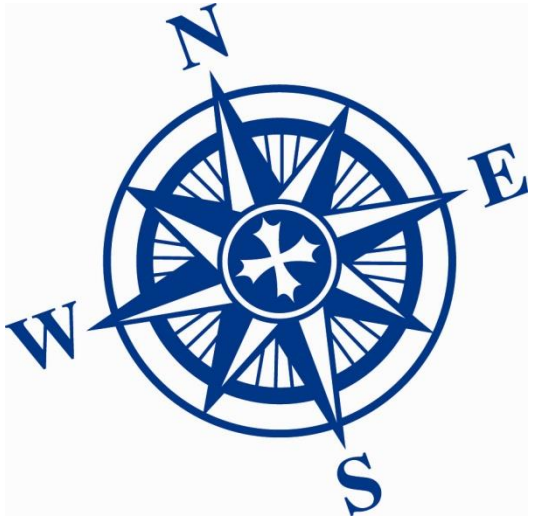
IN2120 Informasjonssikkerhet
Høst 2023

Del 11b: Ledelse av informasjonssikkerhet

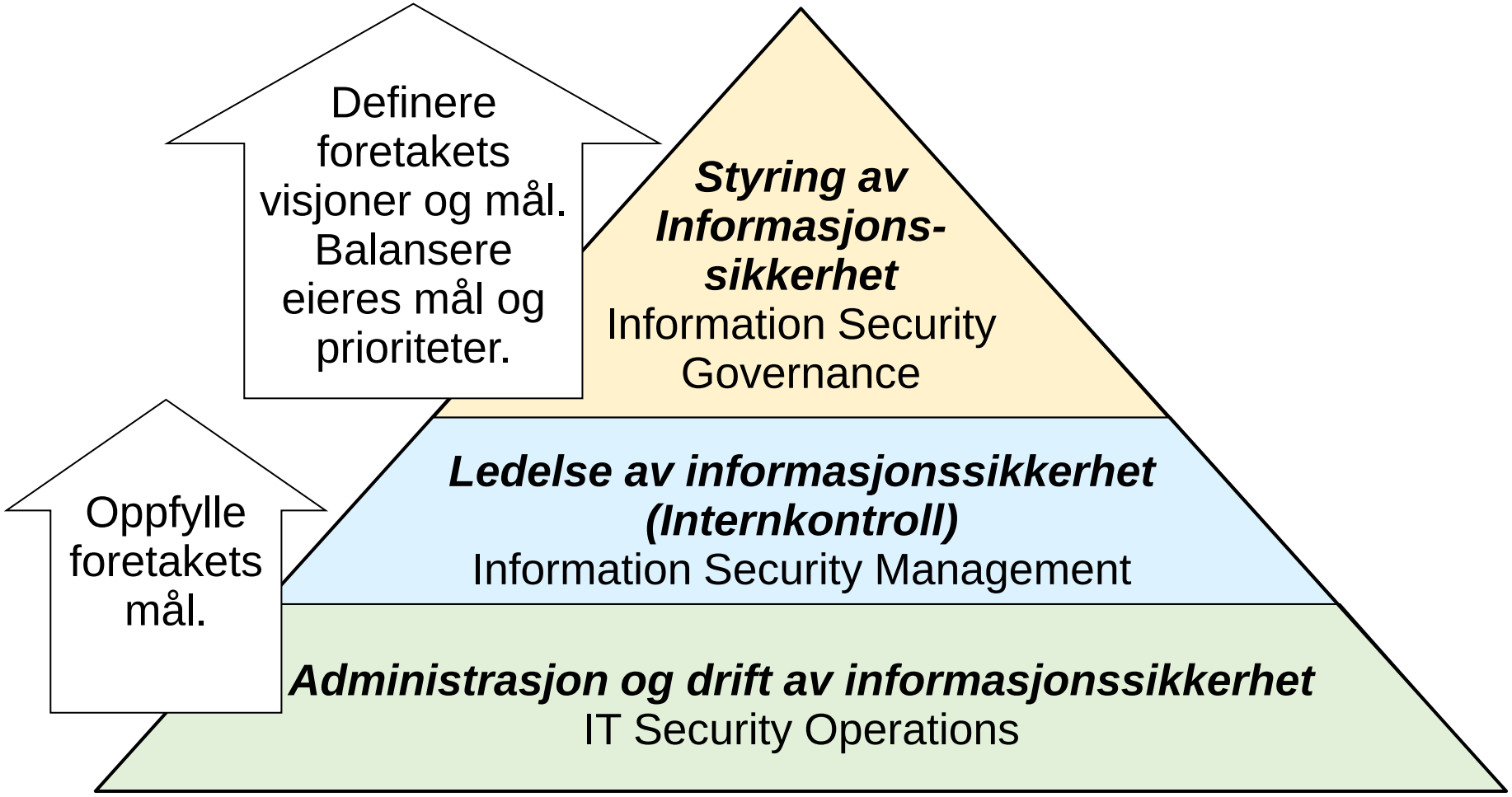
Audun Jøsang
Universitetet i Oslo

Oversikt styring og ledelse av informasjonssikkerhet

- Styring (Governance) og ledelse (Management) av informasjonssikkerhet
- ISMS - Styringssystem for informasjonssikkerhet
- Standarder og rammeverk for informasjonssikkerhet
- Modenhet av ISMS



Abstraksjonsnivårt for styring av informasjonssikkerhet



Styring av informasjonssikkerhet

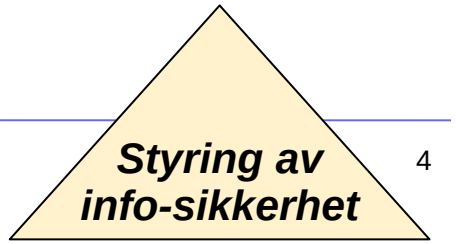
Styring av informasjonssikkerhet er å definere strategiske målsettinger for informasjonssikkerhet, sørge for at disse blir oppnådd, styre sikkerhetsrisiko med effektiv bruk av organisatoriske ressurser, påse at styringssystemet for informasjonssikkerhet fungerer hensiktsmessig og at resultater følger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

"IS governance" oversettes som "styring av informasjonssikkerhet"

"IS management " oversettes som "ledelse av informasjonssikkerhet"

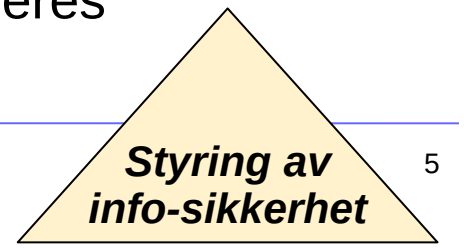
Merk:

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



Mål for styring av informasjonssikkerhet

1. Strategisk tilpasning 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, retningslinjer og prosesser

Informasjonssikkerhet er et fundamentalt krav

- Sett på som essensielt for bærekraftig forretningsdrift

Ledelsen er godt informert

- Ledere forstår sikkerhetsrisikoer og får regelmessig rapportering

Ledelsen viser ansvar

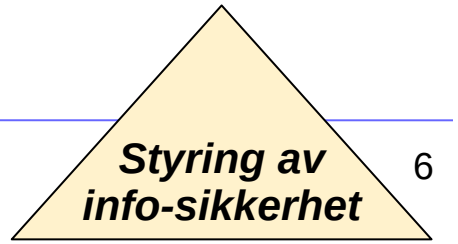
- Synlige ledere som setter klare mål og prioriteringer

