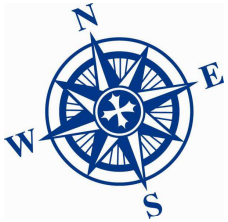
IN5080
Sikkerhets- og risikostyring

Del 5:
Styring og ledelse av informasjonssikkerhet

Audun Jøsang
Universitetet i Oslo
Vår 2024

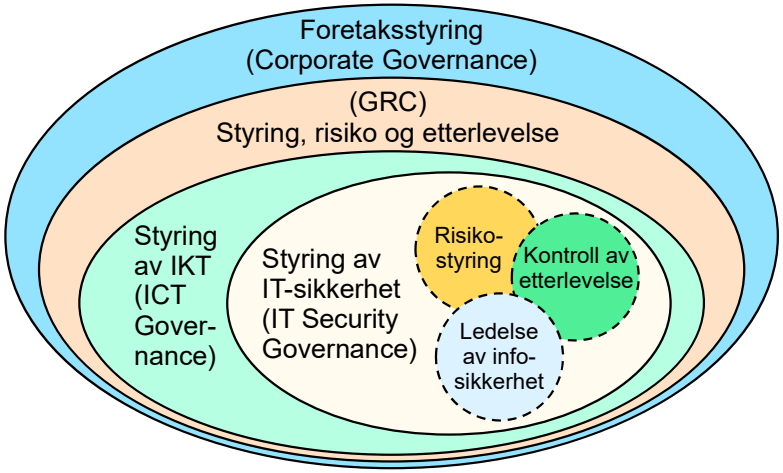
Oversikt styring og ledelse av informasjonssikkerhet

Del A: Standard og rammeverk for styring og ledelse av IS
- Styring (Governance) og ledelse (Management) av IS
- ISMS - Styringssystem for informasjonssikkerhet
- Standarder og rammeverk for informasjonssikkerhet



Del B: Forvaltning av ISMS
- Organisasjonsstruktur rundt informasjonssikkerhet
- Program for informasjonssikkerhet
- Måling av sikkerhetstiltak
- Modenhet av sikkerhetsstyring

Styringskategorier

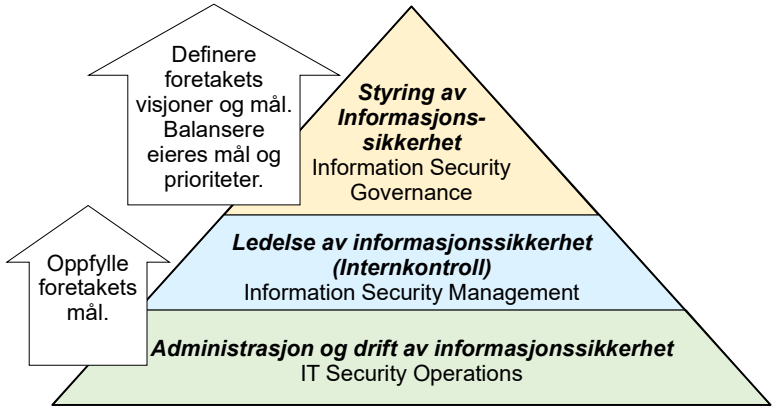


Foretaksstyring

<u>Ansvarsområder for styre og toppledere:</u>

- Definere strategiske målsettinger
  - profitt, yte gode tjenester, godt omdømme (ikke havne på førstesiden i VG)
  - etc.
- Vurdere i hvilken grad målsettinger oppnås
- Sette krav til, og vurdere håndteringen av risiko
- Sørge for at virksomheten forvaltes på lovlig og etisk måte

Abstraksjonsnivåer 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 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
- 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 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

Etterlevelse (compliance): Å følge lover, forskrifter og policyer

- Lovgiving og regulering, f.eks.
  - Nasjonale lover og forskrifter (f.eks. sikkerhetsloven)
  - Internasjonale lover og forskrifter (f.eks. GDPR, Basel II)
  - Lover og forskrifter håndheves av nasjonale myndigheter
    - Krav om etterlevelse fra ekstern revisor (privat sektor)
    - Krav om etterlevelse fra direktorater og Riksrevisjonen (statlig sektor)
    - Foretaksstraff gjennom direktorater og domstoler
- Foretakspolicyer
  - Spesifiserer
    - Styrende sikkerhetspolicyer (mål og strategi)
    - Gjennomførende sikkerhetspolicyer (plan, risikostyring, prosesser)
    - Reviderende policyer(avvikshåndtering og sikkerhetsrevisjon)
  - Avvik fra policyer skal oppfølges og lukkes

