HVILKE RISIKOER LØPER VI NÅR ALLE DATAENE VÅRE ER I NETTSKYEN?

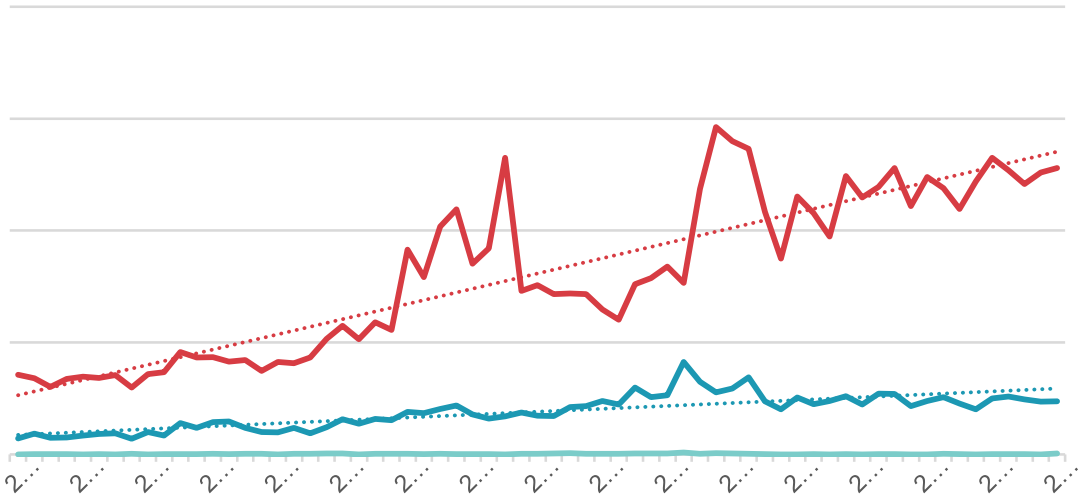
Bente Hoff
Seksjonssjef Strategisk IKT-sikkerhet
NSM

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet.

Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser.