Risikobasert prioritering

- Toleranser til risiko er forstått og etablert – ha bevissthet om forsvarlig risiko

Roller & ansvarsområder er veldefinerte

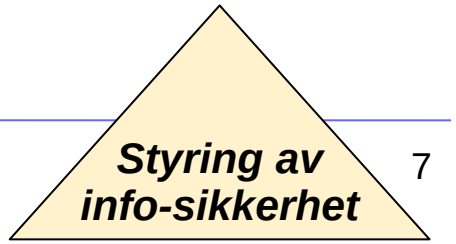
- Klar arbeidsdeling



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



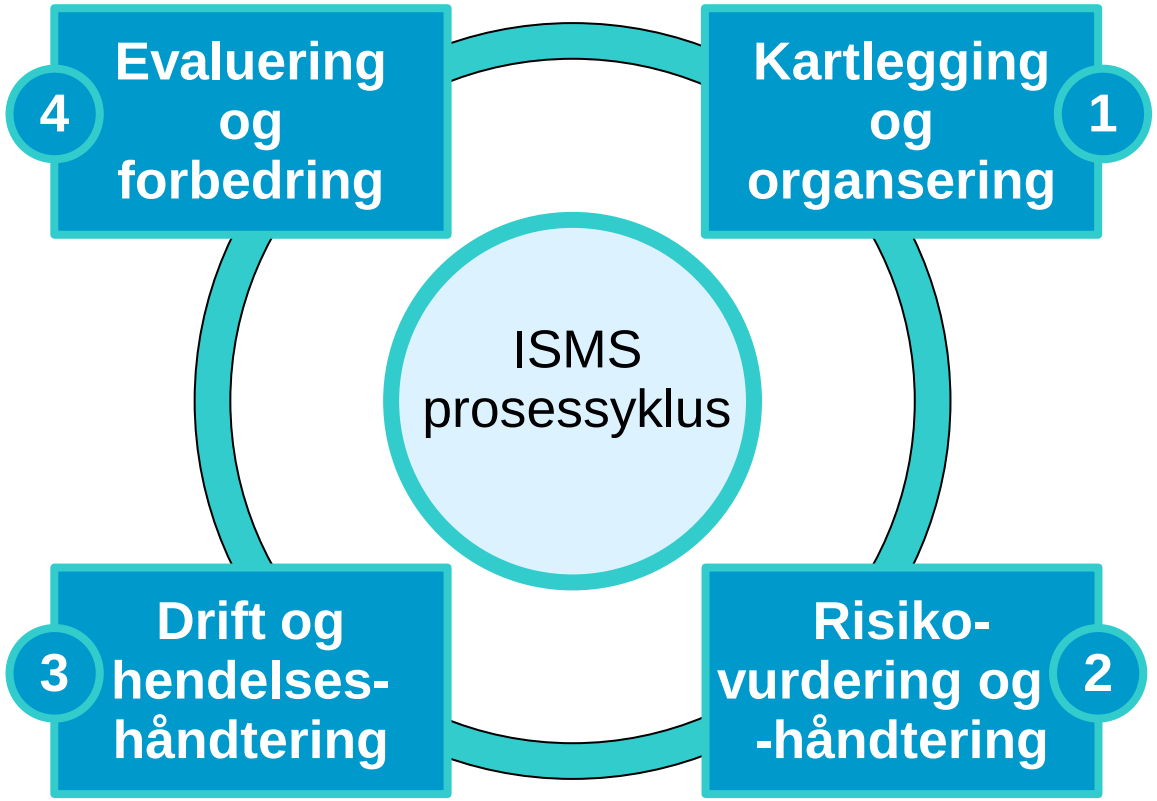
Standarder og rammeverk for ledelse av IS

- ISO/IEC 27K IT-sikkerhetsstandarder:
  - ISO/IEC 27000 Beskrivelse av ISMS og begreper for informasjonssikkerhet
  - ISO 27001: ISMS. Styringssystem 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 – Digdir, Datatilsynet, NSM,
  - Veiledere i sikkerhetsstyring

ISO/IEC 27000 – Hva er det?

- Tittel: *Information security management systems - Overview*
- Definerer begreper for informasjonssikkerhet
- Gir en oversikt over andre standarder i 27000-familien
- Gir en generell beskrivelse av hva ISMS (styrings/ledelsessystem for informasjonssikkerhet) er.
  - Består av policyer, prosedyrer, retningslinjer og tilhørende ressurser og aktiviteter, som forvaltes av en organisasjon med hensikt å beskytte informasjonsverdier.
  - Gir en systematisk tilnærming for å etablere, implementere, drifte, overvåke, gjennomgå, vedlikeholde og forbedre en organisasjons informasjonssikkerhet med hensikt å oppnå forretningsmålene.
  - Er basert på en risikovurdering og hva som anses som forsvarlig risiko, med hensikt å håndtere risikoer på best mulig måte for virksomheten.

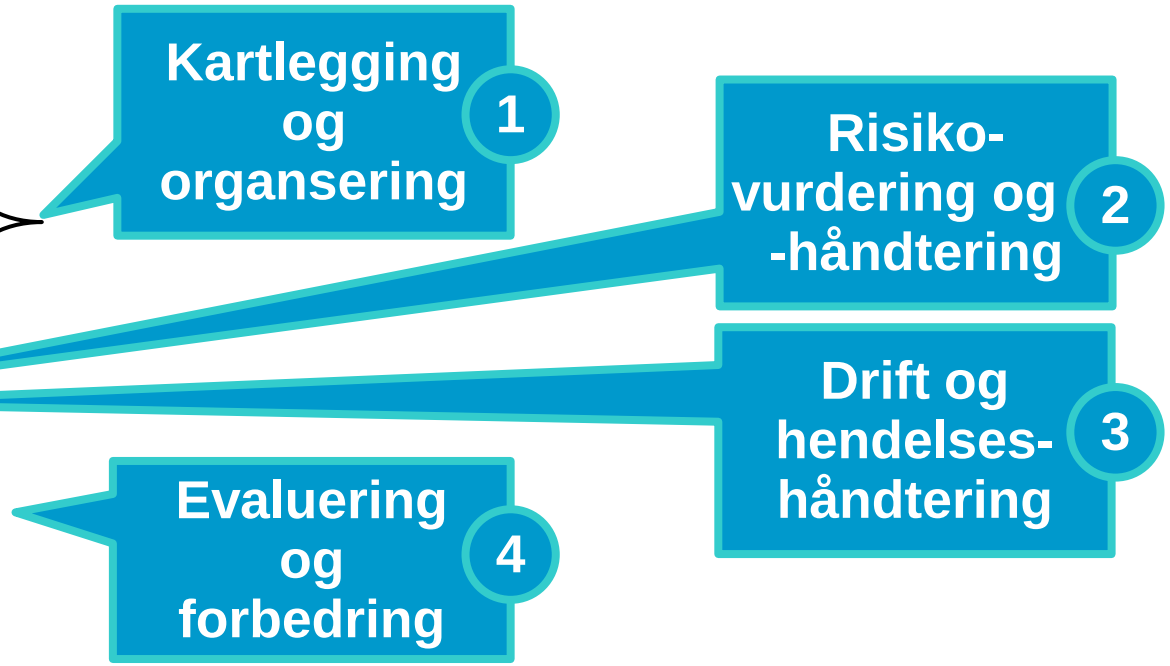
ISMS (Information Security Management System)
Styringssystem for informasjonssikkerhet

