IN2120 – Informasjonssikkerhet

Del 7a: Styring av cybersikkerhet

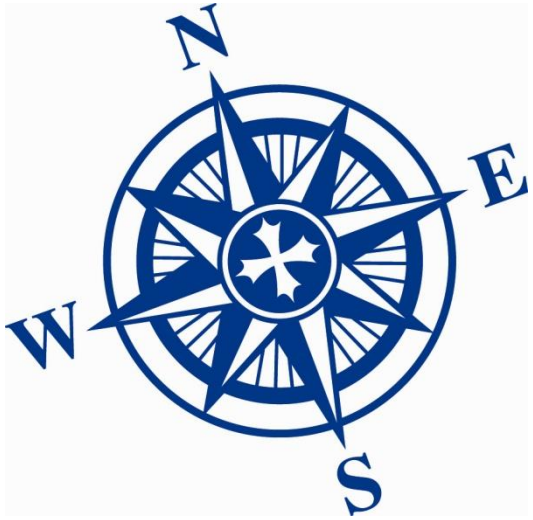
Janne Hagen



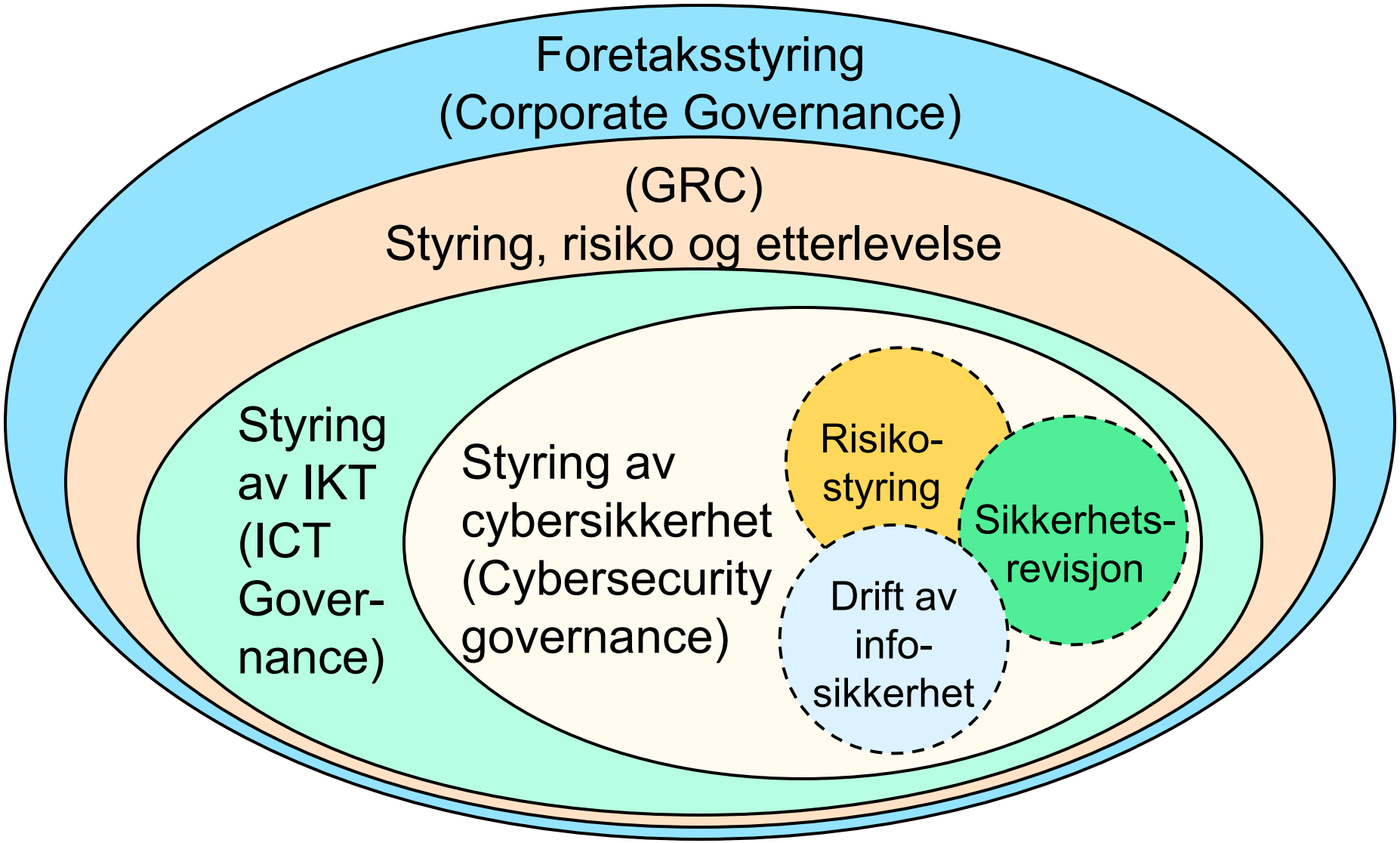
Universitetet i Oslo, høst 2026

Styring av cybersikkerhet - Oversikt

- Styring (Governance) av cybersikkerhet
- ISMS - Styringssystem for informasjonssikkerhet
- Standarder og rammeverk for informasjonssikkerhet



Styringskategorier



Styring av cybersikkerhet

Styring av informasjonssikkerhet er å definere strategiske målsettinger for informasjonssikkerhet, sørge for at disse blir oppnådd, styre sikkerhetsrisiko med effektiv bruk av organisatoriske ressurser, påse at styringssystemet for informasjonssikkerhet fungerer hensiktsmessig og at resultater følger forventninger og målsettinger.

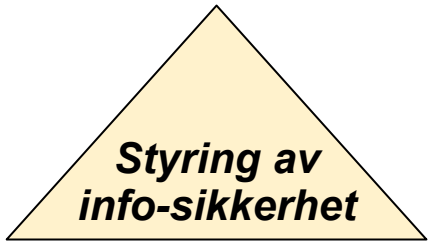
IT Governance Institute ISACA

“IS governance” oversettes som “styring av informasjonssikkerhet”

“IS management ” oversettes som “ledelse av informasjonssikkerhet”

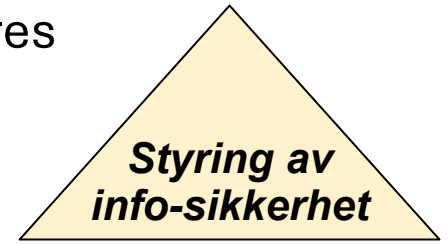
Merk:

Begrepene «styring av IS» og «ledelse av IS» brukes ofte om hverandre.



Mål for styring av informasjonssikkerhet

1. Strategisk tilpassing av sikkerhetsprogrammet
   - IS-aktiviteter skal støtte organisasjonens helhetlige strategi.
2. Risikohåndtering
   - Avdekke relevante trusler og risiko, innfør tiltak for å håndtere risikoen.
3. Verdiskapning
   - Søk optimal balanse mellom ressursbruk og reduksjon av risiko - ROI.
4. Ressursbruk
   - Kartlegge allerede implementerte løsninger for mulig gjenbruk og effektivisering
   - Kompetanse må bygges, brukes og ivaretas på best mulig måte
5. Målbarhet
   - Effekten av sikkerhetsarbeidet skal måles
6. Integrering av sikkerhetsområder
   - Sikkerhetsområder (fysisk, finansiell, IT etc.) skal i størst mulig grad integreres



Karakteristika av god sikkerhetsstyring

Gjelder for hele virksomheten

- Dekkes av felles rammeverk, policyer og prosesser

Informasjonssikkerhet er et fundamentalt krav

- Forutsetning for bærekraftig forretningsdrift

Ledelsen er godt informert

- Ledere forstår sikkerhetsrisikoer og får regelmessig rapportering

Ledelsen viser ansvar og regnskapelighet

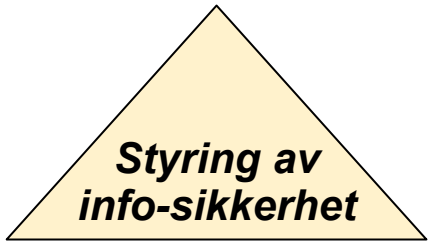
- Synlige ledere som setter klare mål og prioriteringer