ØKNING I ANTALL CYBERHENDELSER

- Antall hendelser øker
- Alvorlige angrep blir mer komplekse



TRUSSELAKTØRENE

Krise / krig

Sabotasje

Spionasje

Økonomisk krim

Politiske protester

Rampestreker

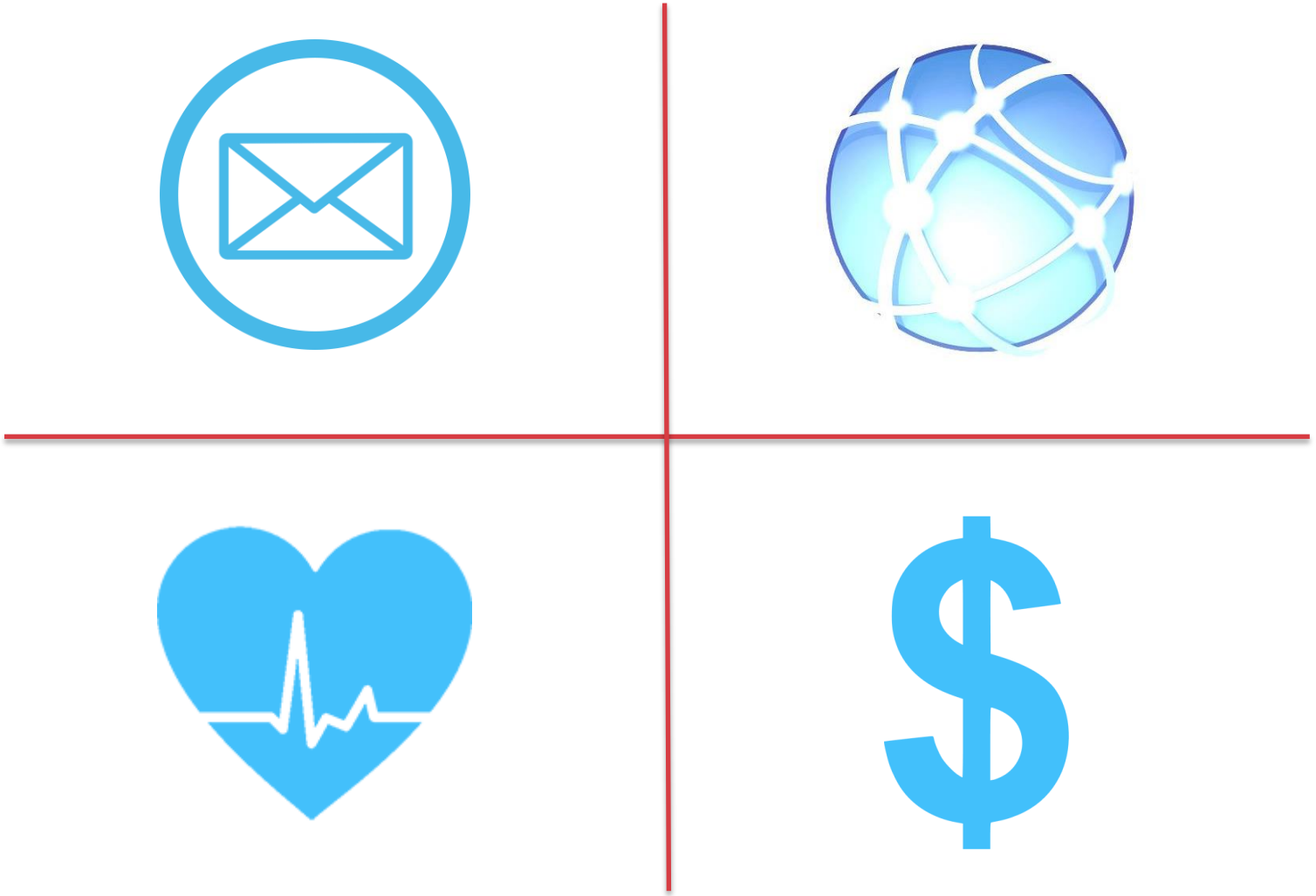
Kaosaktører

Kompetente, ressurssterke aktører

Samfunnsverdi

Nasjonal sikkerhet

TRENDER, METODER OG KONSEKVENSER

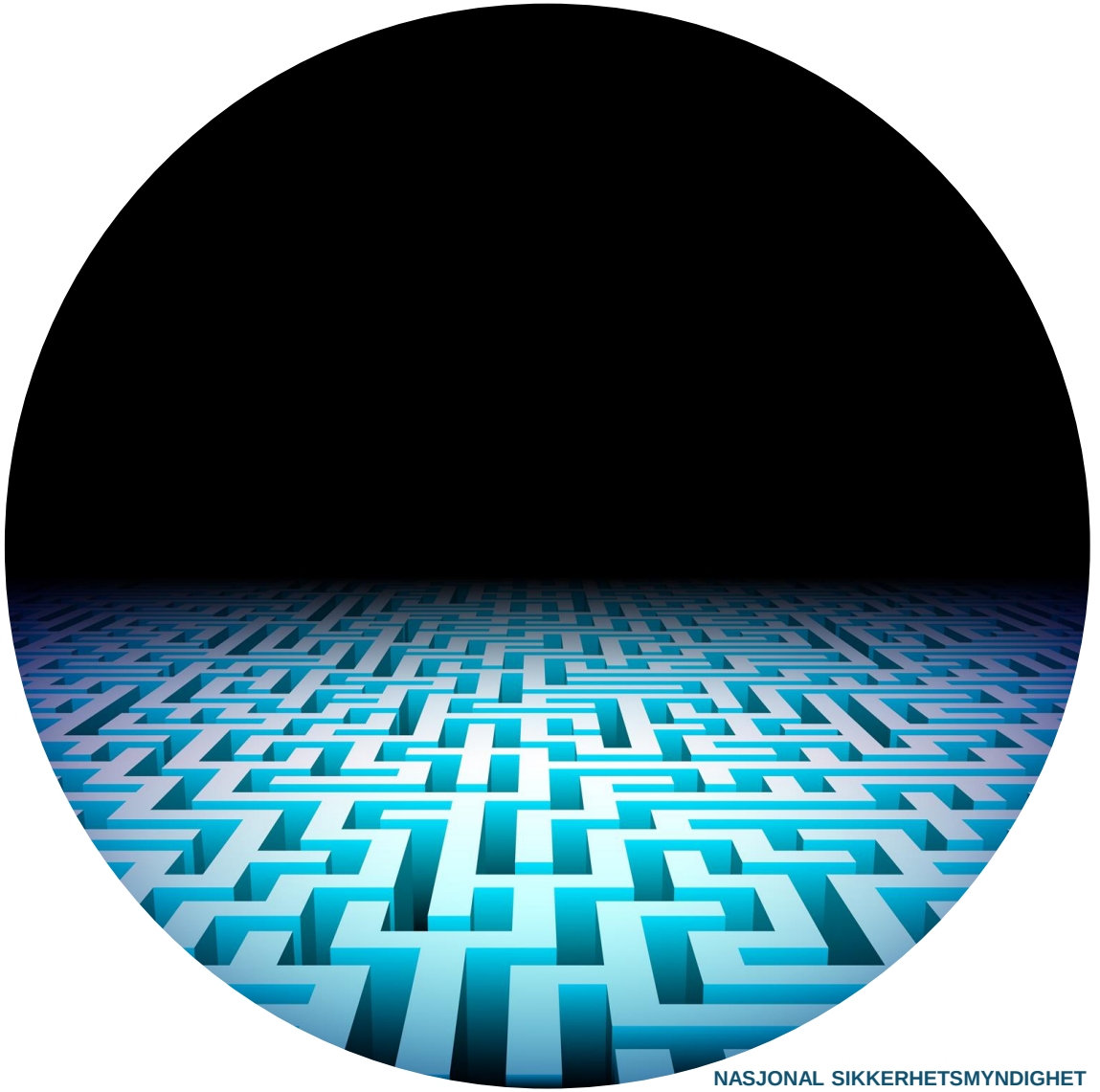


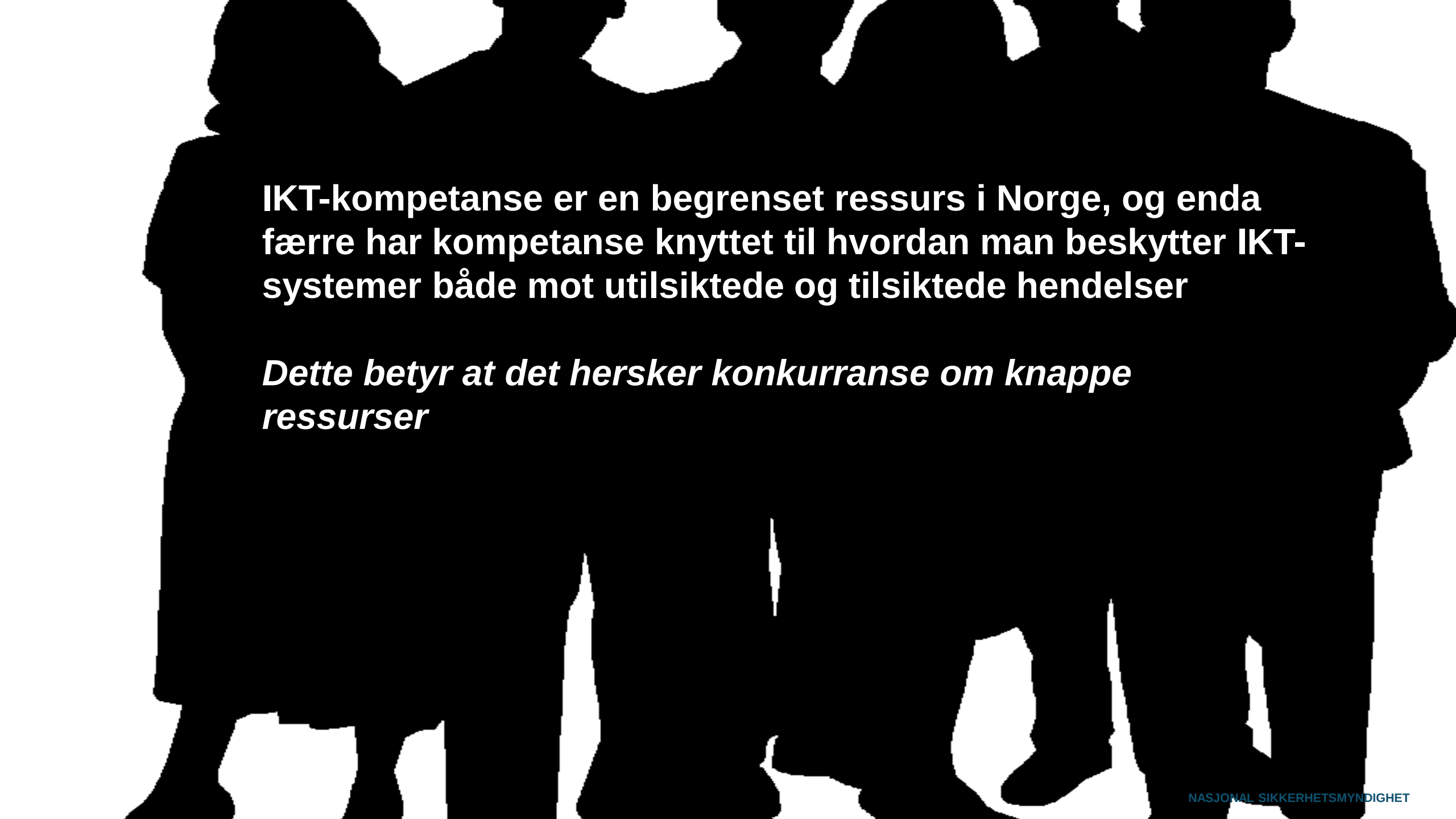
ANGRIPERE UTNYTTER I STØRRE GRAD LEVERANDØRER UTEN TILSTREKKELIG SIKKERHET

GOD SIKKERHET KREVER KOMPETANSE OG KAPASITET

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester

Virksomheten må sørge for at sikkerhetsnivået opprettholdes eller forbedres i forbindelse med tjenesteutsetting





IKT-kompetanse er en begrenset ressurs i Norge, og enda færre har kompetanse knyttet til hvordan man beskytter IKT-systemer både mot utilsiktede og tilsiktede hendelser

Dette betyr at det hersker konkurranse om knappe ressurser

STØRRE, MER KOMPETENTE MILJØER REDUSERER SÅRBARHETENE

Det er for mange små IT-avdelinger

Særlig i offentlig sektor

TJENESTEUTSETTING MEDFØRER ØKT SIKKERHETSRISIKO

Tjenesteutsetting medfører økt sikkerhetsrisiko på grunn av **redusert kontroll på stadig mer komplekse verdikjeder**

Virksomheter må aktivt etablere organisatoriske, prosessuelle, tekniske og juridiske sikringstiltak