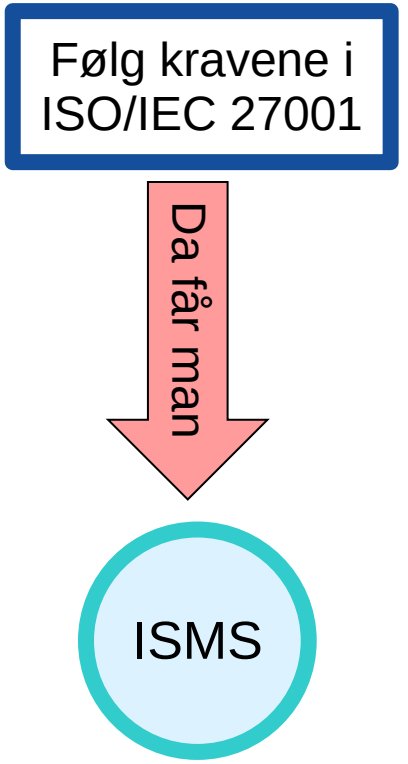


- ISMS har prosesser som kan illustreres som en syklus med 4 faser.
- Syklusen er kun en visuell fortolkning av ISMS som beskrevet i ISO/IEC 27000.
- Fasene utføres i parallell.
- God styring av informasjonssikkerhet krever gode prosesser i hver fase.

ISO/IEC 27001 – Hva er det?

- *ISO/IEC 27001 ISMS – Krav*, spesifiserer nettopp **krav** til å etablere, implementere, vedlikeholde og kontinuerlig forbedre virksomhetens styringssystem for IS.
- Ved å følge kravene i ISO/IEC 27001 vil virksomheten ha et operativt ISMS.
- Kravkategorier:
  - A. Kontekst
  - B. Lederskap
  - C. Planlegging
  - D. Støtte
  - E. Drift
  - F. Evaluering
  - G. Forbedring



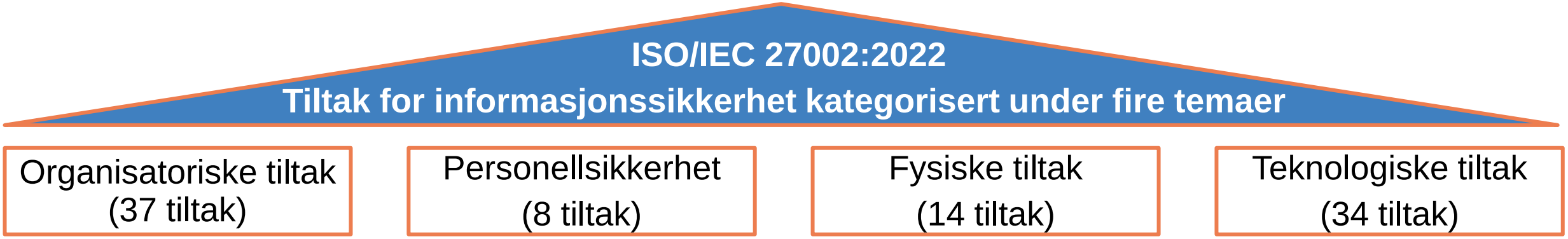


- Virksomheter kan sertifiseres etter ISO/IEC 27001
  - ... ved å vise at de oppfyller alle kravene

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 abstrakte temaer



- 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	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.

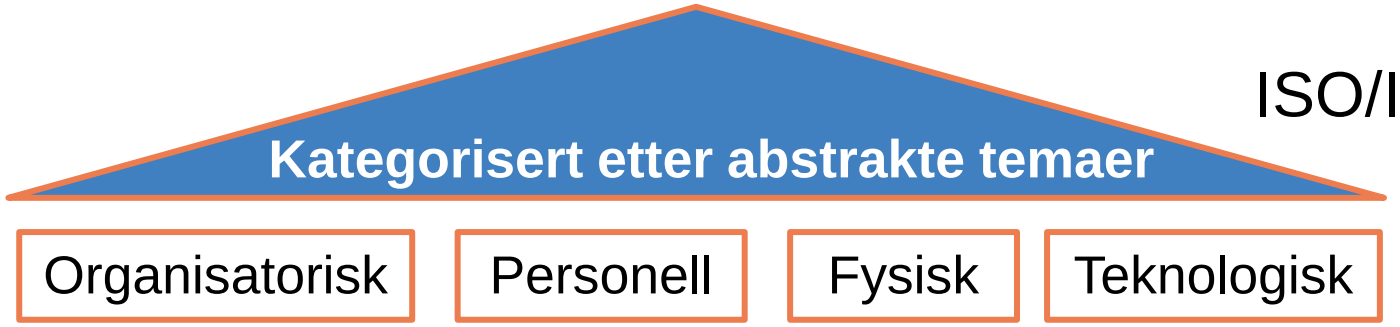
Formål

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

Typer kategorisering av informasjonssikkerhetstiltak

1. :

ISO/IEC 27002:2022



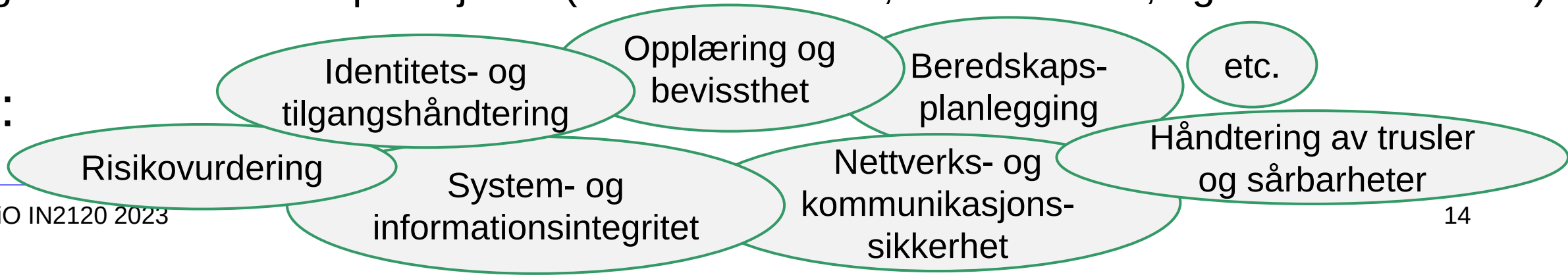
Kategorisert etter styringsprosesser (NSM grunnprinsipper og NIST CSF)

2. :