Risikobasert prioritering

- Toleranser til risiko er forstått og etablert – bevissthet om akseptabel risiko

Roller & ansvarsområder er veldefinerte

- Klar arbeidsdeling

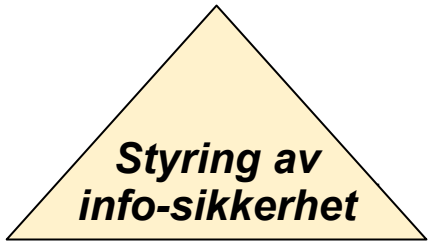


Nytteeffekt av god sikkerhetsstyring

Beskyttelse av verdier = verdiskapning

- Skaper tillit fra kunder, partnere, investorer og ansatte
- Bidrar til godt omdømme for bedriften og dens tjenester
- Gir konkurransefortrinn
- Forhindrer og reduserer tap
- Styrker beredskap og kontinuitet ved kriser
- Øker kvalitet og tilgjengelighet av tjenester
- Øker verdi for (aksje)eiere





Standarder og rammeverk for styring av cybersikkerhet

- ISO/IEC 27000-serien av sikkerhetsstandarder:
  - ISO/IEC 27000 Beskrivelse av ISMS og begreper for informasjonssikkerhet
  - ISO 27001: ISMS. Ledelsessystem for informasjonssikkerhet - Krav
  - ISO 27002: Tiltak for informasjonssikkerhet
  - + mange flere
    - De fleste ISO/IEC-standarder må kjøpes
- USA
  - NIST SP800-Series (Special Publications on Information Security)
  - NIST Cyber Security Framework
    - NIST-standarder er gratis
  - SANS Institute og CIS
- Norge – NSM, Digdir, Datatilsynet
  - Veiledere i sikkerhetsstyring

ISO/IEC 27000 ISMS – Oversikt

- *ISMS: Information security management systems – Overview*
- Standard Norge og UiO kaller det *LSIS: Ledelsessystem for informasjonssikkerhet*
- ISO/IEC 27000 definerer begreper for informasjonssikkerhet
- Gir en oversikt over andre standarder i 27000-serien
- Gir en generell beskrivelse av ISMS
- Et ISMS:
  - Består av policyer, prosedyrer, retningslinjer og tilhørende ressurser og aktiviteter, som forvaltes av en organisasjon med hensikt å beskytte informasjonsverdier.
  - Spesifiserer en systematisk tilnærming for å etablere, implementere, drifte, overvåke, gjennomgå, vedlikeholde og forbedre en organisasjons informasjonssikkerhet med hensikt å oppnå forretningsmålene.
  - Spesifiserer hvordan arbeidet med informasjonssikkerhet skal være basert på en risikovurdering, med hensikt å håndtere risikoer på best mulig måte for virksomheten og slik at risikoen er akseptabel.

ISO/IEC 27001 ISMS - Krav

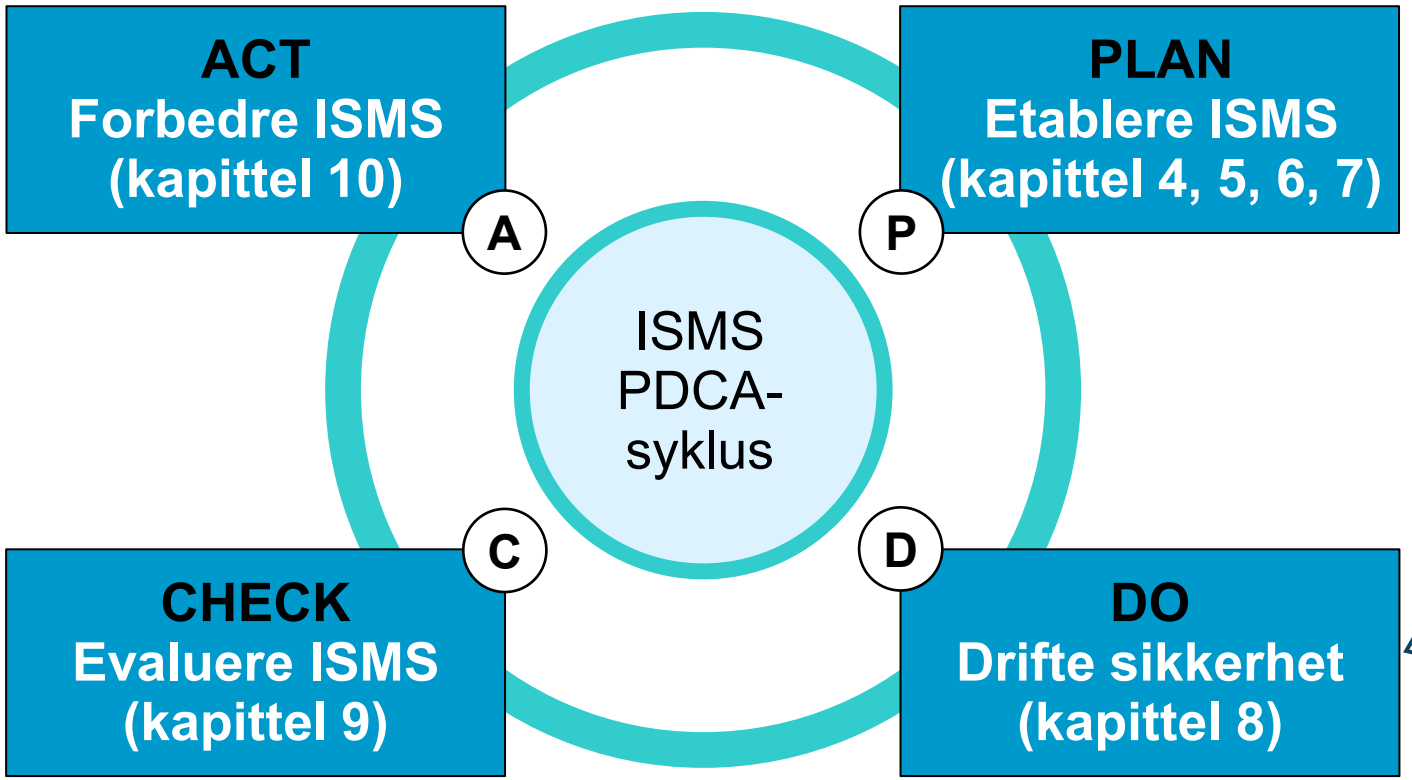
- ISO/IEC 27001 ISMS – Krav, spesifiserer krav for å etablere, implementere, vedlikeholde og kontinuerlig forbedre et selskaps ISMS.
- Innledende kapitler i ISO/IEC 27001
  1. Scope, 2. Normative referanse, 3. Begreper og definisjoner
- Selve kravene er beskreevet i kapittel 4 – 10, se sammendrag av ISO/IEC 27001
  4. Kontekstuelle krav
  5. Ledelseskrav
  6. Planleggingskrav
  7. Krav til ressurser og støttefunksjoner
  8. Krav til drift
  9. Krav til evaluering
  10. Krav til kontinuerlig forbedring
- Organisasjoner kan sertifiseres i henhold til ISO/IEC 27001

  … ved å vise at de oppfyller alle kravene

ISO/IEC 27001 ISMS - krav

Krav til styrings-/ledelsessystem for informasjonssikkerhet

- ISO/IEC 27001 beskriver krav til ISMS, som kan struktureres og visualiseres med PDCA-syklusen.
- Konkret styrking av cybersikkerhet med valg og implementering av sikkerhetstiltak skjer i DO-fasen.
- God styring av DO-fasen krever oppfyllelse av kravene i de andre fasene.



Implementere og drifte sikkerhetsfunksjonene fra NSMs grunnprinsipper for IKT-sikkerhet (alternativt fra NISTs CSF)

1. Identifisere og kartlegge
2. Beskytte og opprettholde
3. Oppdage
4. Håndtere og gjenopprette

ISMS/LSIS/Internkontroll - Kjært barn har mange navn.

