
  - Jo større og flere verdier du har, jo større og flere trusler du er utsatt for, og jo mere sårbar du er, desto større risikoeksponering har du.

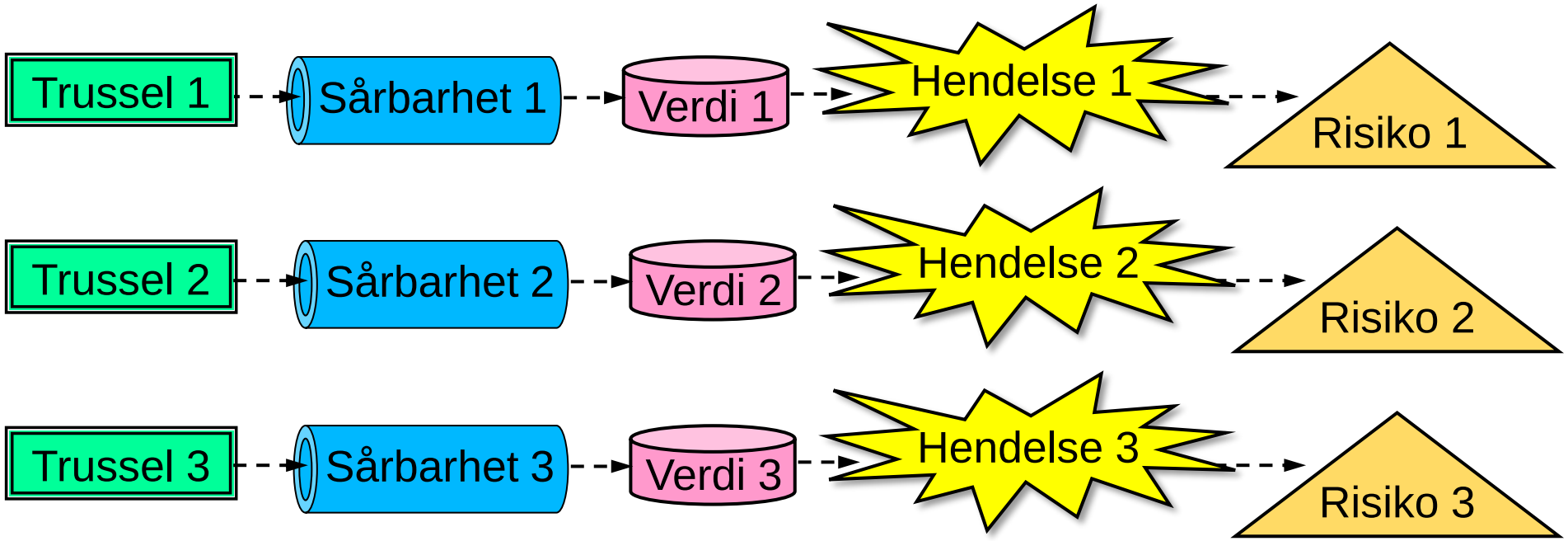
Detaljert risikomodell



- Enhver risiko er et resultat av et gitt trusselscenario som fører til en hendelse som skader verdier.
- Motivasjon, kapasitet, sårbarhet og konsekvens bestemmer risikonivået.

Mange risikoer

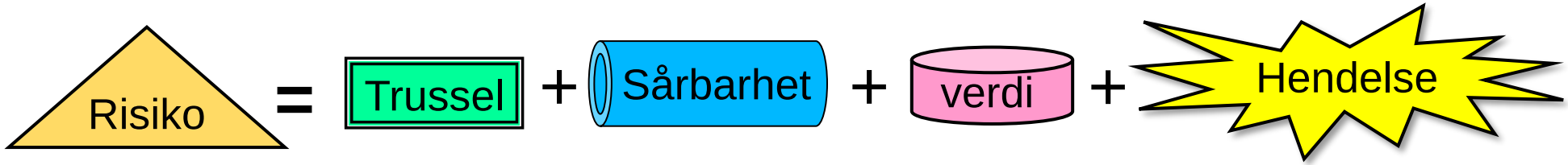
- Flere ulike trusler (scenarier) kan identifiseres
- Hver trussel kan utnytte sårbarheter og forårsake en hendelse
- Hver potensielle hendelse kan skade en verdi og ha negativ konsekvens
- Mange trusler ⇒ mange risikoer



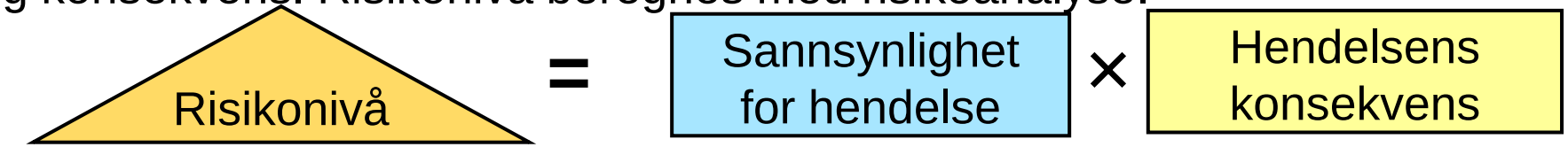
Risiko eller risikonivå?