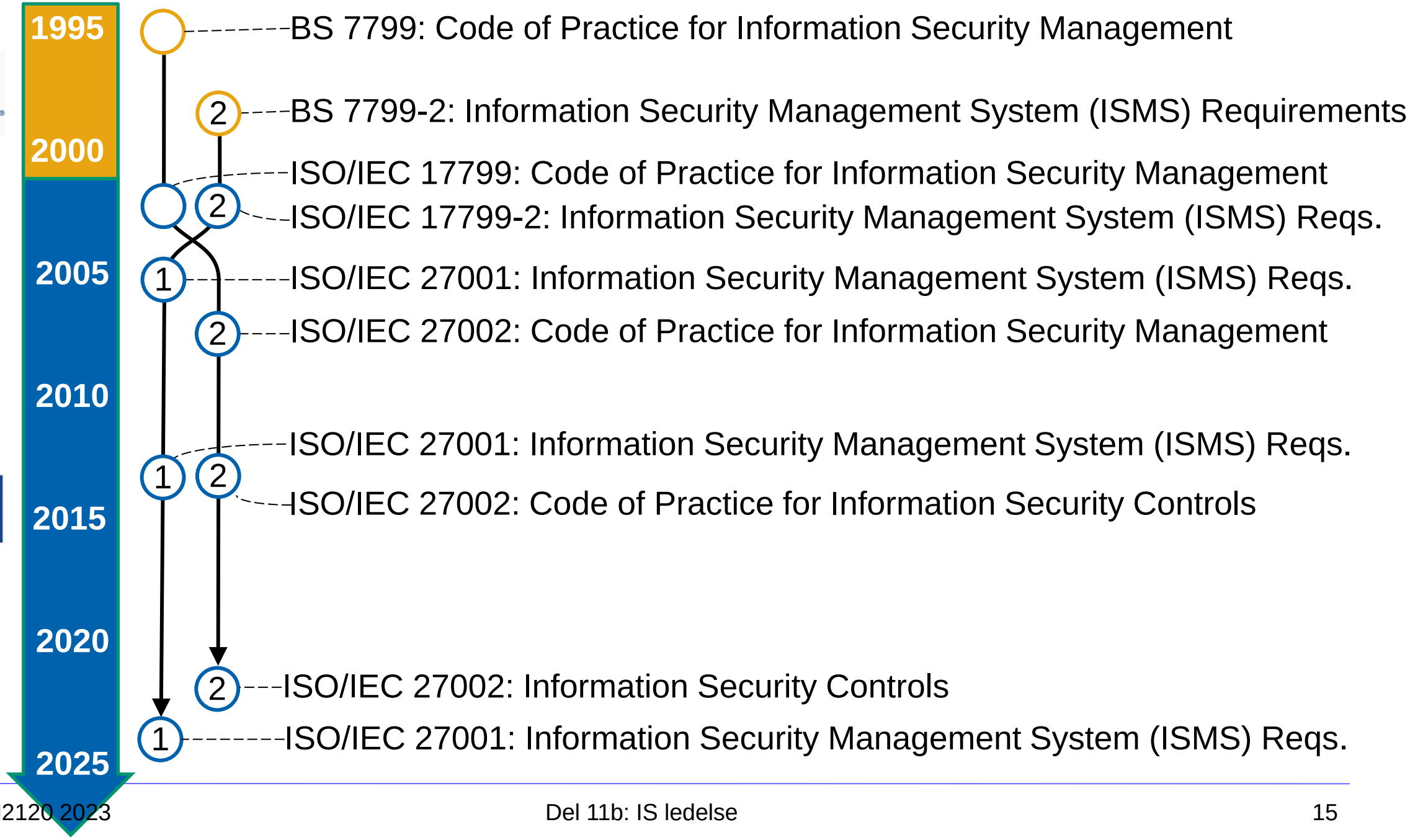
1. **Identifisere og kartlegge**
2. **Beskytte og opprettholde**
3. **Oppdage**
4. **Håndtere og gjenopprette**

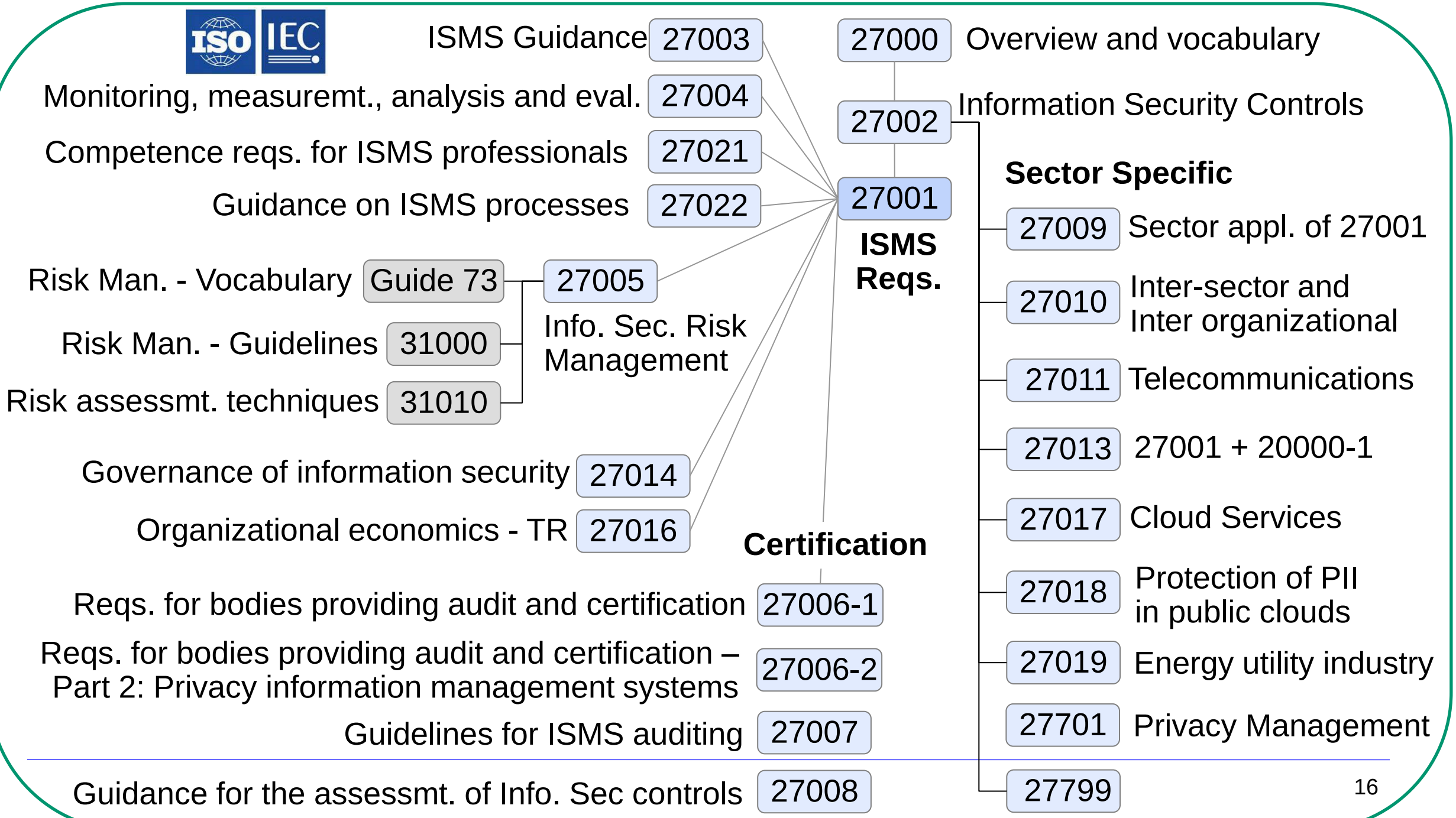
Kategorisert etter driftsoperasjoner (NIST SP 800-53, CIS Controls, og ISO 27002:2013)