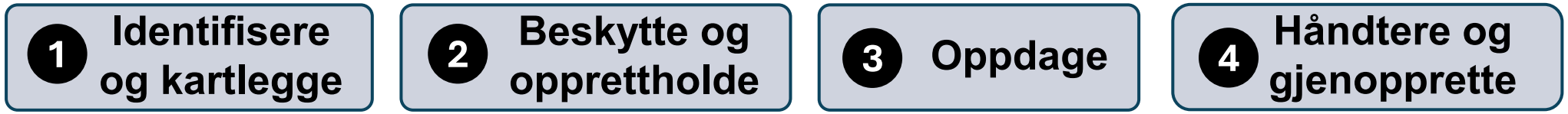
- Styringssystem (ISMS) og ledelsessystem (LSIS) for IS har samme betydning.
- Digdir benytter betegnelsen «internkontroll» omtrent med betydning ISMS/LSIS.
  - Internkontroll/ styringssystem/ ledelsessystem for informasjonssikkerhet | Digdir
- Privat og statlig sektor (NSM) benytter vanligvis begrepet ISMS (Information Security Management System), oversatt som «styringssystem for informasjonssikkerhet».
- Lover og forskrifter benytter begrepet «styringssystem for informasjonssikkerhet» f.eks. eForvaltningsforskriften.
- Standard Norge oversetter ISMS som LSIS (Ledelsessystem for informasjonssikkerhet).
- Begrepet LSIS brukes i undervisningssektoren i Norge generelt, og på UiO.
- Se beskrivelse av UiO sitt LSIS:
  - https://www.uio.no/tjenester/it/sikkerhet/lsis/
- Begrepet LSIS benyttes av noen andre statlige virksomheter, bl.a. Sykehuspartner.
- Merk at internkontroll også kan bety «intern sikkerhetsrevisjon».

Tiltaksbanker for informasjonssikkerhet

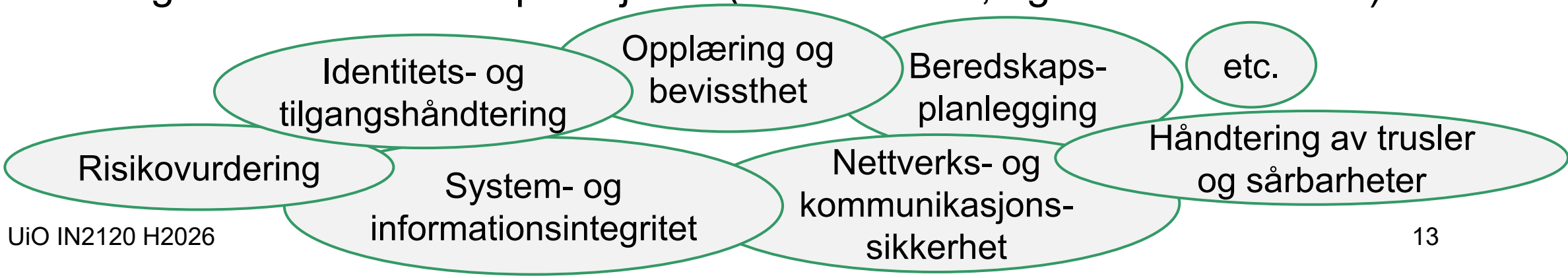
1. :



2. Kategorisert etter sikkerhetsfunksjoner (NSMs grunnprinsipper og NISTs CSF)



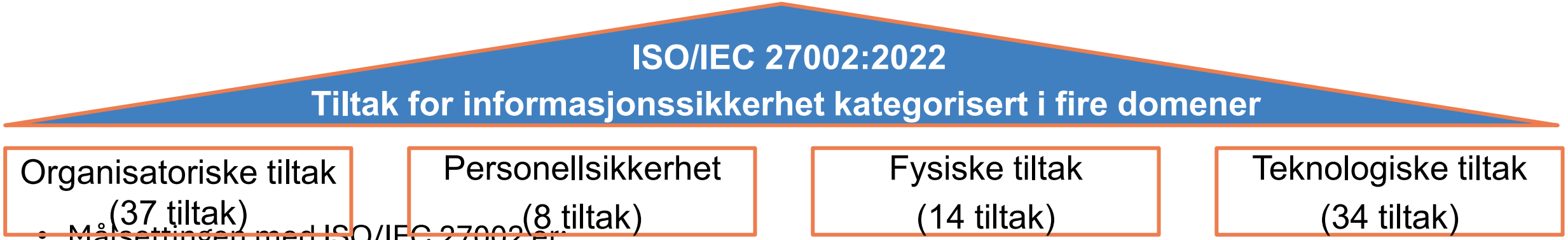
3. : Kategorisert etter driftsoperasjoner (CIS Controls, og NIST SP 800-53)



ISO/IEC 27002 – Informasjonssikkerhetstiltak

Tiltaksbank for informasjonssikkerhet

- ISO/IEC 27002 er en tiltaksbank, dvs. den beskriver et stort utvalg av sikkerhetstiltak som kan vurderes å bli implementert/brukt i organisasjoner
- Beskriver 93 sikkerhetstiltak kategorisert i 4 generelle domener



- Målsettingen med ISO/IEC 27002 er:
  - *å beskrive et sett med generiske sikkerhetstiltak inkludert implementeringsveiledning. Standarden er ment å bli brukt i sammenheng med et ISMS basert på ISO/IEC 27001.*
- Revisjon i henhold til ISO/IEC 27001 krever en SoA (Statement of Applicability)
  - SoA kalles «relevanserklæring» på norsk. Det er en tabell over tiltakene i ISO/IEC 27002, som for hvert tiltak beskriver om det er relevant eller ikke, og hvorfor, og om tiltaket er implementert.

Attributter for hvert tiltak i ISO/IEC 27002:2022

- Attributter er nyttige for å finne sikkerhetstiltak utifra ulike kategoriseringer.
- Foreslåtte kategoriseringer beskrevet med ulike kolonner i tabell.
- Attributter for hvert sikkerhetstiltak merket med #, se eksempel nedenfor:

Sikkerhetstiltak 5.7 Trusseletterretning (organisatorisk sikkerhetstiltak i ISO/IEC 27002:2022)

Type sikkerhetstiltak	Informasjons-sikkerhetsegenskaper	Cybersikkerhets-konsepter (funksjoner)	Operasjonell kapasitet	Sikkerhetsdomener
#Forebyggende #Oppdagende #Korrigerende	#Konfidensialitet #Integritet #Tilgjengelighet	#Identifisere #Oppdage #Respondere	#Håndtering_av_trusler_og_sårbarheter	#Forsvar #Resiliens

Sikkerhetstiltak

Informasjon knyttet til trusler mot informasjonssikkerheten bør samles inn og analyseres for å produsere trusseletterretning.