- I dagligtale er det liten forskjell på «risiko» og «risikonivå»
  - *Hva er risikoen (risikonivået) for å bli hacket med banktrojaner?*

- På fagspråket er den en klar forskjell:
  - **Risiko** er en relevant kombinasjon av trussel / sårbarhet / hendelse som utgjør et brudd på KIT + P for en verdi. Risikoidentifisering er å kartlegge slike relevante kombinasjoner.



  - **Risikonivå** (også kalt risikoeksponering) er kombinasjonen av hendelsens sannsynlighet og konsekvens. Risikonivå beregnes med risikoanalyse.

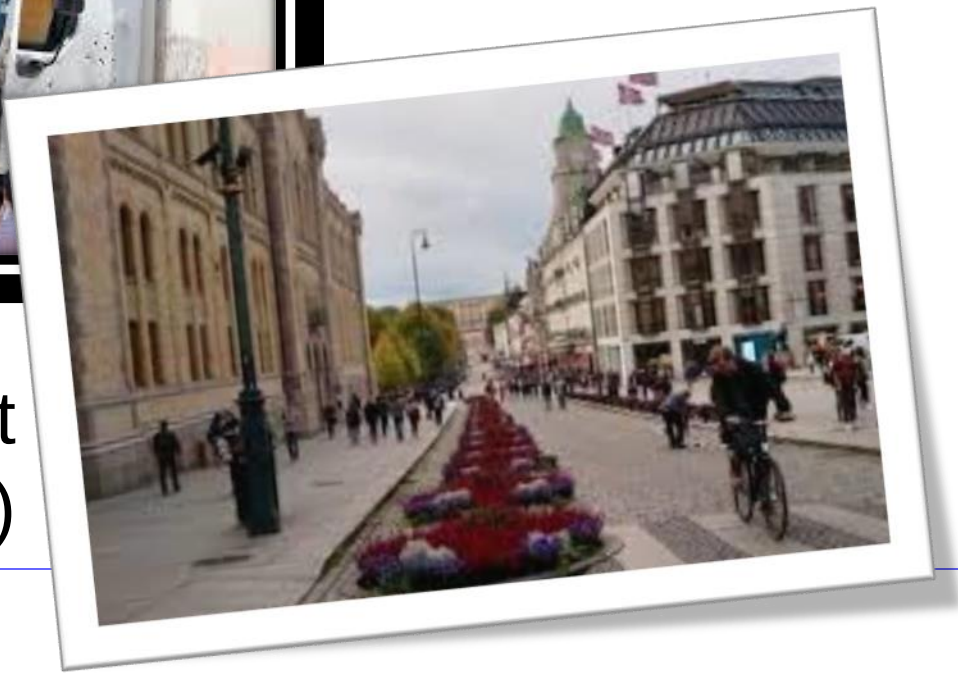


Ingen sårbarhet uten en trussel

Karl Johans gate
Oslo

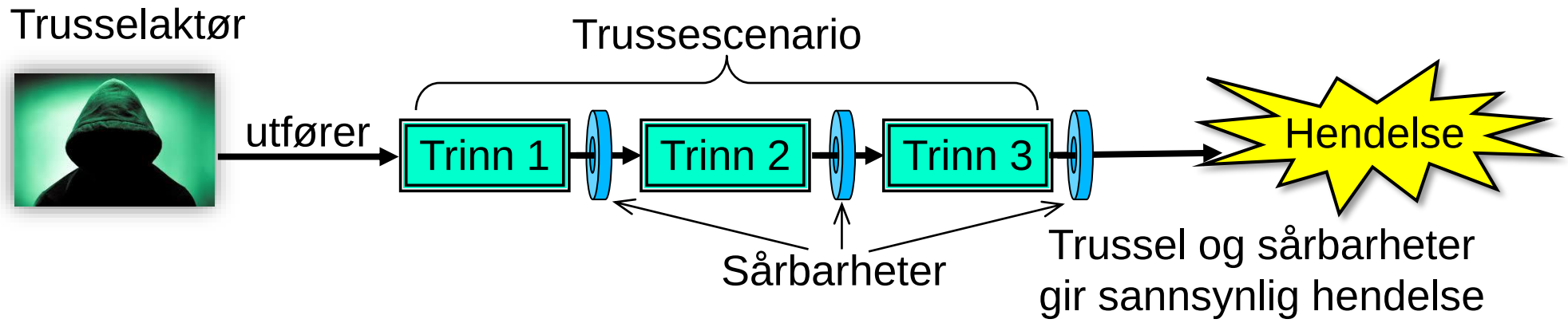
Nice
Berlin
London
Barcelona

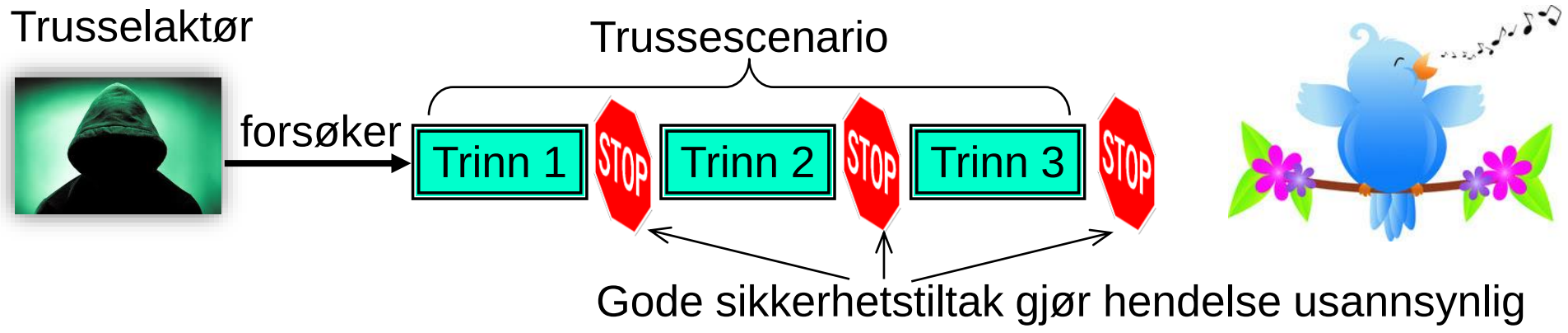
Ny trussel oppstod i 2016

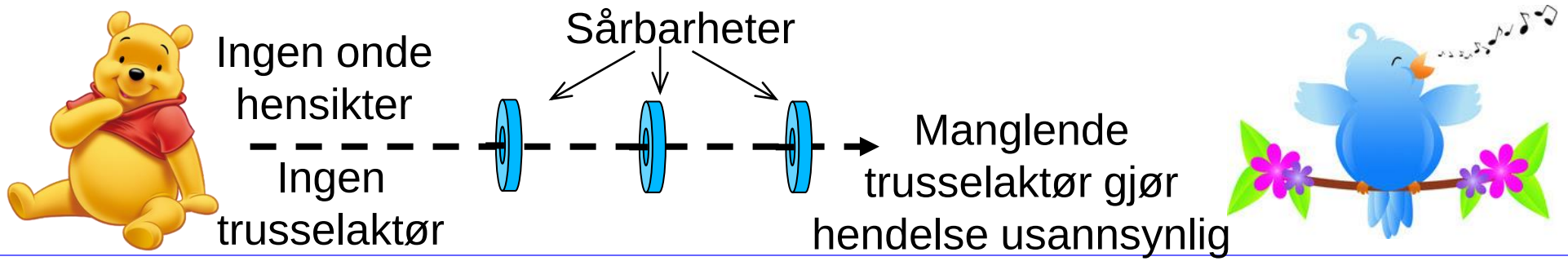


Trussel blokkert
(dvs. sårbarhet fjernet)

Sannsynlighet for at en hendelse inntreffer







Sikkerhetstmål og tiltak/controller

- Sikkerhetsmål
  - Uavhengig av spesifikk implementering
  - Kan implementers med ulike tiltak/controller
- Sikkerhetstiltak / controller / mekanismer
  - Basert på spesifikk implemntering, ofte bundet til spesifikke produkter

Sikkerhetsmål:

Konfidensialitet – Integritet – Tilgjengelighet

støtter

Sikkerhetstiltak, -mekanismer og -tjenester:

f.eks. låser – kryptering – autentisering - sikkerhetskultur

Analogi for sivil sikkerhet

Tiltak/virkemidler/controller for sikkerhet

Fysiske tiltak
- Kameraovervåking
- Adgangskontroll
- Vektere
- Låser
- Alarmer
- etc.

Tekniske/logiske tiltak
- Brukerautentisering
- Tilgangskontroll
- Systemsikkerhet
- Nettverkssikkerhet
- Kryptering
- etc.

Organisatoriske tiltak
- ISMS/Styring/Ledelse
- Policyer/Standarder
- Hendelseshåndtering
- Sikkerhetskultur
- Øvelser
- etc.

Sikkerhetstiltak – ulike faser

- Preventive tiltak:
  - Forhindre og avskrekke angrepsforsøk
    - Eksempel: kryptering av filer for konfidensialitet
- Detektive tiltak:
  - Varsle angrep som forsøkes eller som allerede er skjedd. Eksempel: Inntrengingsdeteksjon (IDS)
- Korrigerende tiltak:
  - Gjenopprette skade på dataressurser etter angrep.
    - Eksempel: Hente backup av programmer og data ved tap/kompromittering av ressurser

- Det er alltid nødvendig å benytte en kombinasjon av tiltak fra alle tre faser for å opprettholde dekkende beskyttelse.

Personopplysningsvern

Personvern i grunnloven

- § 102: Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.

Person(opplysnings)vern

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson.

Begrepet «personopplysning» er ekvivalent med persondata eller personinformasjon.