Standarder og rammeverk for styring og ledelse av IS

- 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

Eksempler på ISO-standarder for styrings- og ledelsessystemer

- ISO 9001 Quality Management
  - ➢ Kvalitetsledelse
- ISO/IEC 20000 Service Management
  - ➢ Tjenesteledelse
- ISO 22300 Security and Resilience
  - ➢ Samfunnssikkerhet
- ISO/IEC 27001(ISMS: Information security management System)
  - ➢ Ledelsessystem for informasjonssikkerhet
- ISO 31000 Risk management
  - ➢ Risikostyring
- ISO 39001 Road Safety Management System
  - ➢ Styringssystem for trafikksikkerhet
- ISO 22000 Food Safety Management System
  - ➢ Ledelsessystem for næringsmiddeltrygghet

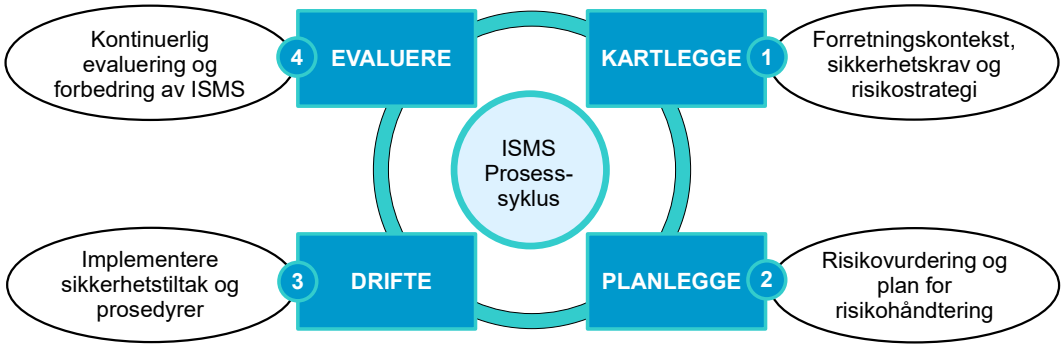
ISO/IEC 27000 – Hva er det?

- *ISMS: Information security management systems - Overview*
- Definerer begreper for informasjonssikkerhet
- Gir en oversikt over andre standarder i 27000-serien
- Gir generell beskrivelse av ISMS (styrings-/ledelsessystem for IS)
- 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

Krav til styrings-/ledelsessystem for informasjonssikkerhet

- Standarden beskriver krav til ISMS, som kan deles inn i en syklus med 4 faser.
- Syklusen er kun en visuell fortolkning av ISMS-krav som beskrevet i ISO/IEC 27001.
- Fasene utføres i parallell.
- God styring av informasjonssikkerhet krever fungerende prosesser i hver fase.



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

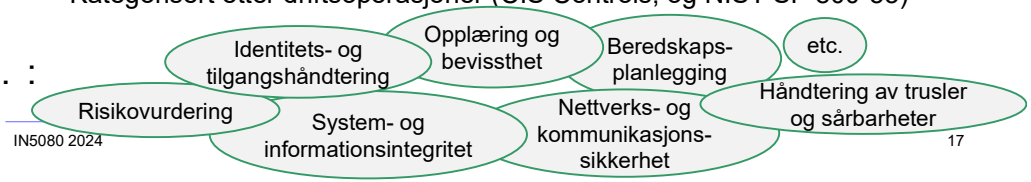
- Styringssystem (ISMS) og ledelsessystem (LSIS) for IS har samme betydning.
- Digdir benytter betegnelsen «internkontroll» omtrent med betydning ISMS/LSIS.
  - Internkontroll/ styringssystem/ ledelsessystem for informasjonssikkerhet | Digdir
- Privat og statlig sektor (NSM) benytter vanligvis begrepet 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».