TJENESTEUTSETTING KREVER SIKKERHETSKOMPETANSE

Ansvaret kan aldri settes bort

Tjenesteutsetting krever gode risikovurderinger og høy bestillerkompetanse

RISIKO MÅ VURDERES FØR INFORMASJON SETTES UT

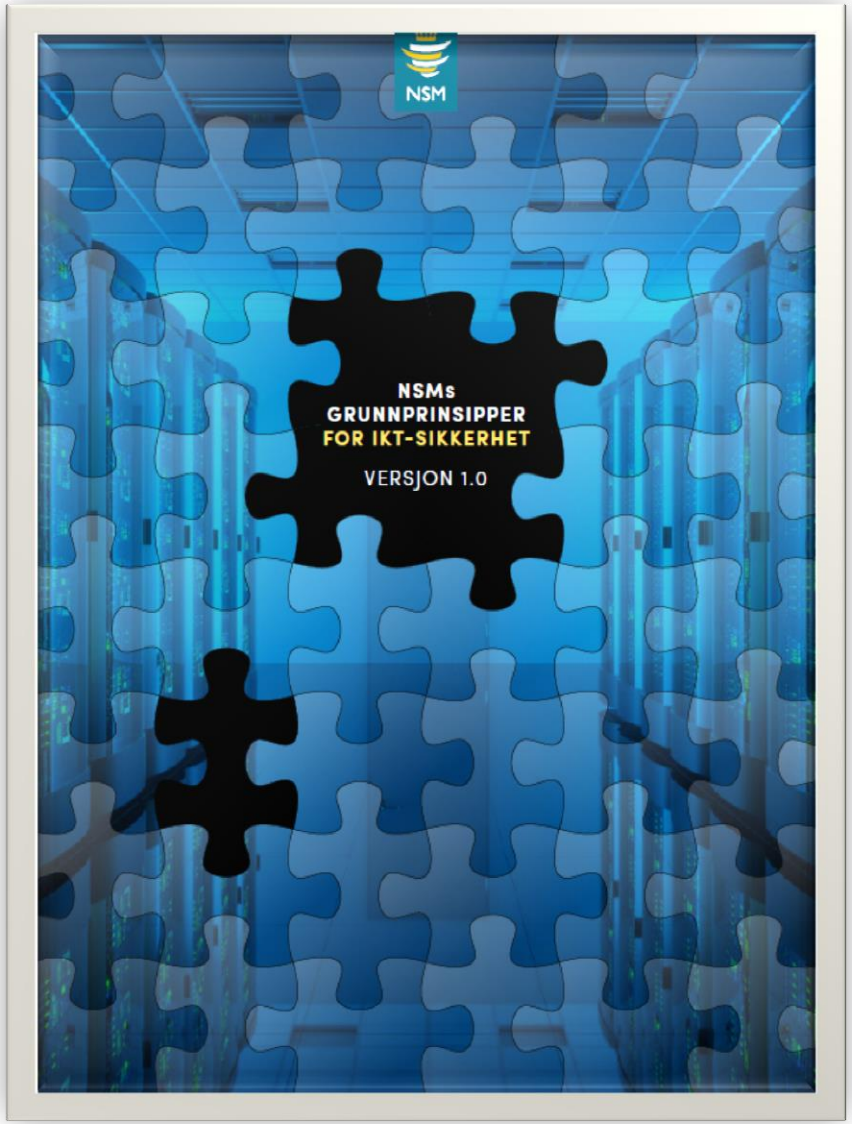
Virksomheten bør kartlegge hvilke verdier som eksponeres ved tjenesteutsetting, og vurdere dette opp mot behovet for **konfidensialitet, integritet og tilgjengelighet**

Risikoprofil, geografisk plassering og nasjonal tilhørighet til tjenesteleverandør er en del av det totale risikobildet som må vurderes.