Person(opplysnings)vern er å beskytte spesifikke aspekter ved personopplysninger:

- Forhindre urettmessig innsamling og oppbevaring av personinformasjon
- Forhindre urettmessig bruk av innsamlet personinformasjon
- Sørge for at personinformasjon er korrekt
- Sørge for åpenhet og innsyn
- Sørge for adekvat informasjonssikkerhet (KIT) rundt personinformasjon
- Definere klar ansvarsfordeling

LOVDATA

Søk etter lover, forskrifter, dommer og stortingsvedtak

Rettskilder

- Lover
- Stortingsvedtak
- Sentrale forskrifter
- Lokale forskrifter
- Norsk Lovtidend
- Norges traktater
- Dommer
- Statens personalhåndbok
- Oversatte lover /

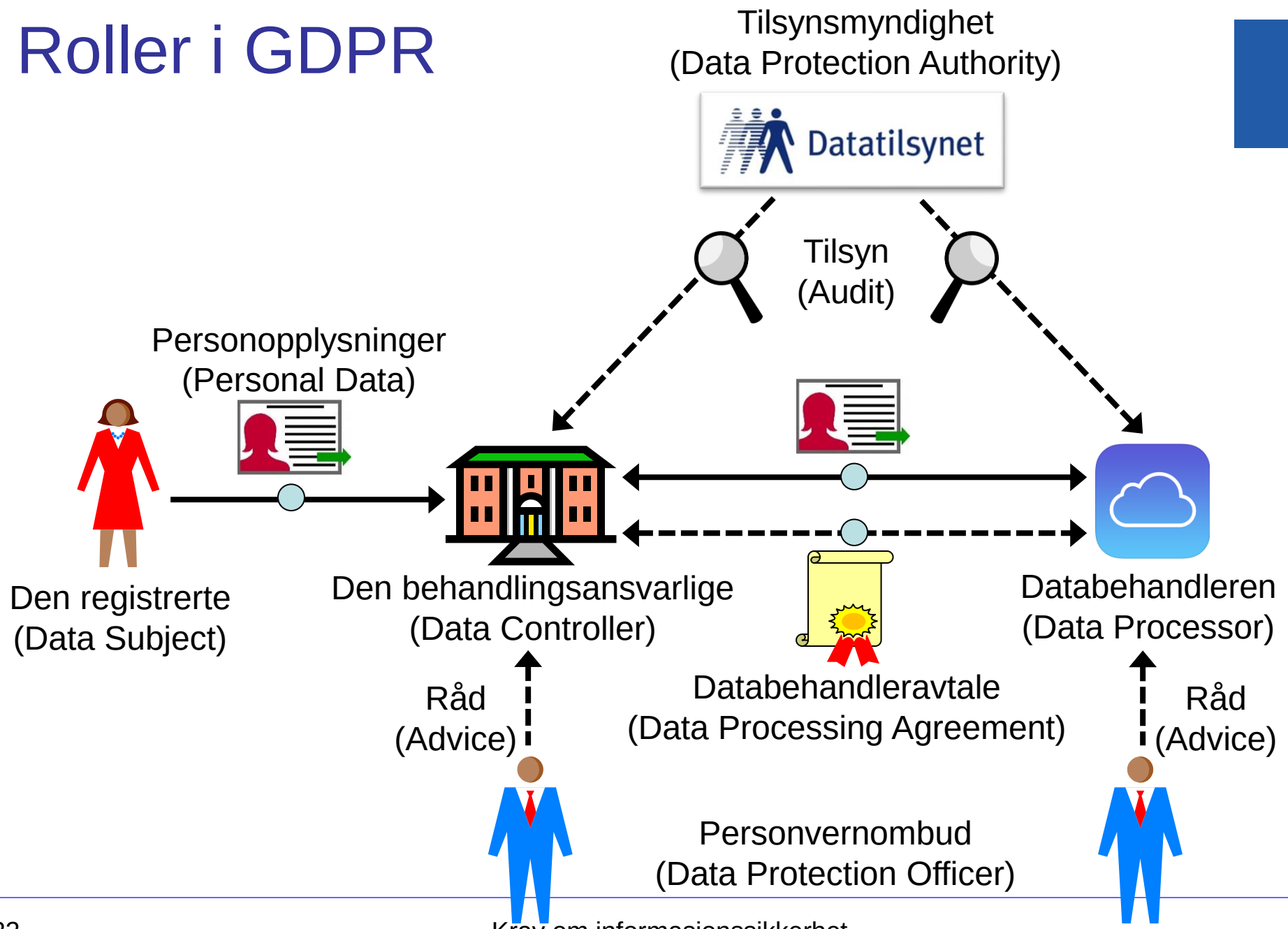
Lov om behandling av personopplysninger (personopplysningsloven)

➡ Gå til opprinnelig kunngjort versjon

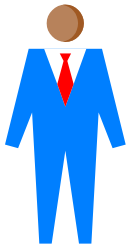
Lov om behandling av personopplysninger (personopplysningsloven)

Dato	LOV-2018-06-15-38
Departement	Justis- og beredskapsdepartementet
Sist endret	LOV-2018-12-20-116
Ikrafttredelse	20.07.2018
Endrer	LOV-2000-04-14-31
Kunngjort	15.06.2018
Rettet	11.02.2019 (GDPR art 40)
Korttittel	Personopplysningsloven

Roller i GDPR



Personvernombud



Personvernombudet gir råd til behandlingsansvarlige eller databehandleren om forpliktelser som virksomheten har etter personvernloven. Alle virksomheter kan ha personvernombud.

Personvernombud må oppnevnes når:

- Behandlingen utføres av en offentlig myndighet.
- Databehandlingen har en art, omfang og/eller formål som krever regelmessig og systematisk monitorering i stor skala.
- Behandlingsansvarliges eller databehandlerens hovedvirksomhet består av behandling i stor skala av særlige kategorier av opplysninger i henhold til artikkel 9 (sensitive personopplysninger) eller personopplysninger knyttet til straffedommer og straffbare forhold som er nevnt i artikkel 10.