3. :



Historien bak 27001 og 27002




ISMS Guidance
27003
Monitoring, measuremt., analysis and eval.
27004
Competence reqs. for ISMS professionals
27021
Guidance on ISMS processes
27022
Risk Man. - Vocabulary
Guide 73
Risk Man. - Guidelines
31000
Risk assessmt. techniques
31010
27005
Info. Sec. Risk Management
Governance of information security
27014
Organizational economics - TR
27016
27000
Overview and vocabulary
27002
Information Security Controls
27001
ISMS Reqs.
Sector Specific
27009
Sector appl. of 27001
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
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

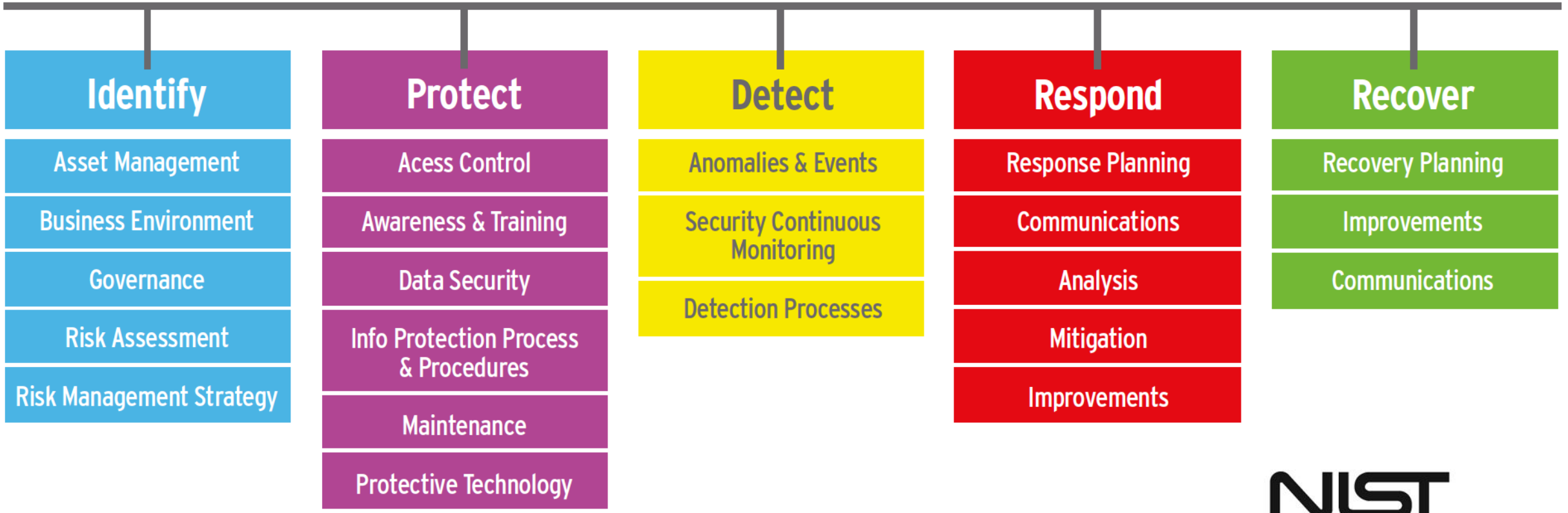
NIST Cyber Security Framework

- Publiseres gratis av NIST (US National Institute of Standards and Technology).
- Er ment å støtte føderale etater til å redusere cybersikkerhetsrisiko.
- Beskriver 5 funksjoner/styringsprosesser med tilhørende sikkerhetstiltak
  1. Identify
  2. Protect
  3. Detect
  4. Respond
  5. Recover

  } Kategorisering etter 5 styringsprosesser (CSF functions)
- Refererer og kartlegger til sikkerhetstiltakene i NIST SP800-53 og ISO/IEC 27002.
- Er basert på eksisterende standarder, retningslinjer og beste praksis.
- Beskriver en metodikk for å vurdere og forvalte sikkerhetstiltak.
- Gir også veiledning om beskyttelse av personvern og sivile friheter i en cybersikkerhetskontekst.
- Er i ustrakt bruk av virksomheter i mange land, deriblant i Norge.
- Kan brukes sammen med ISO/IEC 27001 ved kartlegging av tiltak.

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

NIST Cyber Security Framework



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

NSM Grunnprinsipper for IKT-sikkerhet

- NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk.
- 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 styringsprosesser

- 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

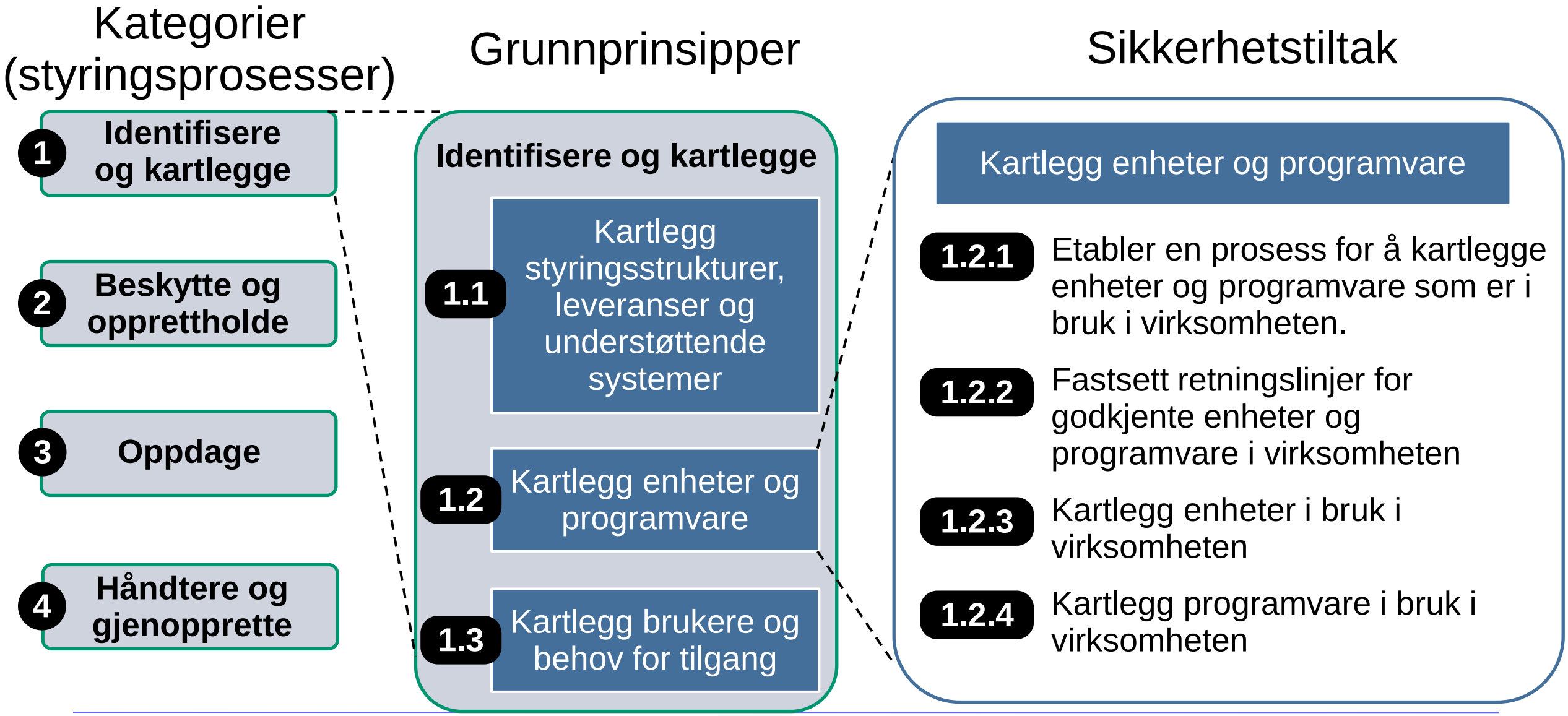
- Oppdag og fjern kjente sårbarheter
- Etabler sikkerhets-overvåking
- Analyser data fra sikkerhetsovervåking
- Gjennomfør inntrengingstester