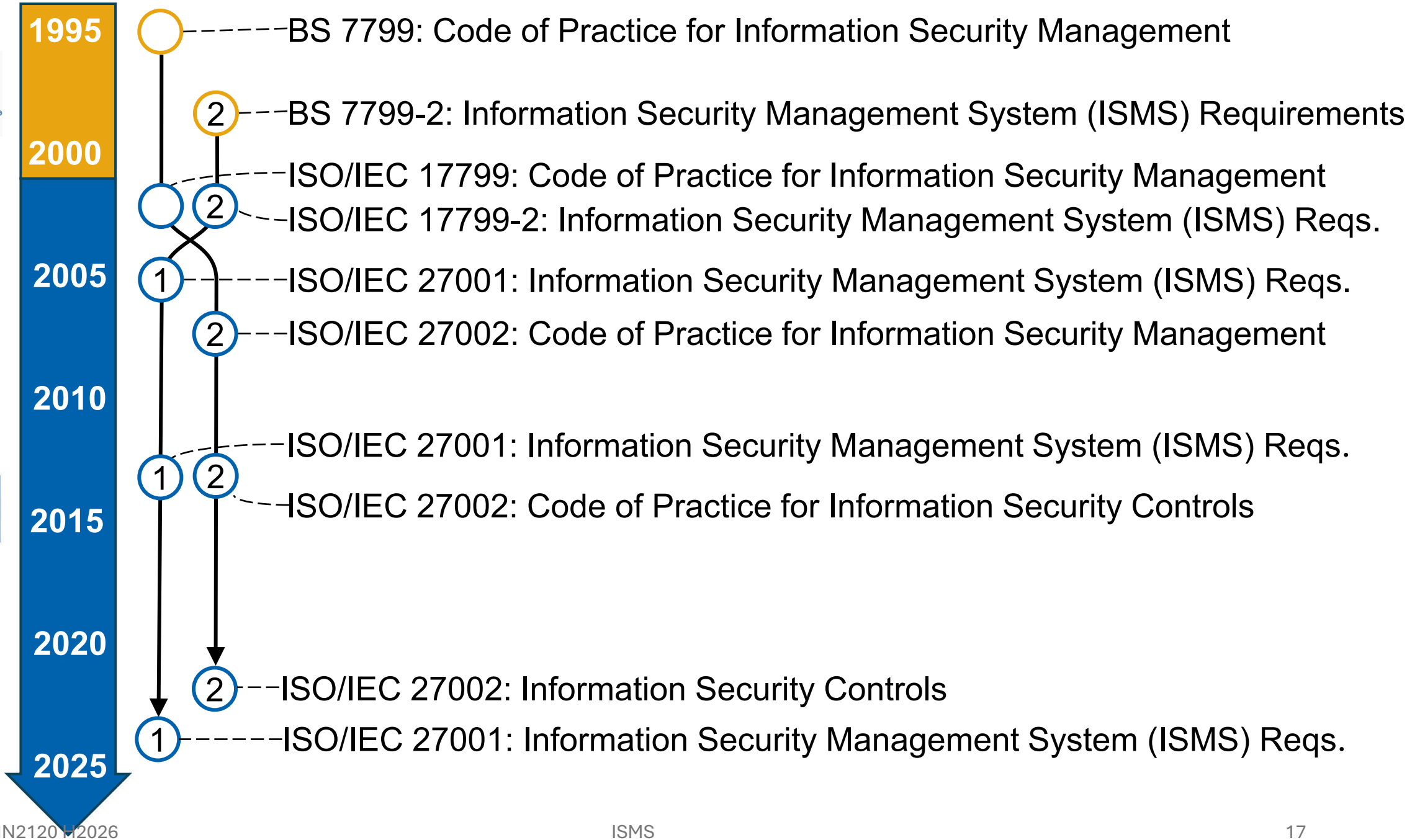
Formål

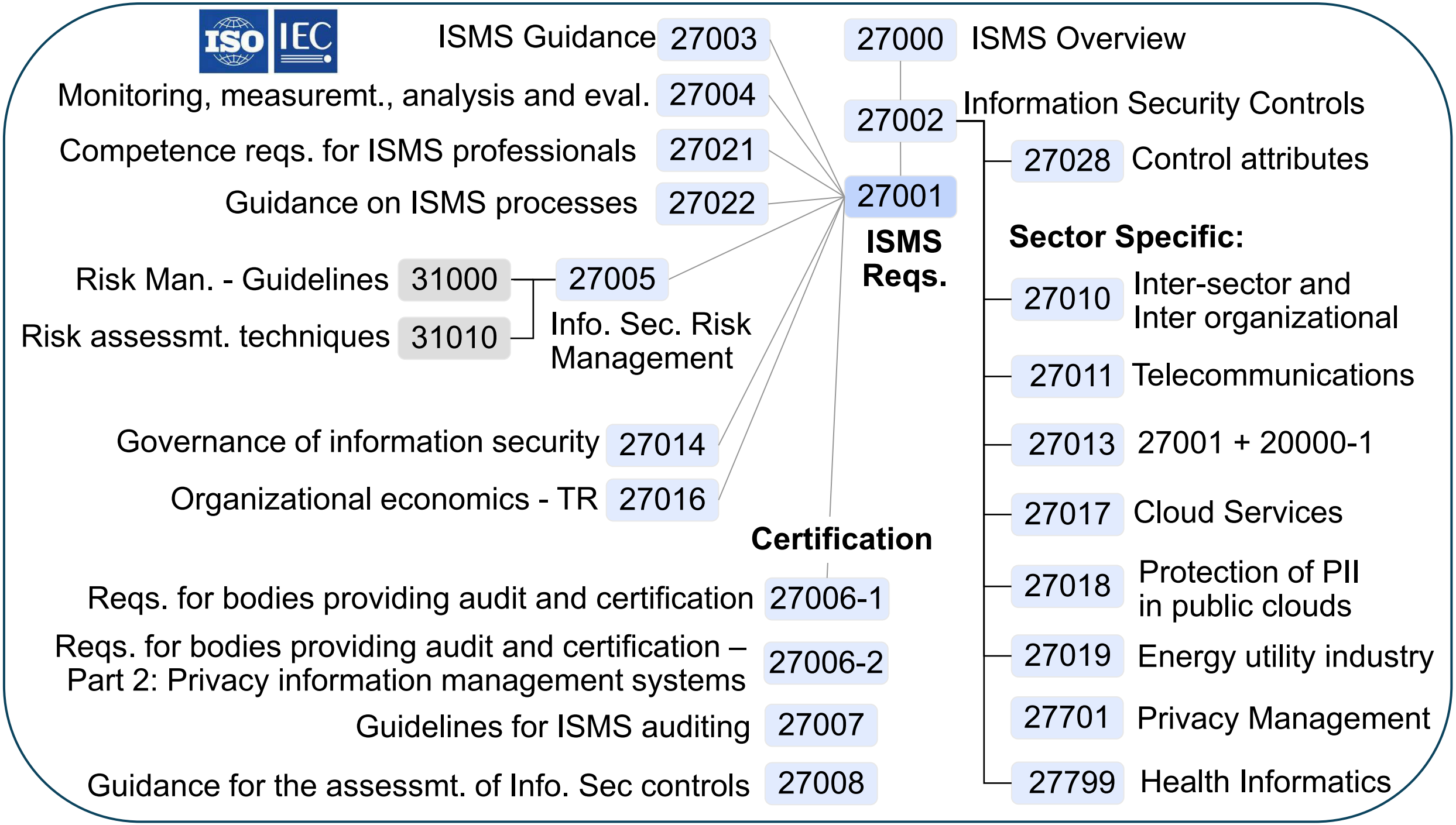
Å sørge for bevissthet om organisasjonens trusselbilde slik at det kan iverksettes egnede forebyggende tiltak.

Attributtkategorier i ISO/IEC 27002:2022

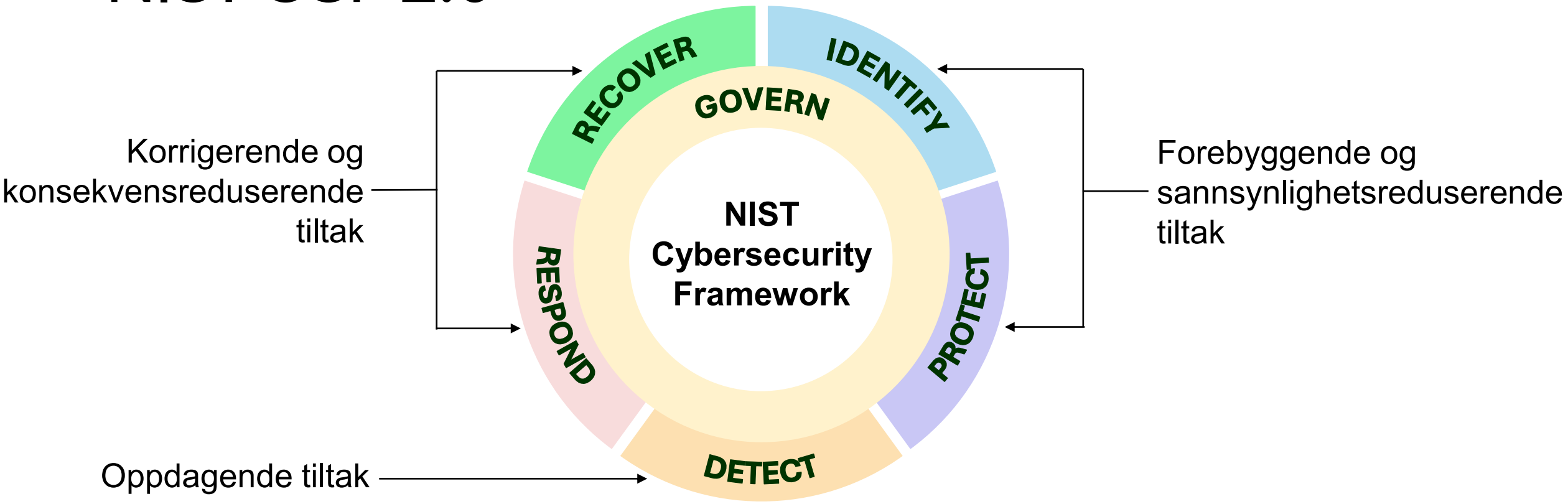
- **Type sikkerhetstiltak**
  - #Forebyggende, #Oppdagende, #Korrigerende.
- **Informasjonssikkerhetsegenskaper**
  - #Konfidendialitet, #Integritet, #Tilgjengelighet.
- **Cybersikkerhetskonsepter** (tilsvarer funksjoner i NIST CSF og NSM Grunnprins.)
  - #Identifisere, #Beskytte, #Oppdage, #Respondere, #Gjenopprette.
- **Operasjonell kapasitet** (tilsvarer CIS Controls og SP 800-53:2020)
  - 15 ulike attributter
- **Sikkerhetsdomener**
  - #Styring_og_økosystem, #Beskyttelse, #Forsvar, #Resiliens.