Typer kategorisering av tiltak for informasjonssikkerhet

1. : ISO/IEC 27002:2022

2. : Kategorisert etter styringsprosesser (NSM grunnprinsipper og NIST 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

ISO/IEC 27002:2022
Tiltak for informasjonssikkerhet kategorisert i fire domener

Organisatoriske tiltak (37 tiltak)	Personellsikkerhet (8 tiltak)	Fysiske tiltak (14 tiltak)	Teknologiske tiltak (34 tiltak)

- 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

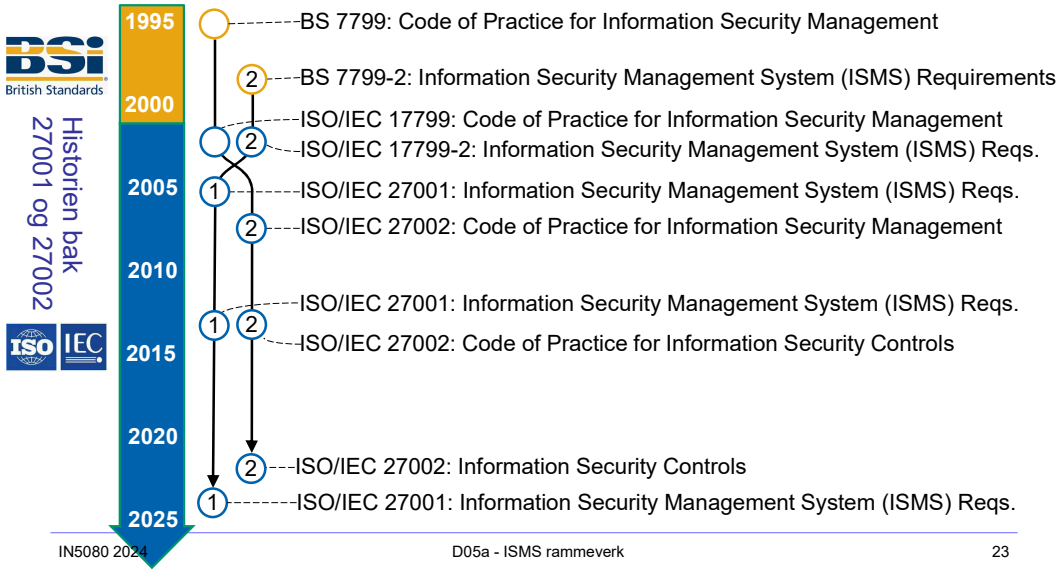
Informasjon knyttet til trusler mot informasjonssikkerheten bør samles inn og analyseres for å produsere trusseletterretning.

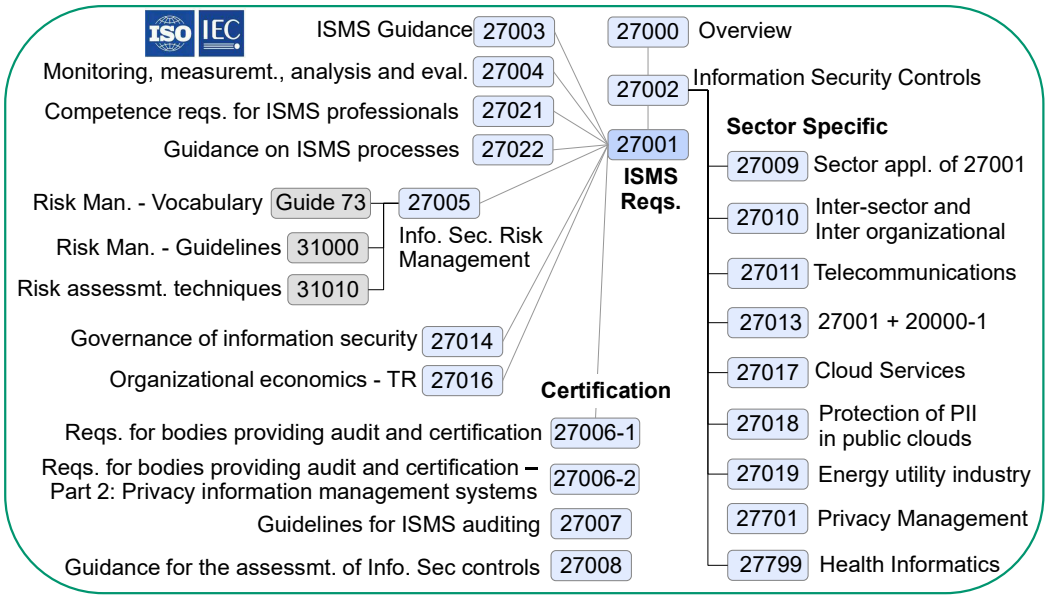
Formål

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

Attributtkategorier i ISO/IEC 27002:2022

- **Type sikkerhetstiltak**
  - #Forebyggende, #Oppdagende, #Korrigerende.
- **Informasjonssikkerhetsegenskaper**
  - #Konfidendialitet, #Integritet, #Tilgjengelighet.
- **Cybersikkerhetskonsepter** (tilsvarer NIST CSF og NSM Grunnprinsipper)
  - #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.