4 Håndtere og gjenopprette

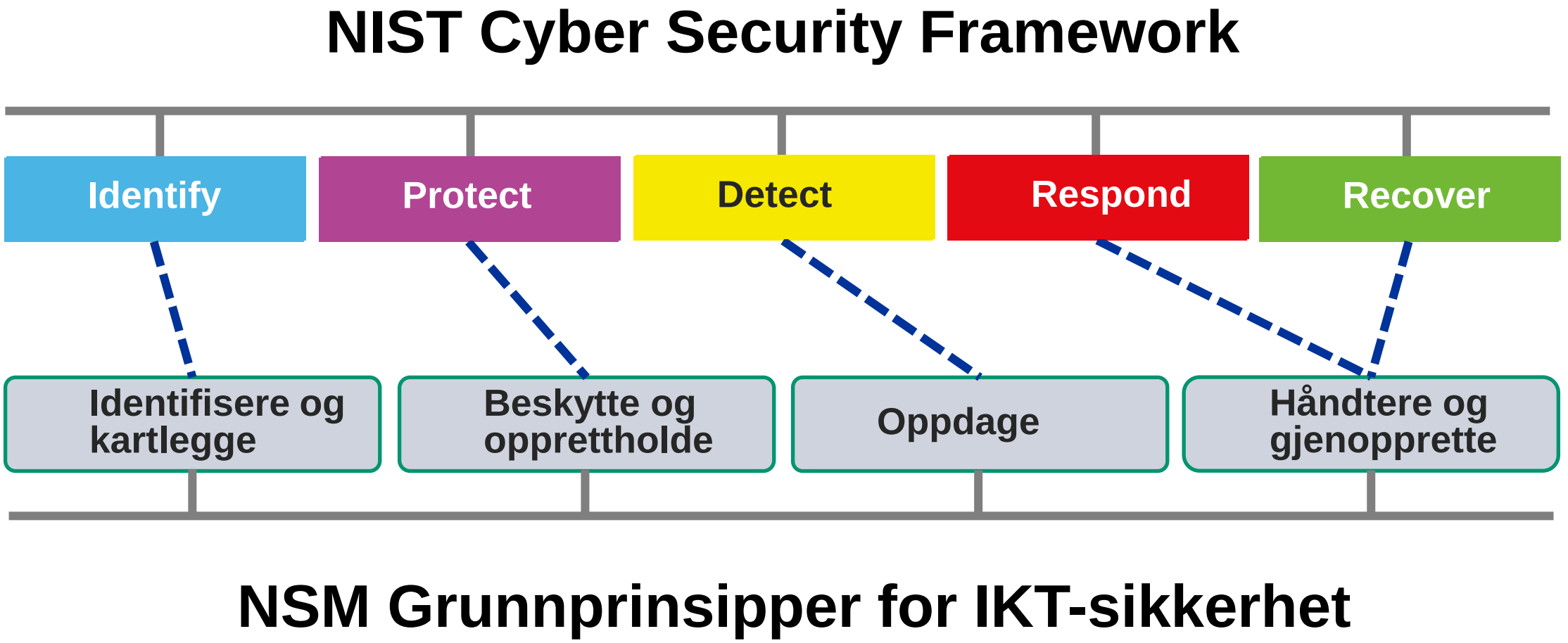
- Forbered på håndtering av hendelser
- Vurder og klassifiser hendelser
- Kontroller og håndter hendelser
- Evaluer og lær av hendelser

NSM

Struktur i NSM Grunnprinsipper for IKT-sikkerhet



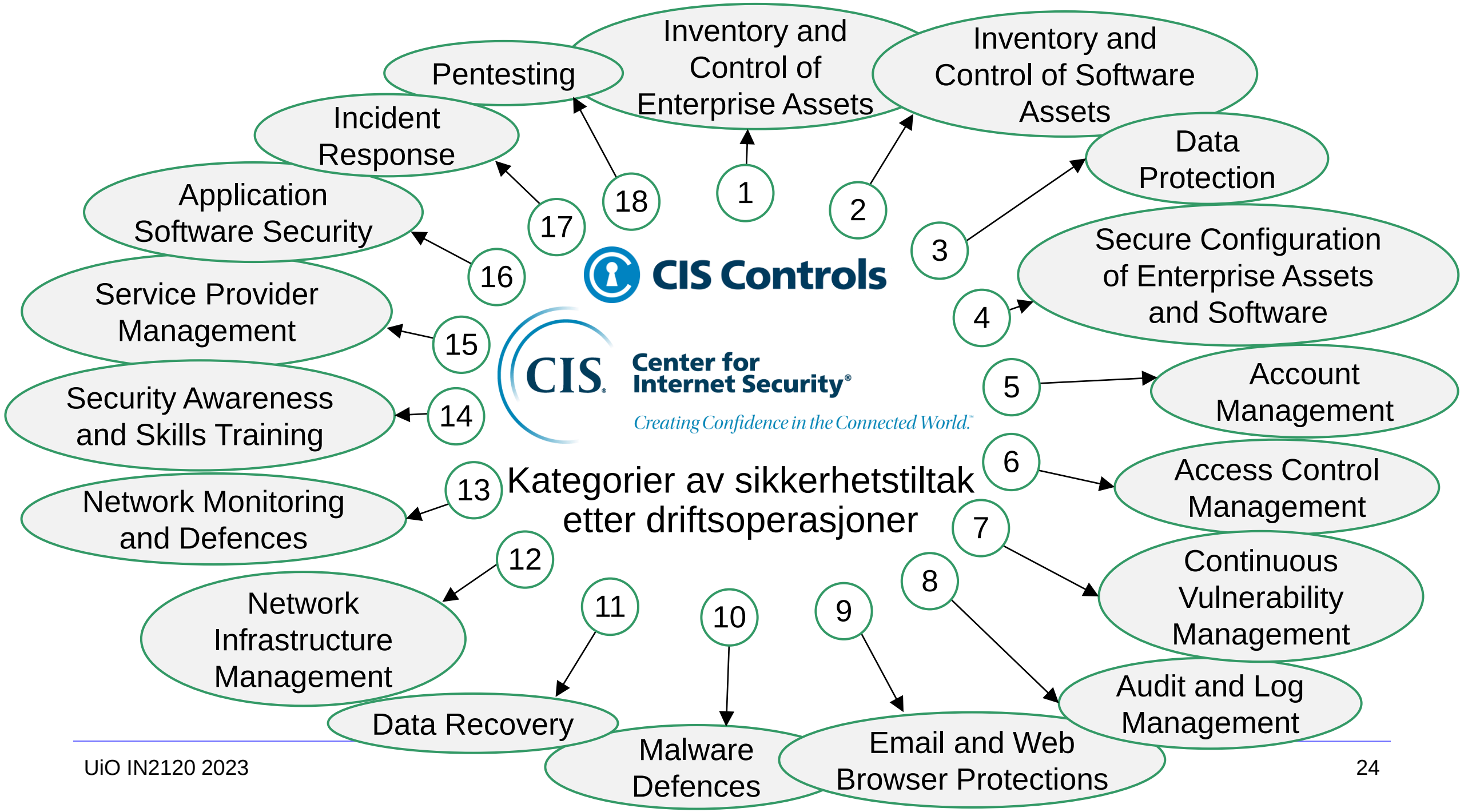
Kartlegging mellom NIST CSF og NSM grunnprinsipper