To typer personvernrisiko

Hvem er trusselaktøren?

Trusselaktører:

- script kids
- hacktivisme
- organisert kriminalitet
- terrorisme
- statlige cyberoperasjoner

Trusler er f.eks.:

- brudd på KIT for personopplysninger
- tyveri og publisering av personopplysninger

→ Risikovurdering ifølge Art. 32.

Trusselaktører:

- den behandlingsansvarlige
- databehandleren

Trusler er f.eks:

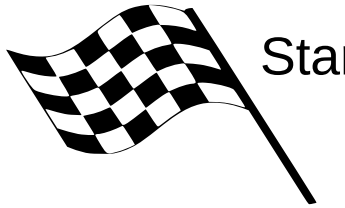
- uønsket innsamling
- urettmessig diskriminering
- re-identifisering
- lagring lenger enn nødvendig

→ DPIA ifølge Art. 35.

Mulige konsekvenser av dårlig personvern

- Personlig belastning
- Uønsket oppmerksomhet
- Forskjellsbehandling
- Identitetstyveri eller –bedrageri
- Økonomisk tap
- Skade på omdømme
- Tap av fortrolighet for taushetsbelagte personopplysninger
- Uautorisert oppheving av pseudonymisering
- Andre økonomiske eller sosiale ulemper

Prosess rundt DPIA



Start

Sannsynlighet for høy risiko? Art. 35(1),(3),(4)

JA

NEI

Unntak? Art. 35(5),(10)

JA

NEI

Ikke krav om DPIA, behandlingen kan begynne

Atferdsnormer Art. 35(8)

(codes of conduct)

Råd fra PVO Art. 35(2) PVO kontrollerer gjennomføringen Art. 39(1c)

Innhente synspunkter fra de registrerte Art. 35(9)

DPIA Art. 35(7)

Revidering ved behov, Art. 35(11)

Høy restrisiko? Art 36(1)

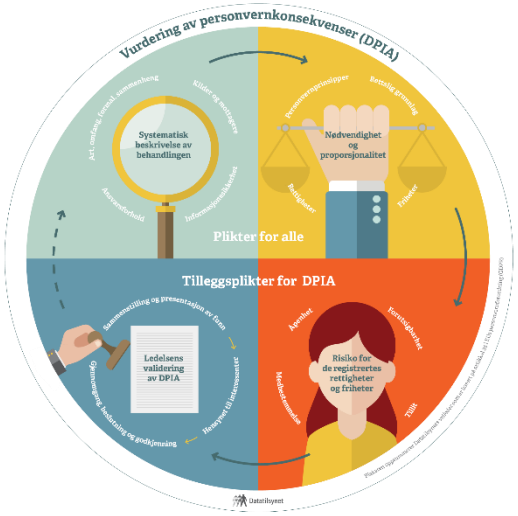
JA

NEI

Forhåndsdrøftelse med Datatilsynet

Behandlingen kan begynne

Vurdering av personvernkonsekvens DPIA (Data Protection Impact Assessment)



Trinn i DPIA-prosessen:

1. «Lag en systematisk beskrivelse av den planlagte behandlingen og formålet med behandlingen»,
2. «Foreta en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene»,
3. «Gjør en vurdering av risikoene for de registrertes rettigheter og friheter»,
4. «Spesifiser de planlagte tiltakene»:
   - «for å håndtere risikoene»,
   - «for å påvise at Personvernforordning overholdes».
5. Få ledelsens validering av DPIA.

Art. 35 (7)

General Data Protection Regulation (GDPR)

på norsk: Personvernforordningen (PVF)

- Trådte i kraft som lov i EU 25.05.2018, i Norge 20.07.2018, kalles som regel GDPR.
- Brudd på GDPR kan medføre bøter opp til €20 mill. eller 4% av omsetning.
- Håndheves av hvert lands tilsynsmyndighet, som er Datatilsynet i Norge.
- EUs lovtekst (GDPR) oversatt til norsk uten endring, 99 artikler .
- Følgende artikler presenteres her:
  - Art. 5: Prinsipper for behandling av personopplysninger
  - Art. 6: Behandlingens lovlighet (behandlingsgrunnlag)
  - Art. 25: Innebygd personvern
  - Art. 32: Sikkerhet ved behandlingen (innebygd informasjonssikkerhet)
  - Art. 35: Vurdering av personvernkonsekvens (DPIA)
  - Art. 45: Overføringer på grunnlag av en beslutning om tilstrekkelig beskyttelsesnivå
  - Art. 46: Overføringer som omfattes av nødvendige garantier
  - Art. 83: Generelle vilkår for ilegging av overtredelsesgebyr

Art. 6: Behandlingens lovlighet (behandlingsgrunnlag)

1. *Behandlingen er bare lovlig når minst ett av følgende vilkår er oppfylt:*
   - *a) den registrerte har samtykket til behandling for ett eller flere spesifikke formål,*
   - *b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,*
   - *c) behandlingen er nødvendig for å oppfylle behandlingsansvarliges rettslig forpliktelser,*
   - *d) behandlingen er nødvendig for å verne den registrertes eller andre personers vitale interesser,*
   - *e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,*
   - *f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.*

     Punkt f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver (fordi dette tilfellet dekkes av punkt e)).