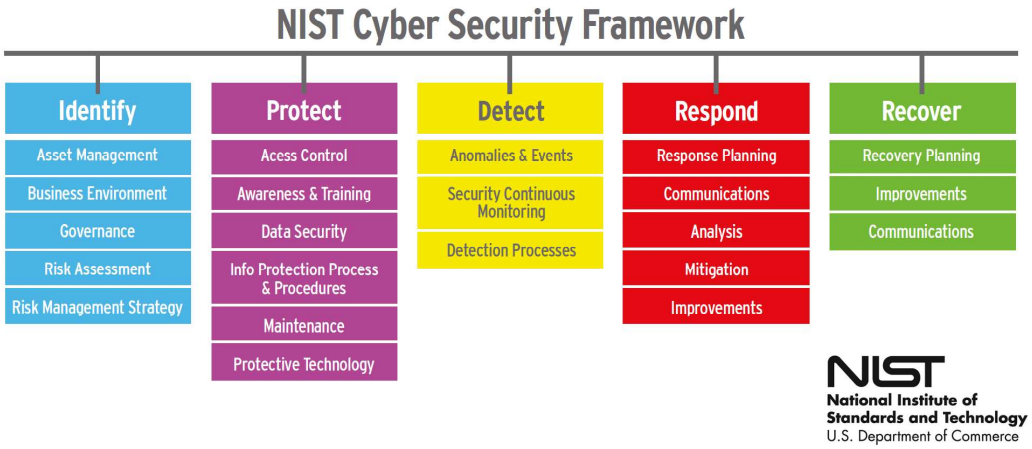


NIST Cyber Security Framework

- 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 ISO/IEC 27002 og NIST SP800-53.
- 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.

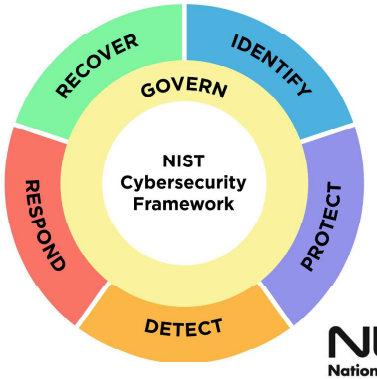
NIST National Institute of Standards and Technology U.S. Department of Commerce



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

2023 utkast til revidert NIST CSF 2023

- **GOVERN** er ny generell funksjon
- Økt fokus på alle typer virksomheter, ikke bare kritisk infrastruktur
- Forbedret veiledning for bruk av CSF, bl.a. med profiler for ulike typer virksomheter, og eksempler på bruk av CSF.



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

NSM Grunnprinsipper for IKT-sikkerhet

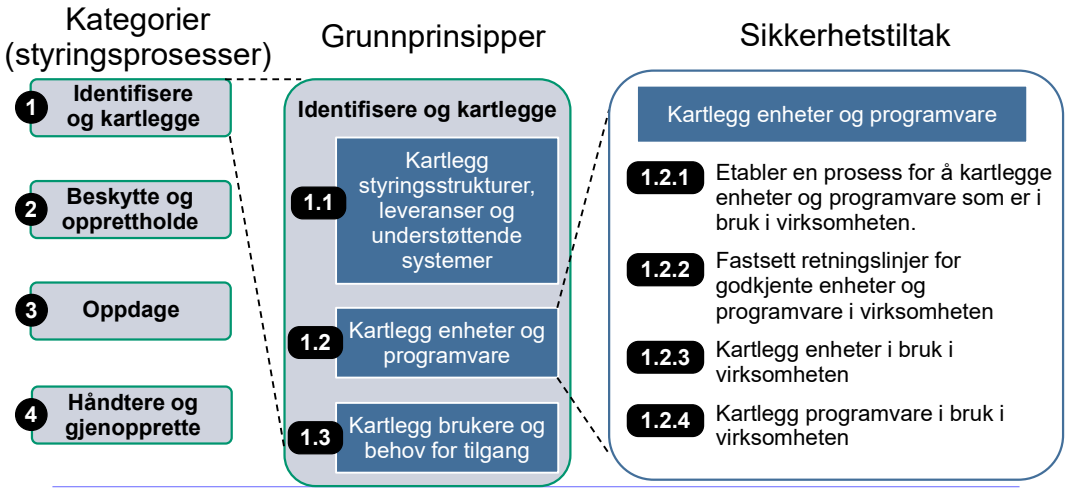
- NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med sikkerhetstiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk.
  - https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt
- Publiseres gratis for 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 styringsprosesser