Sammenheng mellom NIST Cyber Sec Framework og NSMs grunnprinsipper for IKT-sikkerhet

NIST Cybersecurity Framework	NSMs grunnprinsipper for IKT-sikkerhet
5 funksjoner (functions)	4 kategorier
23 kategorier (categories)	21 grunnprinsipper
108 underkategorier (subcategories)	118 sikkerhetstiltak

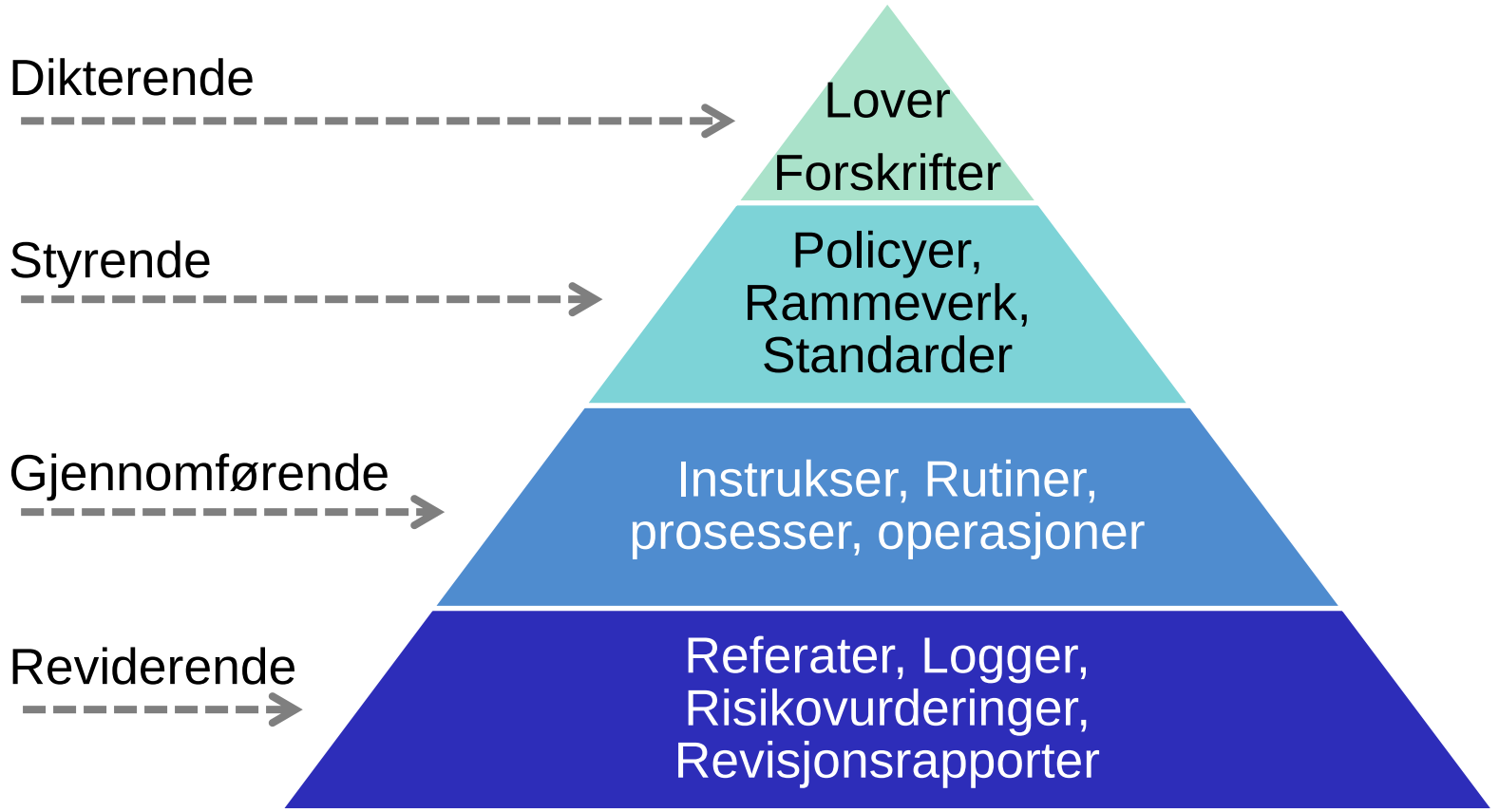
- NIST CSF og NSMs grunnprinsipper har likhetstrekk
- Kategoriserer sikkerhetstiltak etter naturlige faser (NIST functions eller NSM kategorier)


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

Fra IS-rammeverk til ISMS

- Intet enkelt IS-rammeverk dekker alle behov
  - Ulike organisasjoner har forskjellige behov
  - Hvert enkelte rammeverk/standard har et begrenset fokus
  - En komplett strategi må baseres på ulike rammeverk/standarder
- Velg de mest egnede rammeverk
- Definering av egne policyer
- Virksomhetens ISMS bygges med utvalgte rammeverk og egne policyer

Dokumenthierarki



Elementer i sikkerhetspolicyer

- Sette tonen fra ledelsen mhp. informasjonssikkerhet
- Etablere roller og ansvar, finansiering
- Definere klassifisering av verdier/aktiva
- Definere autoritetsstrukturer og beslutningsprosesser
- Gi et grunnlag for bruk av standarder og rammeverk
- Sette krav til sporbarhet
- Definer akseptabel bruk av utstyr og eiendom
- Definer ansvar for overholdelse av juridiske krav

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

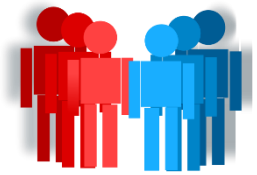
Definere sikkerhetsmålsettinger,
Etablere organisering av informasjonssikkerhet,
Godkjenne sikkerhetspolicyer, risikovurderinger og risikohåndtering