Art. 45: Overføringer på grunnlag av en beslutning om tilstrekkelig beskyttelsesnivå

1. *Personopplysninger kan overføres til en tredjestat eller en internasjonal organisasjon når Kommisjonen har fastslått at tredjestaten, et territorium eller en eller flere angitte sektorer i nevnte tredjestat eller den aktuelle internasjonale organisasjonen sikrer et tilstrekkelig beskyttelsesnivå. En slik overføring skal ikke kreve en særlig godkjenning.*
2. *Ved vurderingen av om beskyttelsesnivå er tilstrekkelig skal Kommisjonen særlig ta hensyn til det følgende:*
   a) *prinsippet om rettsstaten*
   b) *om det finnes en eller flere velfungerende, uavhengige tilsynsmyndigheter i tredjestaten*
   c) *de internasjonale forpliktelsene som den berørte tredjestaten har påtatt seg*
3. *Etter å ha vurdert om beskyttelsesnivået er tilstrekkelig, kan Kommisjonen beslutte at en tredjestat sikrer et tilstrekkelig beskyttelsesnivå i henhold til nr. 2 i denne artikkel (adekvansbeslutning).*

Land som omfattes av adekvansbeslutning

- Adekvansbeslutning for en stat eller område betyr at overføringen vil være sammenlignbar med overføringer mellom land innenfor EØS.
  - gjør overflødig å definere annet overføringsgrunnlag eller godkjenning fra Datatilsynet.
- Per 2022 gjelder adekvansbeslutning for følgende land:

Andorra	Argentina	Guernsey	Isle of Man
Israel	Jersey	New Zealand	Sveits
Storbritannia	Uruguay		

- Under gitte betingelser gjelder adekvansbeslutning også for følgende land:

Canada	Færøerne	Japan	Sør-Korea

- **NB:** USA omfattes **ikke** av noen adekvansbeslutning. Den 16. juli 2020 besluttet EU-domstolen (Schrems-II-dommen) at Privacy Shield er ugyldig som overføringsgrunnlag, fordi mekanismen ikke gir tilstrekkelig beskyttelsesnivå.

Schrems-II dommen

- Max Schrems anklaget EU fordi han mente at adekvansbeslutning for USA var brudd på GDPR, fordi amerikanske myndigheter har lovlig innsyn i europeiske personopplysninger etter følgende lover:
  - FISA Section 702 (Foreign Intelligence Surveillance Act) åpner for å innhente etterretning om ikke-amerikanske personer som ikke befinner seg i USA.
  - Executive Order 12333 regulerer all amerikansk utenlandsk etterretningsvirksomhet, inkludert aktiviteter som faller utenfor FISA, f.eks. utført utenlands mot ikke-amerikanske personer. Etterretningsvirksomheten kan foregå hemmelig.
  - Presidential Policy Directive 28 åpner for masseinnhenting av (person)data for overvåking uten at berørte personer er spesifikt mistenkt eller utpekt som interessante. Dog kan innhentede data kun benyttes for nasjonal sikkerhet, og ikke f.eks. til industrispionasje.
- Pga. Schrems-II-dommen må overføringsgrunnlag til USA baseres på GDPR Art. 46 *Overføringer som omfattes av nødvendige garantier*, og den tilhørende Art. 47 *Bindende virksomhetsregler.*

Innebygd informasjonssikkerhet og personvern

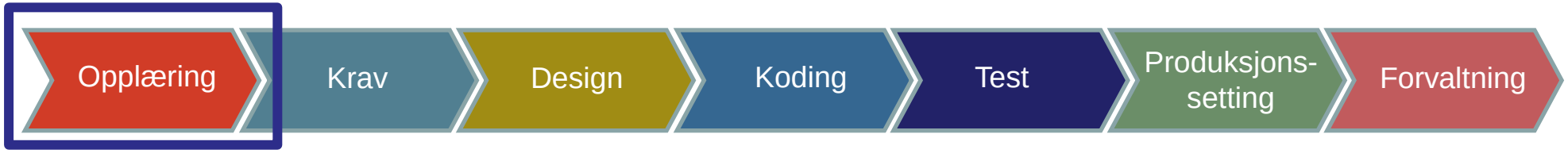
- «Innebygd» informasjonssikkerhet og personvern betyr at det tas eksplisitt hensyn til informasjonssikkerhet og personvern i hele livssyklusen til programvare og applikasjoner.
- Et viktig mål er å finne og redusere sårbarheter tidlig i utviklingsprosessen slik at det blir færre hendelser og sårbarheter å håndtere under drift.
- Microsoft så dette behovet tidlig og har vært ledende her og utviklet *Microsoft Security Development Lifecycle (SDL)*
  - Denne er nå en integrert del av programvareutviklingsprosessen hos Microsoft (og andre)
- Vi kan beskrive livssyklusen som en prosess av 7 faser:

Fase 1: Opplæring

Alle som deltar i utvikling og drift av digitale tjenester og applikasjoner skal ha basiskunnskap og forståelse for