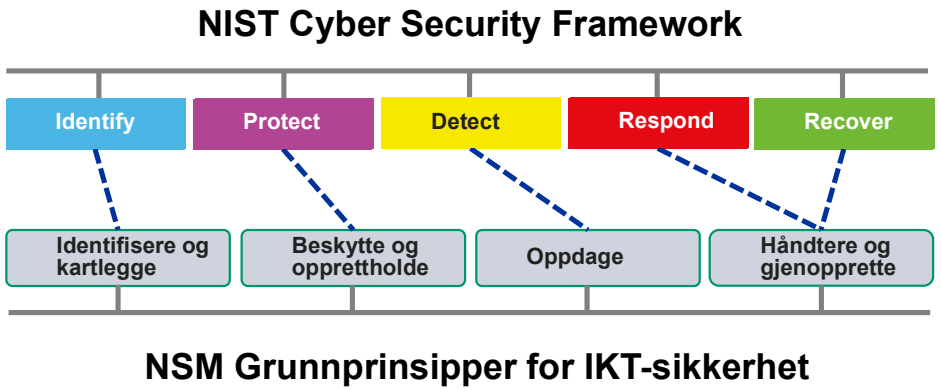
- Kategoriene ligner på NIST Cybersecurity Framework
- Hvert tiltak er merket med prioriteringsgruppe 1, 2 eller 3
- 90% av sikkerhetshendelser kan unngås ved å implementer alle tiltak i gruppe 1
- En SoA (Statement of Applicability) i henhold til ISO/IEC 27001 krever en kartlegging mellom tiltak fra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

Grunnprinsipper for IKT-sikkerhet

Struktur i NSM Grunnprinsipper for IKT-sikkerhet



Sammenheng mellom NIST CSF og NSM grunnprinsipper



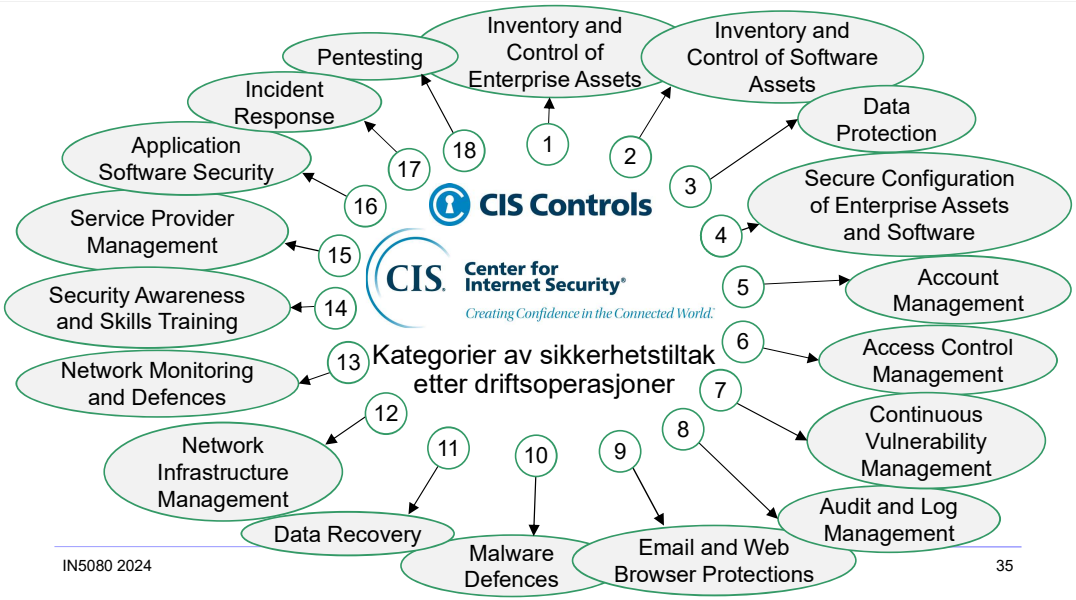
Sammenheng mellom NIST Cyber Sec Framework og NSMs grunnprinsipper for IKT-sikkerhet