Historien bak 27001 og 27002




ISO IEC
ISMS Guidance 27003
Monitoring, measuremt., analysis and eval. 27004
Competence reqs. for ISMS professionals 27021
Guidance on ISMS processes 27022
Risk Man. - Guidelines 31000
Risk assessmt. techniques 31010
27005
Info. Sec. Risk Management
Governance of information security 27014
Organizational economics - TR 27016
27000 ISMS Overview
27002 Information Security Controls
27001
ISMS Reqs.
27028 Control attributes
Sector Specific:
27010 Inter-sector and Inter organizational
27011 Telecommunications
27013 27001 + 20000-1
27017 Cloud Services
27018 Protection of PII in public clouds
27019 Energy utility industry
27701 Privacy Management
27799 Health Informatics
Certification
Reqs. for bodies providing audit and certification 27006-1
Reqs. for bodies providing audit and certification – Part 2: Privacy information management systems 27006-2
Guidelines for ISMS auditing 27007
Guidance for the assessmt. of Info. Sec controls 27008

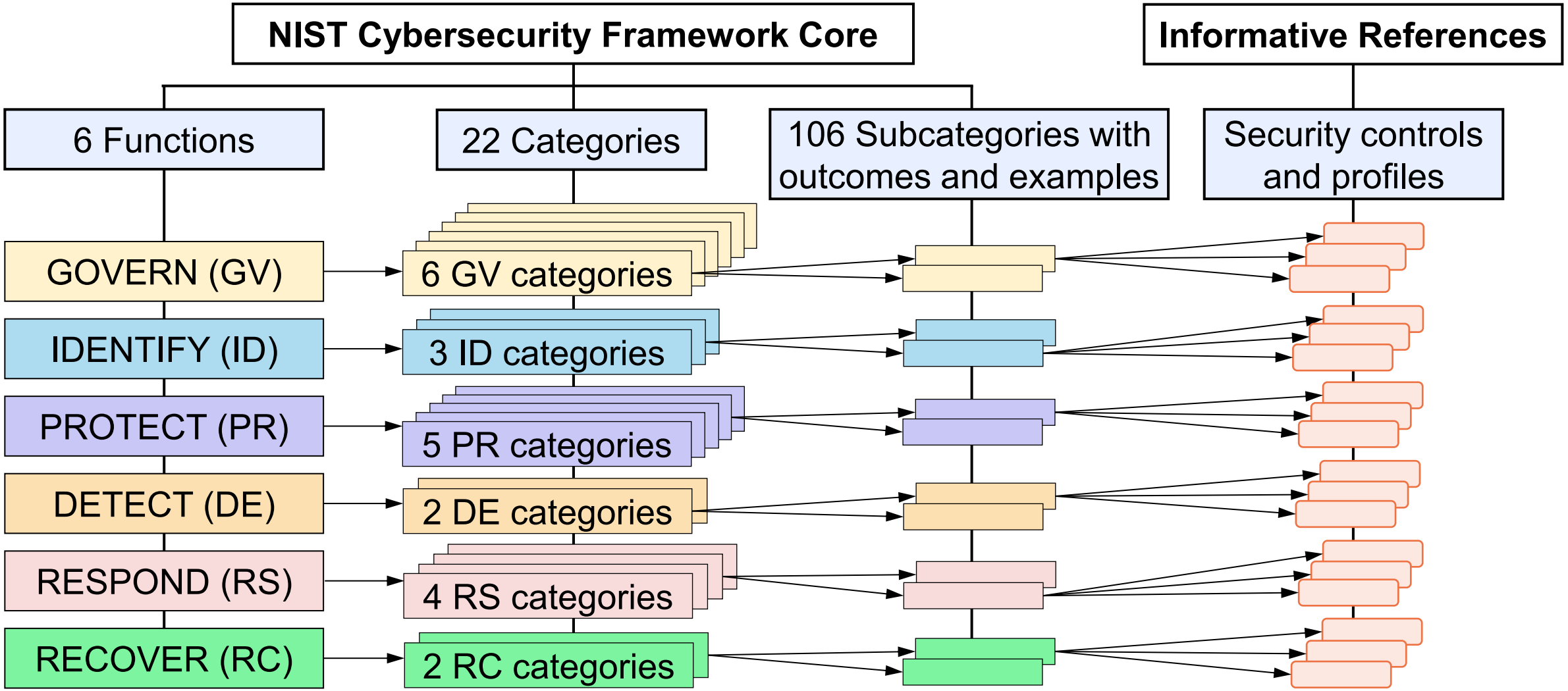
NIST CSF 2.0



- Ny funksjon GOVERN lagt til i CSF 2.0 (2024)

Struktur av NIST CSF 2.0

National Institute of Standards and Technology
U.S. Department of Commerce



NIST CSF 2.0 med 6 sikkerhetsfunksjoner og 22 kategorier

National Institute of Standards and Technology
U.S. Department of Commerce

GOVERN (Styre)	IDENTIFY (Identifisere)	PROTECT (Beskytte)	DETECT (Oppdage)	RESPOND (Håndtere)	RECOVER (Gjenopprette)
Org. Context	Access Mgmt.	IAM	Contin. Monitoring	Incident Mgmnt.	In. Rec-Plan-Exe
Risk Mgmt. Strat.	Risk Assesment	Awareness Train.	Adv. Ev. Analysis	Incident Analysis	In. Recover-Com
C-SCRM	Improvement	Data Security		In. Rsp-Rep-Com	
Roles-Resp-Auth		Platform Security		Incident Mitigation	
Pols-Prcss-Prcds		Tech. Infra. Res.			
Oversight					

NSMs Grunnprinsipper for IKT-sikkerhet

- NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med sikkerhetstiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk.
  - https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt
- Publiseres gratis for å hjelpe virksomheter med å redusere cybersikkerhetsrisiko.
- Beskriver 118 tiltak delt opp i 21 prinsipper gruppert i 4 kategorier.
  1. Identifisere og kartlegge
  2. Beskytte og opprettholde
  3. Oppdage
  4. Håndtere og gjenopprette

  } Kategorisering etter 4 sikkerhetsfunksjoner

NSM

- Kategoriene ligner på NIST Cybersecurity Framework
- Hvert tiltak er merket med prioriteringsgruppe 1, 2 eller 3
- 90% av sikkerhetshendelser kan unngås ved å implementer alle tiltak i gruppe 1
- En SoA (Statement of Applicability) i henhold til ISO/IEC 27001 krever en kartlegging mellom tiltak fra NSMs grunnprinsipper og fra ISO/IEC 27002.