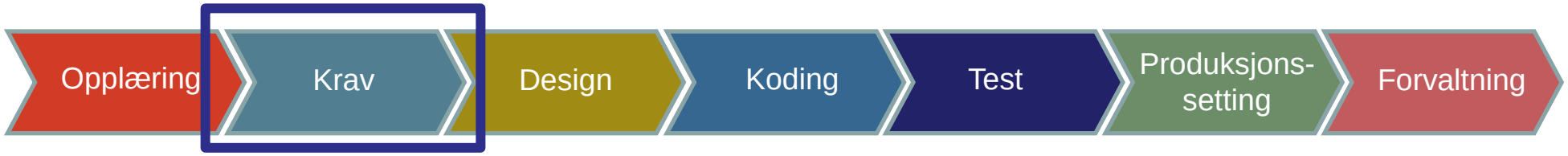
- Informasjonssikkerhet og personvern
- Risikovurderinger
- Trusselmodellering

Dette er egentlig en selvfølge. Det ville være uforsvarlig å utdanne bygningsarkitekter og ingeniører uten å gi dem kunnskap om branntrygghet, fordi arkitekter og ingeniører da ville bygget brannfeller inn i våre bygninger. På samme måte er det uforsvarlig å utdanne informatikere og dataingeniører uten obligatoriske kurs om informasjonssikkerhet, fordi de ferdigutdannede da nødvendigvis ville bygget en sårbar IKT-infrastruktur.



Fase 2: Krav om informasjonssikkerhet og personvern

- Kilder til krav om informasjonssikkerhet og personvern:
  1. Krav som følger av god praksis for adekvat sikkerhet i applikasjoner og forretningsprosesser.
  2. Krav om å begrense sikkerhetsrisiko til et akseptabelt nivå.
  3. Juridiske lovbestemte, regulatoriske og kontraktsmessige krav til informasjonssikkerhet og personvern.
- Sikkerhetskrav må kontinuerlig oppdateres for å gjenspeile endringer i nødvendig funksjonalitet, trusselslandskap, lover, forskrifter, reguleringer,…
- Bør gjøres tidlig i utviklingsløpet (innledende design- og planleggingsfasen)
- OWASP Top 10 / ASVS definerer beste praksis for krav om applikasjonssikkerhet



Fase 3: Sikker design, og Fase 4: Sikker koding

3. Sikker design

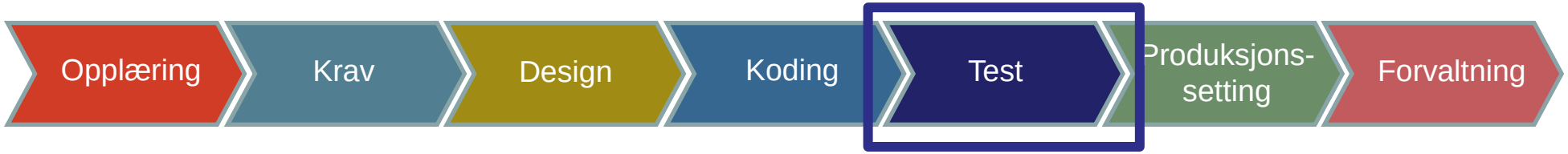
- Viktig del å spesifisere «sikre funksjoner», som er godt designet med hensyn til sikkerhet.
- Sikkerhetsfunksjoner som krypto, autentisering, logging etc er viktig. Designer må ha god kompetanse på disse.
- Trusselmodellering (mer om dette senere) er en viktig del her for å unngå sårbarheter

4. Sikker koding

- Målet med sikker koding er å unngå at sårbarheter bygges inn i systemet under koding og at sikkerhetsfunksjoner fungerer i henhold til krav og design
- Moderne utvikling benytter i stor grad tredjepartskomponenter, og det er viktig å forstå innvirkningen disse kan ha på sikkerheten. Usikre komponenter skal ikke brukes.
- Verktøy for kodeskanning og statisk analyse, gjennomgang av kode samt bruk av «sikre» programmeringsspråk er viktig her.

Fase 5: Sikkerhetstesting

- Mål er å avdekke sårbarheter som ikke har blitt oppdaget i design- eller kodefasene.
- **Dynamisk testing/sårbarhetsanalyse** av den fullstendige programvaren sjekker funksjonalitet som blir synlig når alle komponentene er integrert sammen. Sjekker blant annet at bruker får tilgang til informasjon/funksjonalitet den skal (og ikke informasjon som bruker ikke skal ha tilgang til).
- **Penetrasjonstesting** går et steg videre og er et (autorisert) simulert angrep for å evaluere sikkerheten («etisk hacking» brukes ofte om dette). Skiller mellom
  - hvitbokstesting der angriper har informasjon om system på forhånd
  - svartbokstesting der angriper ikke har slik informasjon.
- **Fuzztesting** forsøker å fremprovosere feil i systemet ved å gi korrupte inputverdier (tilfeldig eller misformet data).