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 prosesser (NIST functions eller NSM kategorier)

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 personvern som standard
- CIS / SANS
  - Critical Security Controls

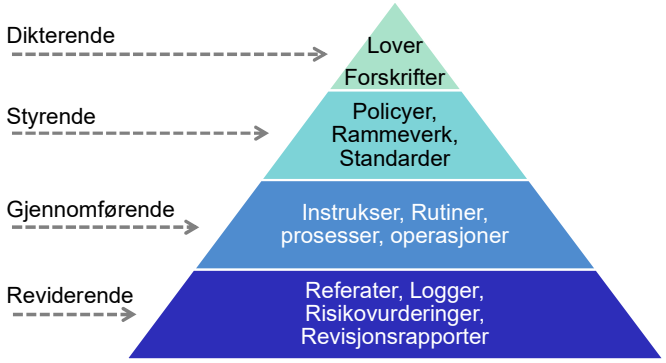


The 20 Security Control Categories of NIST SP 800-53: 2020

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
  - En komplett strategi må baseres på ulike rammeverk/standarder
- Velg de mest egnede rammeverk
- Definering av egne policyer
- Virksomhetens ISMS/LSIS bygges med utvalgte rammeverk og egne policyer
- Eksempel: UiO LSIS
  - https://www.uio.no/tjenester/it/sikkerhet/lsis/

Dokumenthierarki



DEL B: ISMS FORVALTNING

Oversikt

- Organisasjonsstruktur rundt informasjonssikkerhet
- Program for informasjonssikkerhet
- Måling av sikkerhetstiltak
- Modenhet av sikkerhetsstyring

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 Definere sikkerhetspolicyer 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.

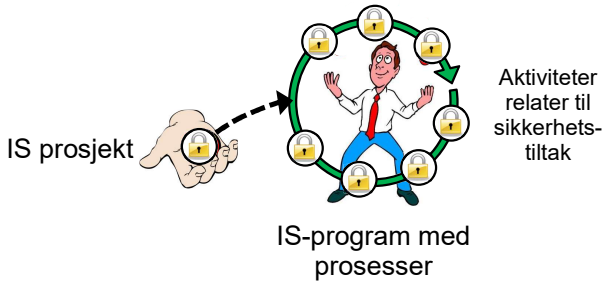
Oppgaver for SIS

- 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.
- SIS utfører, eller tar initiativ til, intern revisjon av ISMS

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 mangel på samsvar med forskrifter
  - Organisere strategiseminar for informasjonssikkerhet med toppledelsen og styret.

IS-program = et sett med IS-aktiviteter

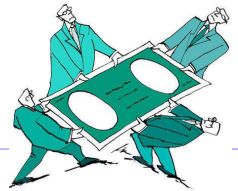


- Et IS-prosjekt skiller seg ut fra driften av sikkerhetstiltaket.
- Når prosjektet er fullført, er sikkerhetstiltaket operativt som en prosess.

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
  - Produkt og leveranser
  - Konsulentkostnader
  - Plassbehov (kontorplass, IT-utstyr)
  - Ressursbruk for testing (personell, systemtid)
  - Dokumentasjonsutvikling
  - Behov for drift og vedlikehold
  - Overhead i oppstartfasen
  - Planer ved uforutsette kostnader

4P: People, Process, Product, Partner



Måling av sikkerhet og sikkerhetstiltak

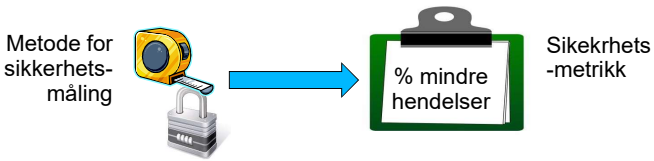
- Hva er effekten av et sikkerhetstiltak?
  - Du må måle det for å vite det.
- Måling av sikkerhet og sikkerhetstiltak gir
  - info om hvor godt sikkerhetstiltakene fungerer
  - grunnlag for å sammenligne effekten av risikostyring
  - referanse for nyttevurdering av sikkerhetsinvesteringer

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."

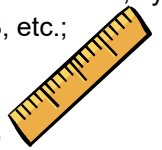
Hva er en sikkerhetsmetrikk?

- 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.