Grunnprinsipper for IKT-sikkerhet

1 Identifisere og kartlegge

- Kartlegg styringsstrukturer, leveranser og understøttende systemer
- Kartlegg enheter og programvare
- Kartlegg brukere og behov for tilgang

2 Beskytte og opprettholde

- Ivareta sikkerhet i anskaffelses- og utviklingsprosesser
- Sikker IKT-arkitektur
- Sikker konfigurasjon
- Beskytt nettverk
- Kontroller dataflyt
- Identiteter og tilganger
- Beskytt data i ro og transitt
- Beskytt e-post og nettleser
- Gjenoppretting av data
- Sikkerhet i prosess for endringshåndtering

3 Oppdage

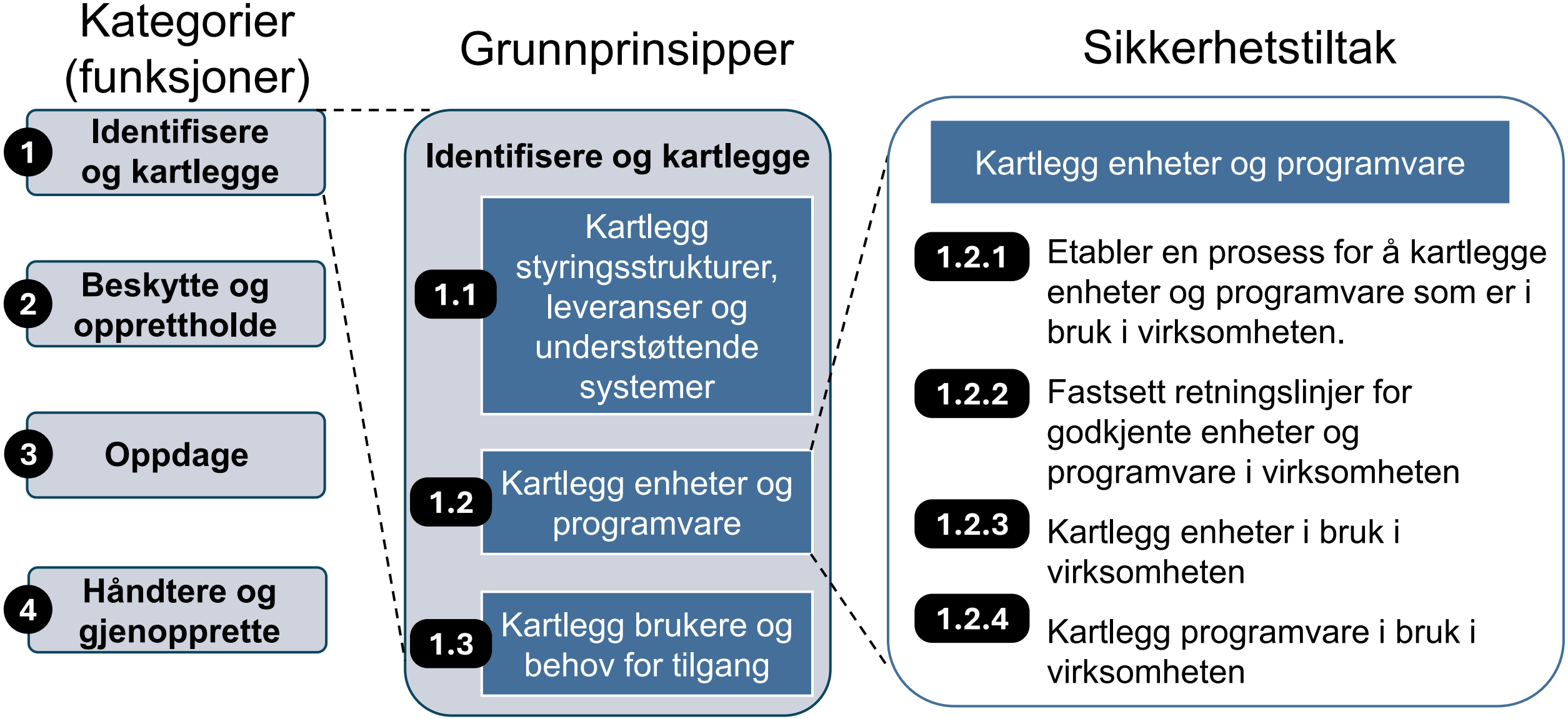
- Oppdag og fjern kjente sårbarheter
- Etabler sikkerhets-overvåking
- Analyser data fra sikkerhetsovervåking
- Gjennomfør inntrengingstester

4 Håndtere og gjenopprette

- Forbered på håndtering av hendelser
- Vurder og klassifiser hendelser
- Kontroller og håndter hendelser
- Evaluer og lær av hendelser