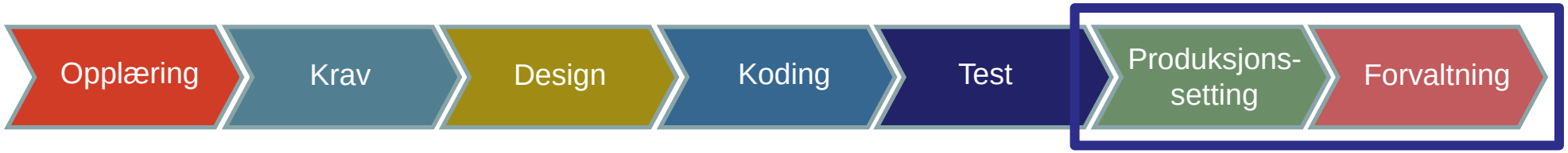
Fase 6: Produksjonssetting og Fase 7: Forvaltning

6. Produksjonssetting

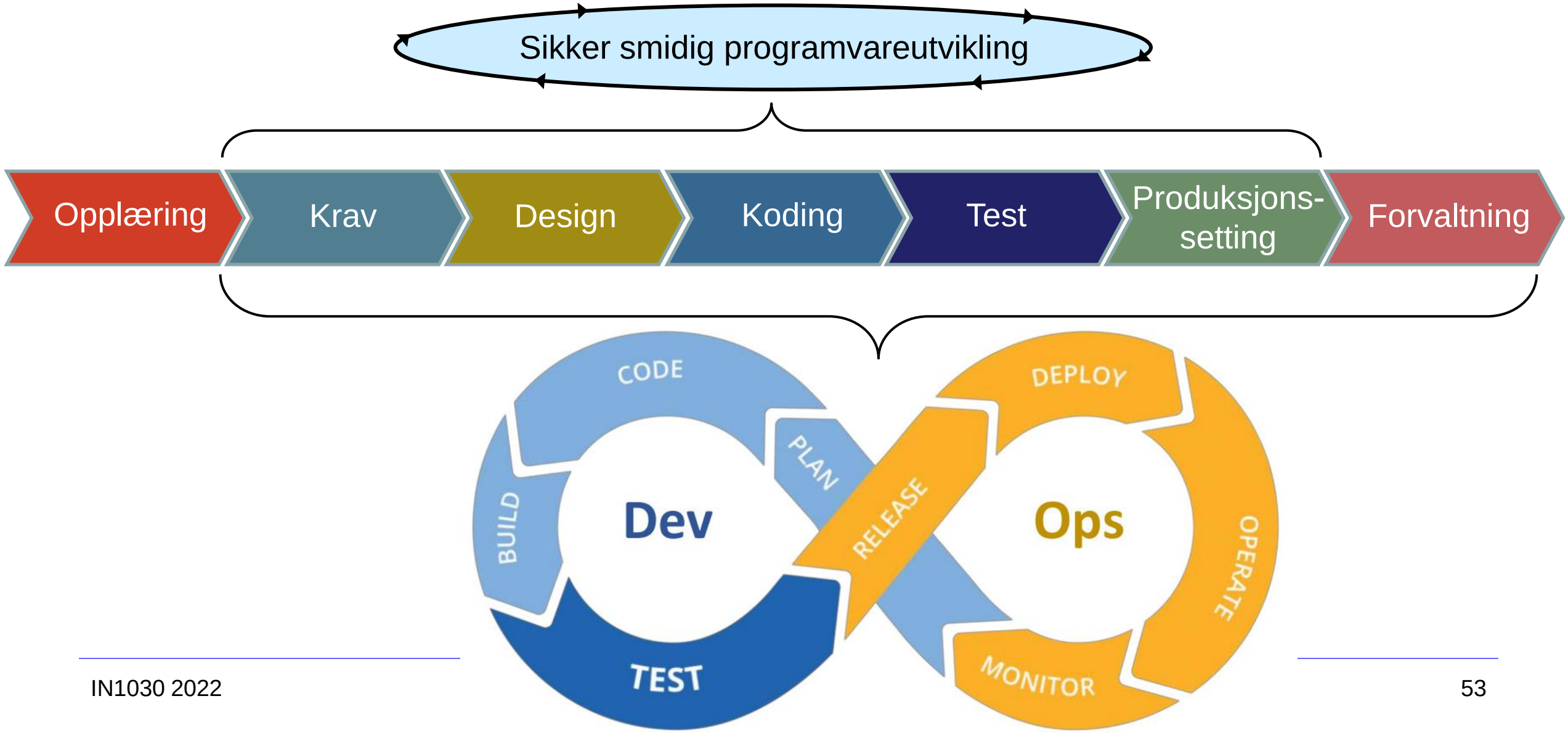
- **Plan for drift, vedlikehold og hendelseshåndtering** må definere prosedyrer for drift (inkl. patching), avviksrapportering og hendelseshåndtering (mer om dette neste uke)
- **Formell godkjenning av produksjonssetting** vil kreve at det verifiseres og dokumenteres at alle krav til sikkerhet og personvern er oppfylt og identifiserte sårbarheter er tilstrekkelig fjernet. Formelt ansvar/mandat må defineres og relevant data og dokumentasjon arkiveres.

7. Forvaltning

- **Drift og vedlikehold** innebærer at prosedyrer og rutiner for drift og vedlikehold av programvare skal følges, også over tid. Revisjoner bør gjennomføres regelmessig og et ledelsessystem for informasjonssikkerhet bør være på plass. Man må klart definere hva som skal logges og hvordan loggene håndteres.
- **Avviks- og hendelseshåndtering** Avvik og hendelser skal rapporteres som beskrevet i planene. (Mer om hendelseshåndtering neste uke).



DevOps: Sikker smidig programvareutvikling i skyen



Slutt på presentasjonen