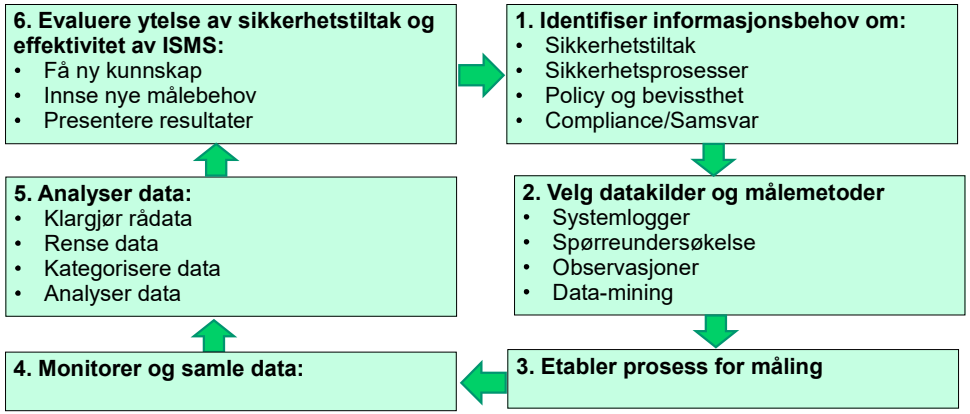
Data typer

- 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

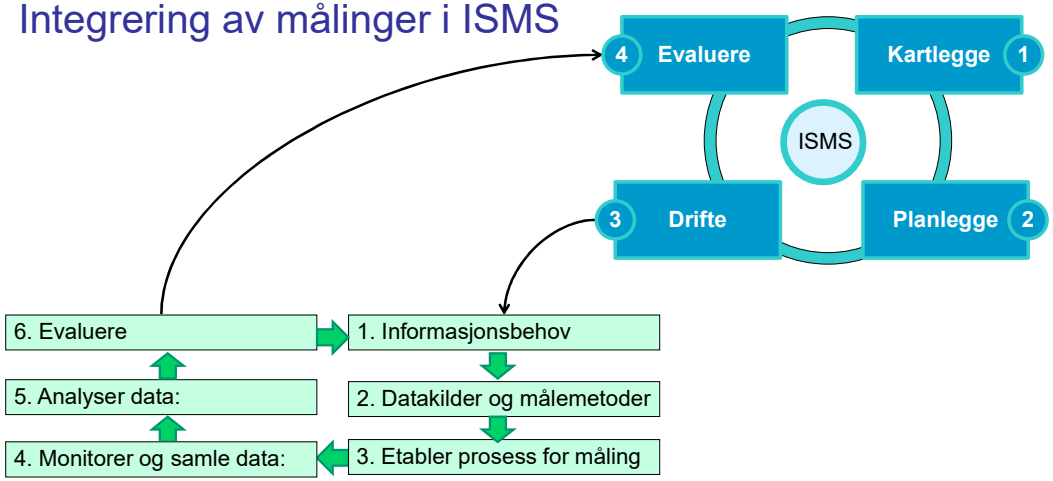


- Kvalitative data
  - Tekst
  - Utsagn
  - Kategorier
  - Multimedia

Modell for sikkerhetsmåling (ISO/IEC 27004)