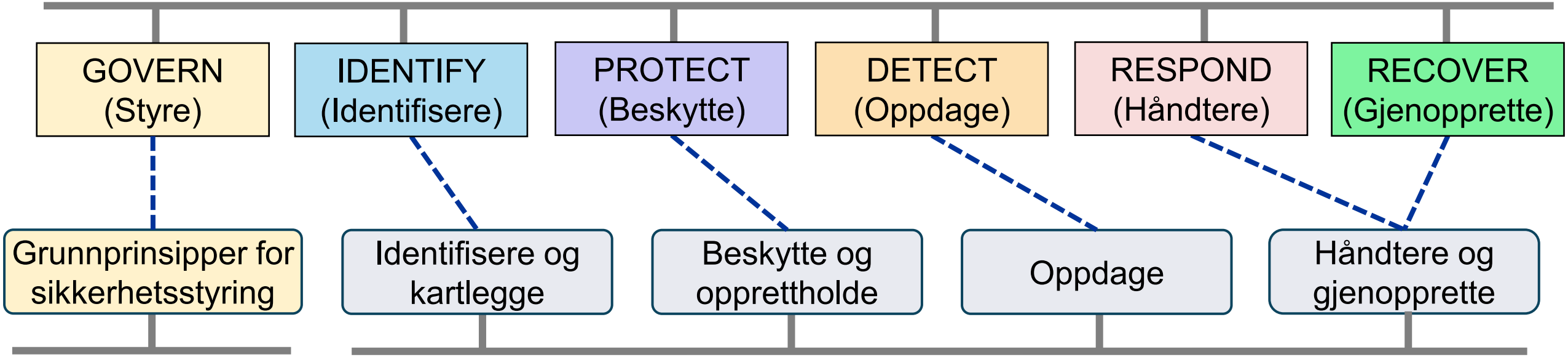
NSM

Struktur i NSMs Grunnprinsipper for IKT-sikkerhet



Rammeverk for cybersikkerhet

Funksjoner i NIST Cybersecurity Framework



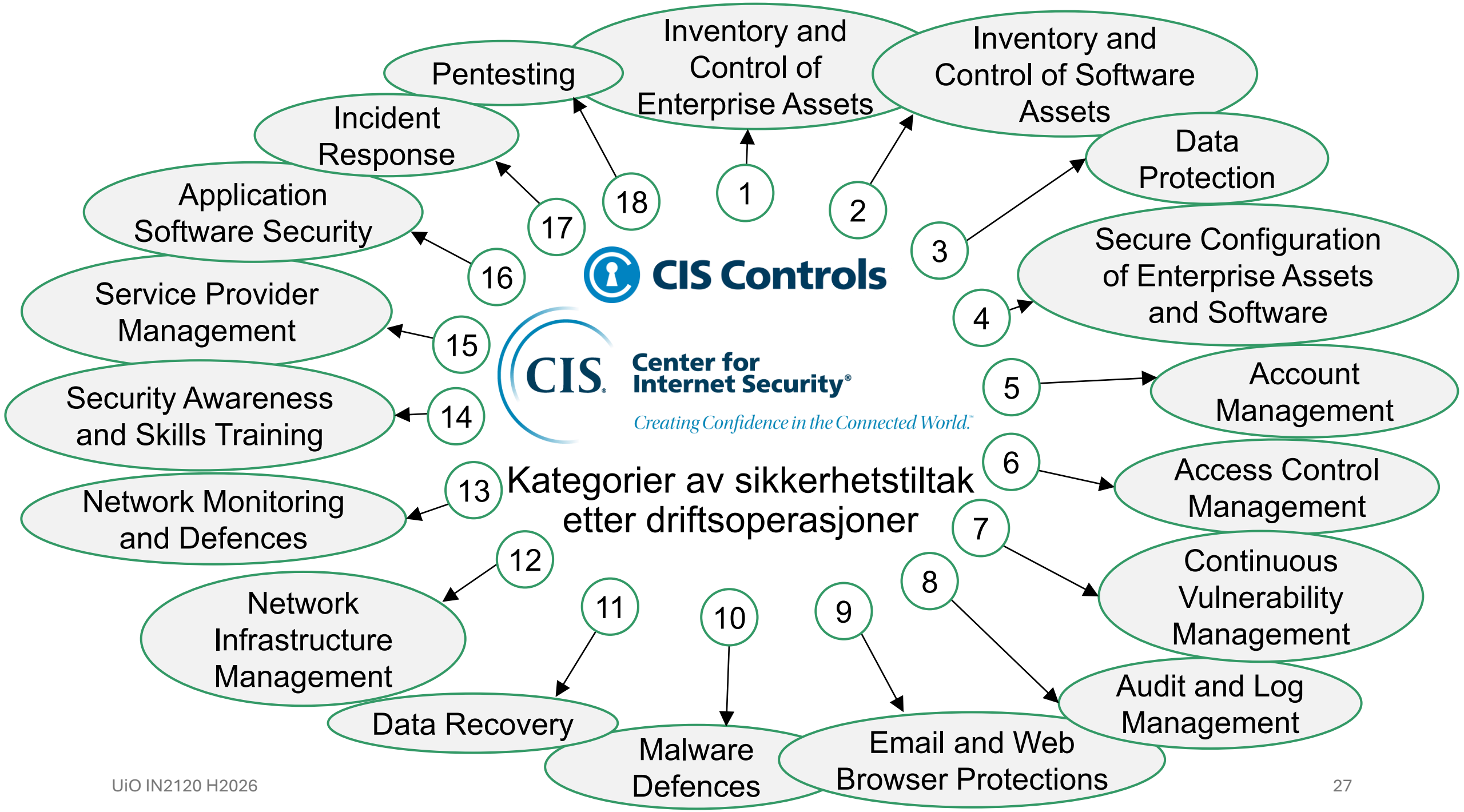
NSM-veileder

Sikkerhetsfunksjoner i NSMs grunnprinsipper for IKT-sikkerhet

Andre rammeverk for IT-sikkerhet

- CobiT
  - Control Objectives for Information and Related Technology (CobiT)
- Information Security Forum (ISF International)
  - Standard of Good Practice for Information Security
  - www.securityforum.org
- ITIL
  - Information Technology Infrastructure Library
  - Management guidelines for IT, including IT security
- DigDir:
  Internkontroll i praksis – informasjonssikkerhet
  - Grunnleggende innføring
  - Rikt utvalg med maler og eksempler
- Datatilsynet
  - Innebygd personvern og sikkerhet som standard
- CIS / SANS
  - Critical Security Controls

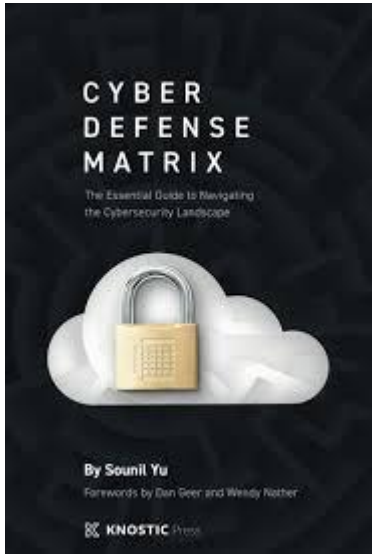



Inventory and Control of Enterprise Assets
Inventory and Control of Software Assets
Data Protection
Secure Configuration of Enterprise Assets and Software
Account Management
Access Control Management
Continuous Vulnerability Management
Audit and Log Management
Email and Web Browser Protections
Malware Defences
Data Recovery
Network Infrastructure Management
Network Monitoring and Defences
Security Awareness and Skills Training
Service Provider Management
Application Software Security
Incident Response
Pentesting
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
CIS Controls
CIS Center for Internet Security®
Creating Confidence in the Connected World.™
Kategorier av sikkerhetstiltak etter driftsoperasjoner

The 20 Security Control Categories of NIST SP 800-53: 2020



Cyberforsvarsmatrisen



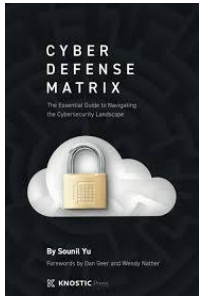
- Cyberforsvarsmatrisen (Cyber Defense Matrix: CDM) gir

  et todimensjonalt syn på cybersikkerhetsstyring som dermed utvider NIST CSFs perspektiv på cybersikkerhet.

  https://cyberdefensematrix.com

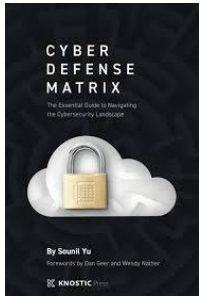
- Den første dimensjonen av CDM er representert av de opprinnelige fem funksjonene til NIST CSF som er IDENTIFISERE, BESKYTTE, OPPDAGE, RESPONDERE, og GJENOPPRETTE, som beskrevet av NIST CSF.
- Den andre dimensjonen av CDM er representert av de fem viktigste klassene av digitale verdier som er ENHETER, APPER, NETTVERK, DATA og BRUKERE.
- Selv om betydningen av verdiklassene kan virke åpenbar ut fra navnene deres, er det lærerikt å gi en kort beskrivelse av hver eiendelclass.

Digitale verdier



- ENHETER er maskinvare og standard installert programvaren som OS.
  - Fastvare, operativsystemer og standardapplikasjoner fra leverandører
  - Skill mellom ENHETER basert på hvem som eier enheten, for eksempel organisasjon, ansatte (BYOD) eller skyleverandører.
  - Nettverksenheter som svitsjer og rutere tilhører også denne klassen.
- APPER er applikasjoner og prosesser spesielt utviklet av eller for virksomheten.
  - APP-er produserer vanligvis tjenestene og produktene som leverer organisasjonens verdi og forretningsfunksjoner. Derfor er kontinuiteten og integriteten til APPS vanligvis kritisk.
- NETTVERK er kommunikasjonskanaler, rutere, protokoller og brannmurfiltreringer.
  - Konfigurasjon av nettverksenheter som DNS (Domain Name System), AS (Autonomous Systems) og PKI (Public Key Infrastructure), og som gir ruting, filtrering og VPN
- DATA er forretningsdata, som er lagret, som overføres eller brukes av verdiene over.
- BRUKERE er personer og KI-agenter, med deres ID-er og autentikatorer.
  - En AI-agent kan kanskje betraktes som en enhet, men hvis den har egenskapene til en bruker med sin egen ID, autentiseringslegitimasjon, tilgangsautorisasjoner og intelligente beslutninger.

Bruksområder for cyberforsvarsmatrisen

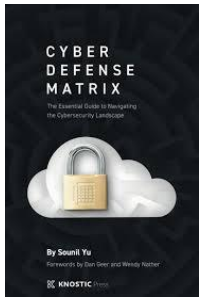


Cyberforsvarsmatrisen har flere anvendelser som:

- Gap-analyse av cybersikkerhetstiltak
- Fordeling av utførende og overordnet ansvar for cybersikkerhet
- Måling og beregninger
- Profilstatus og planlegging av sikkerhet for ulike digitale verdier
- Strukturell og situasjonsforståelse
- Produktklassifisering av leverandører av cybersikkerhet

- Neste side viser et eksempel på nåværende profil og målprofil beskrevet ovenfor. Cyberforsvarsmatrisen illustrerer en gap-analyse av sikkerhetsprofiler.
- Det andre eksemplet viser hvordan cyberforsvarsmatrisen kan brukes til å illustrere ansvarsfordeling

Cyberforsvarsmatrisen (Cyber Defense Matrix) Gap-analyse

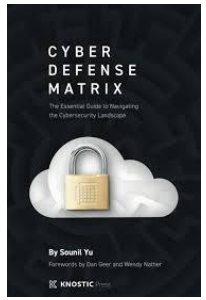


Sikkerhetsfunksjoner

Digitale verdier	IDENTIFISERE	BESKYTTE	OPPDAGE	HÅNDTERE	GJEN-OPPRETTE
ENHETER	■ ● ●	■ ■ ● ● ●	■ ● ●	■ ● ● ●	■ ● ●
APPER	●	■ ■ ■ ● ● ● ●	■ ● ●	●	●
NETTVERK	■ ● ● ● ●	■ ■ ■ ■ ● ● ● ●	■ ■ ● ● ●	■ ● ●	■ ■ ● ●
DATA	■ ● ●	■ ■ ■ ● ●	●	■ ●	■ ● ●
BRUKERE	■ ● ● ●	■ ● ●	● ●	●	●

Forklaring: ■ Nåværende profil ● Ønsket profil

Cyberforsvarsmatrisen brukt til ansvarsfordeling



- Cyberforsvarsmatrisen er perfekt for å forstå fordelingen av sikkerhetsansvar i organisasjonen, som vist i eksemplet nedenfor.