CISO
PVO
Ledere for IS og PV

Chief Information Security Officer - Leder av SIS (Styringsgruppe for IS)
Chief Risk Officer (CRO)
Personvernombud (PVO)
Koordinerer arbeidet med informasjonssikkerhet og personvern

SIS (Styringsgruppe for info.sikkerhet)

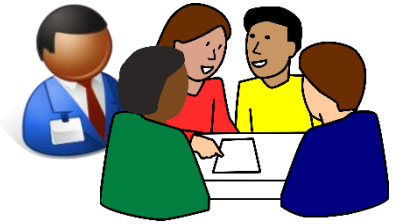
Representanter (eiere) for ulike forretningsområder
Samordning og balansering av (IT-)sikkerhetsprogrammet
Utføring av risikovurderinger
Vurdering av personvernkonsekvens (DPIA)



Drift og SOC-team

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

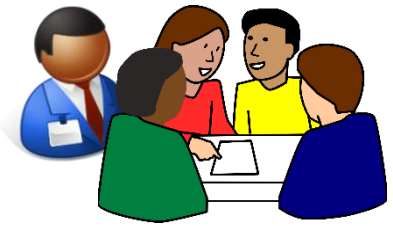
SIS: Styringsgruppe for informasjonssikkerhet



- Å etablere en styringsgruppe for informasjonssikkerhet (SIS) er viktig for å opprettholde god styring av informasjonssikkerhet.
- SIS 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 SIS. 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 SIS

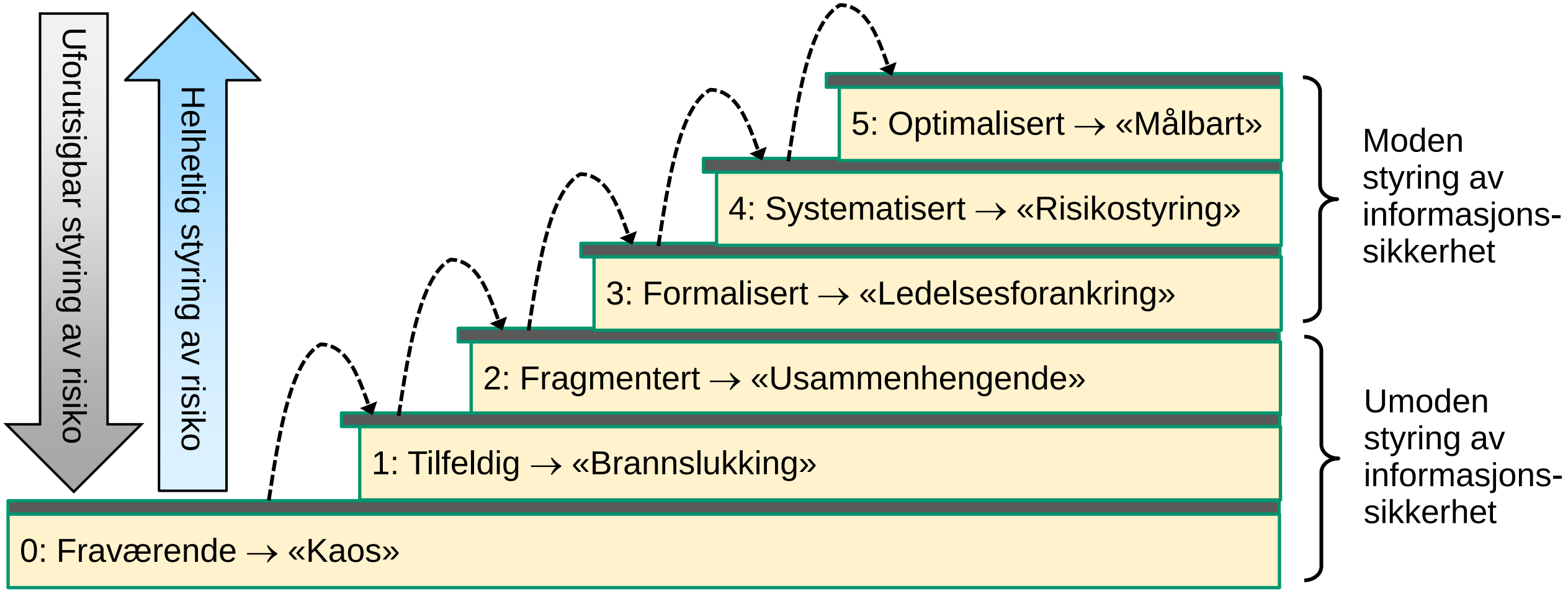
- Medlemmer i SIS representerer forretningsinteresser, noe som sikrer at sikkerhetsprosjekter og tiltak er strategisk tilpasset forretningsmålene.
- SIS må identifisere viktige organisatoriske spørsmål og utfordringer knyttet til informasjonssikkerhet.
- SIS lager policyer for informasjonssikkerhetsprogrammet.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



Kommunisere sikkerhet til toppledelse og styre

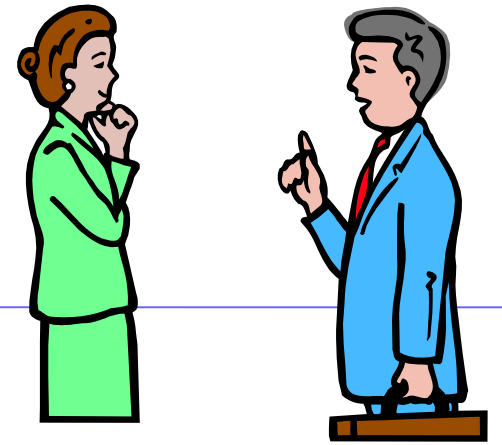
- Fokus på:
  - Vise sammenfallende målsettinger for sikkerhet og forretningsstrategi
  - Forklare oppdatert trusselbilde og identifiserte risikoer
  - Forklare målsettinger med sikkerhetsarbeidet
  - Spesifisere budsjettposter slik at toppledelsen kan tallfeste kostnadene for sikkerhetsprogrammet
  - 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.

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



Spørsmål ledelsen bør stille seg selv

1. Hvordan holder virksomheten seg oppdatert om cybertrusler generelt, og for egen sektor og virksomhet spesielt?
2. Har virksomheten god oversikt og forståelse av risiko relatert til informasjonssikkerhet?
3. Hvor godt er risikostyring for informasjonssikkerhet integrert i helhetlig risikostyring?
4. Bør cyberforsikring inkluderes i virksomhetens forsikringspoliser?
5. Hvor modent er virksomhetens ISMS?
6. Hvor godt er ISMS forankret hos ledelsen?
7. Jobbes det med god sikkerhetskultur som del av virksomhetskulturen generelt?
8. Dekker beredskapsplanen også cybersikkerhetshendelser, og er planen testet?
9. Hvor god er virksomhetens etterlevelse av lover og forskrifter relatert til informasjonssikkerhet?
10. I hvilken grad bør virksomheten outsource sikkerhetsfunksjoner, som f.eks. gjennom å kjøpe MSS (sikkerhetstjenester)?
11. Hvor god er beskyttelsen av informasjon som overføres til tredjeparter?
12. Hvor god er virksomhetens etterlevelse av GDPR?



Slutt på presentasjonen