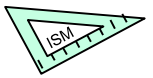


Integrering av målinger i ISMS



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

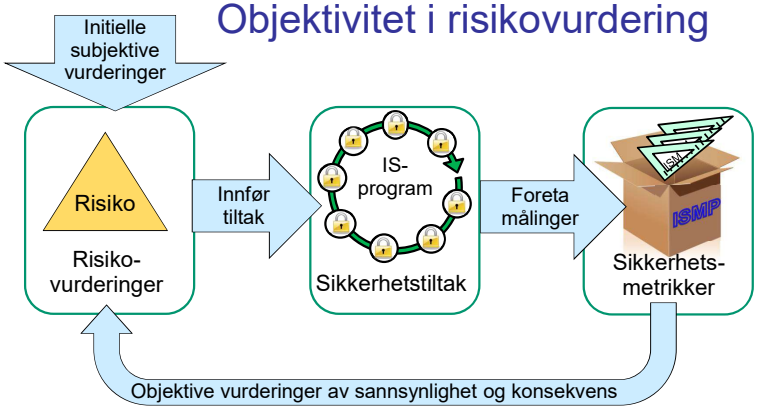
Eksempler på sikkerhetsmetrikker

- System
  - Antall kritiske sårbarheter oppdaget med sårbarhetsskanning
- Nettverk
  - Mengde og type åpne porter funnet med DMZ-portskanninger
- Antall svake passord som kan knekkes
  - % av knekkbare passord oppdaget ved å kjøre et krakkeverktøy på passorddatabasen
- Antall hendelser (per år) av hver alvorlighetskategori
  - Statistikk av hendelsesstyper/-alvorlighetskategorier
- Tid det tar å oppdage infisering (eng. MTTD: Mean Time To Detect)
  - Statistikk av tiden mellom første infisering til infiseringen/hendelsen faktisk oppdages
- Tid det tar å håndtere hendelse (eng. MTTR: Mean Time To Recovery)
  - Statistikk over tiden mellom oppdaging av hendelse og gjenoppretting
- Industri
  - Antall sikkerhetshendelser i sektoren med alvorlighetsgrad Z
- Politisk
  - Antall trusselaktører som utpeker sektor / selskap ABC som potensielt angrepsmål

Målinger ⇒ Forpliktelser

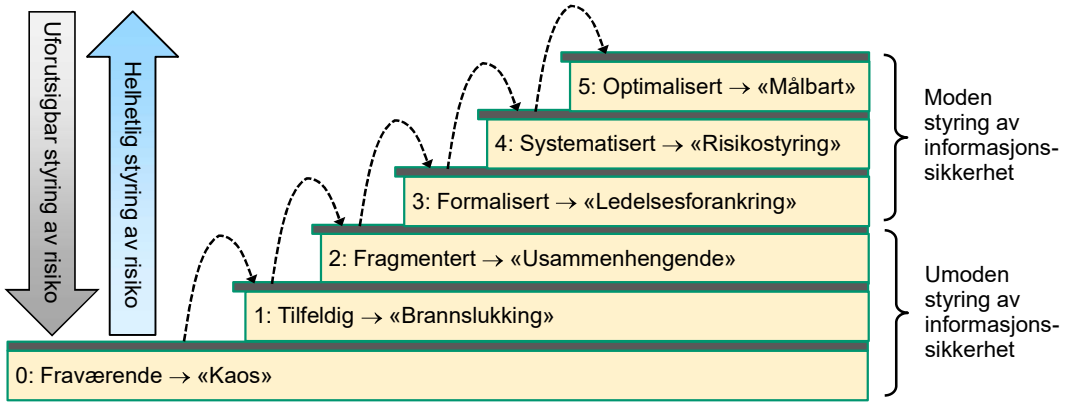
- Sikkerhetsmåling kan bli en forpliktelse
  - Kunnskap om mangler i sikkerhetstiltak skaper en forpliktelse til å gjøre noe med det.
  - Hendelser som følge av kjent – men forsømt – svakhet har ansvar
  - Aktsomhetsprinsippet (eng. due care), dvs. gjøre som forventet av virksomheter i samme situasjon
- Måling uten oppfølging = sløsing med penger!
  - Bruk av sikkerhetsbudsjett i stedet for å redusere risikoen.
- Vær forberedt på oppfølging når du starter et ISMP

Objektivitet i risikovurdering



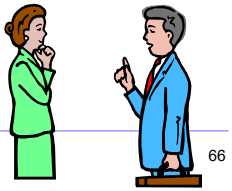
- Initielle risikovurderinger er subjektive
- Risikovurderinger blir objektive når de er basert på objektive sikkerhetsmålinger.

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



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. Har ledelsen tilstrekkelig kompetanse om informasjonssikkerhet?
4. Hvor godt er risikostyring for informasjonssikkerhet integrert i helhetlig risikostyring?
5. Bør cyberforsikring inkluderes i virksomhetens forsikringspoliser?
6. Hvor modent er virksomhetens ISMS?
7. Hvor godt er ISMS forankret hos ledelsen?
8. Jobbes det med god sikkerhetskultur som del av virksomhetskulturen generelt?
9. Dekker beredskapsplanen også cybersikkerhetshendelser, og er planen testet?
10. Hvor god er etterlevelsen av lover og forskrifter om informasjonssikkerhet og personvern?
11. Hvor god er beskyttelsen av informasjon som overføres til tredjeparter?
12. I hvilken grad bør virksomheten outsource sikkerhetsfunksjoner, som f.eks. gjennom å kjøpe MDR (Managed Detection and Response)?



Slutt på presentasjonen