Sikkerhetsfunksjoner

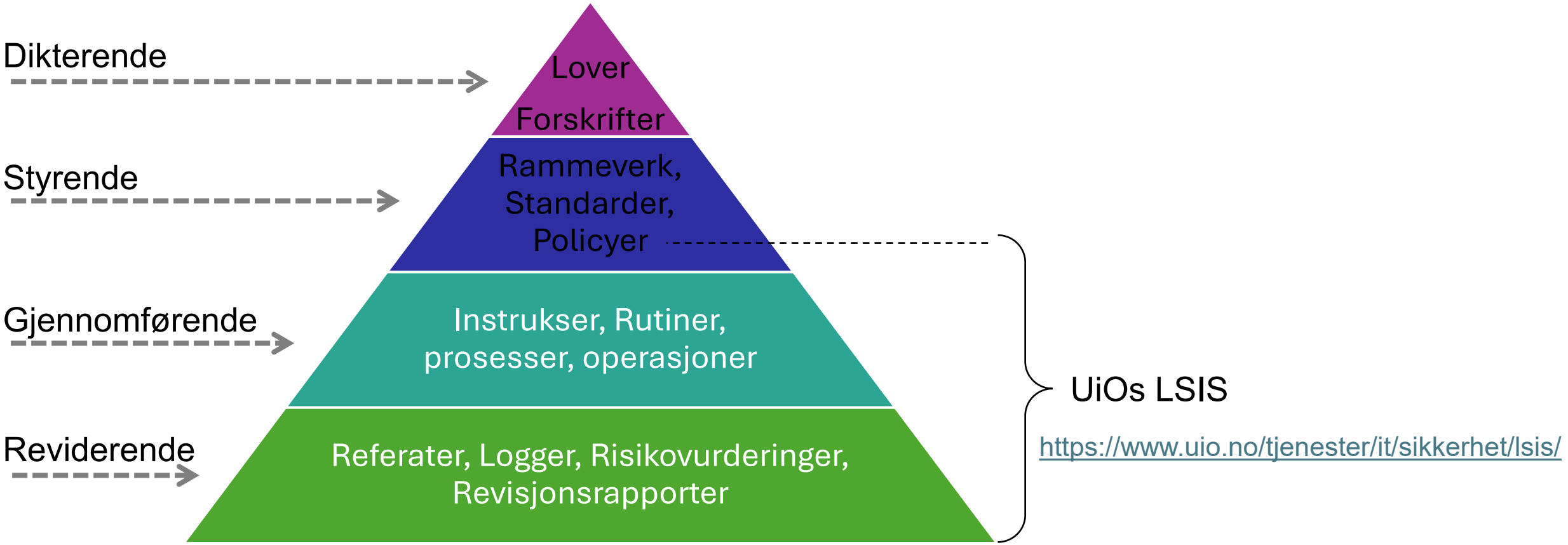
Digitale verdier	IDENTIFISERE	BESKYTTE	OPPDAGE	HÅNDTERE	GJEN-OPPRETTE
ENHETER	IT-tjenester, eiere		SOC/CERT/CSIRT Overvåking av enheter		IT-tjenester, eiere
APPER	DevOps-team, eiere		SOC/CERT/CSIRT Overvåking av apper		DevOps-team, eiere
NETTVERK	Nettverksadministrator		SOC/CERT/CSIRT Overvåking av nettverk		Nettverks-administrator
DATA	Dataeiere (CDO), personvernombud (PVO)		SOC/CERT/CSIRT IT-drift		CDO, PVO, eiere
BRUKERE	HR-avdelingen		Overvåking av innsidetrusler	HR-avdelinge, fysisk sikkerhet	

Fra IS-rammeverk til ISMS/LSIS

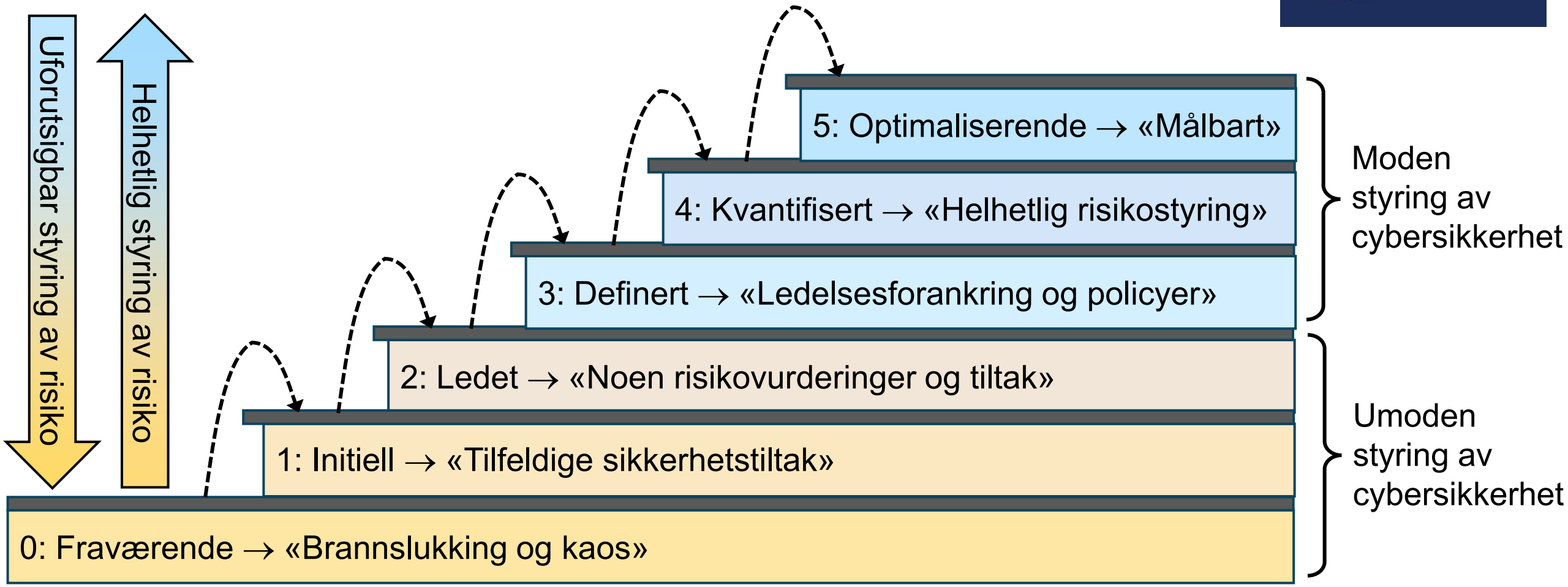
- Intet enkelt IS-rammeverk dekker alle behov
  - Ulike organisasjoner har forskjellige behov
  - Hvert enkelte rammeverk/standard har et begrenset fokus
- Velg de mest egnede rammeverk for virksomheten
- Definering av egne policyer
- Virksomhetens ISMS/LSIS bygges med utvalgte rammeverk og egne policyer
- SANS institute: Security policy templates:
  - https://www.sans.org/information-security-policy/
- Eksempel: UiO LSIS
  - https://www.uio.no/tjenester/it/sikkerhet/lsis/



Dokumenthierarki



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



Slutt på presentasjonen