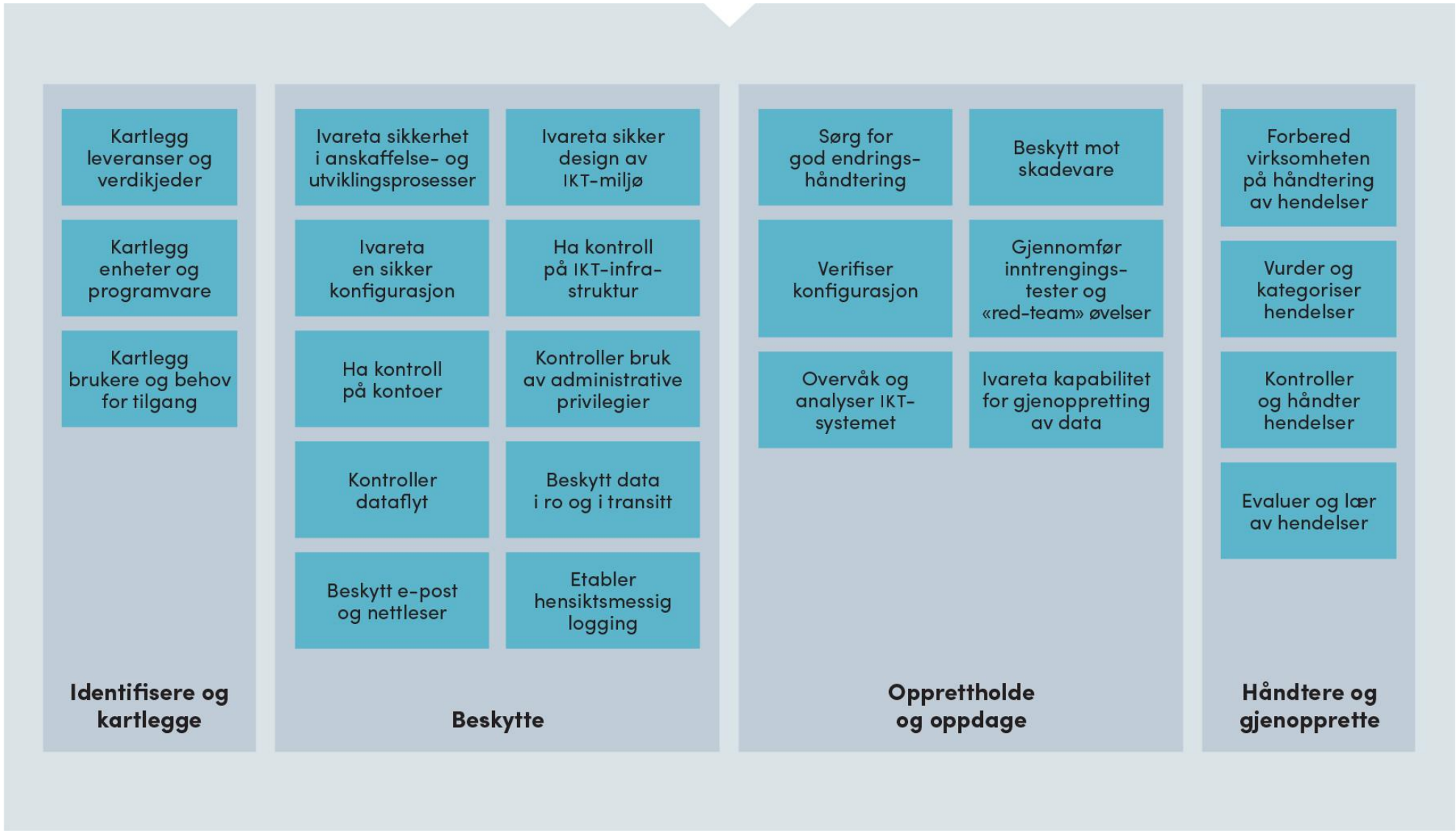
NSMS GRUNNPRINSIPPER FOR IKT-SIKKERHET BESKRIVER EN MINIMUMSBASELINE SOM BØR IVARETAS FOR ALLE IKT-SYSTEMER

https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

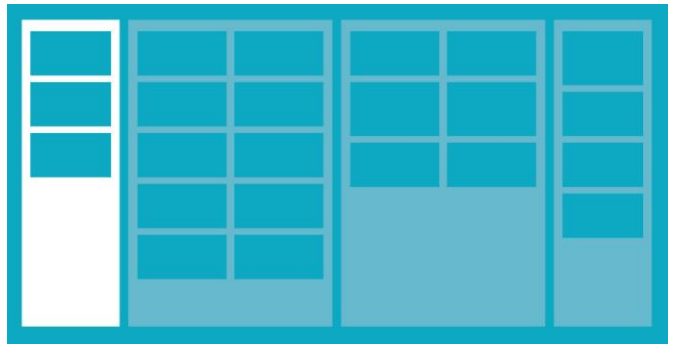
I tillegg gjelder sikringskrav beskrevet i relevante lovverk og sektorvise regelverk



NSMs GRUNNPRINSIPPER FOR IKT-SIKKERHET



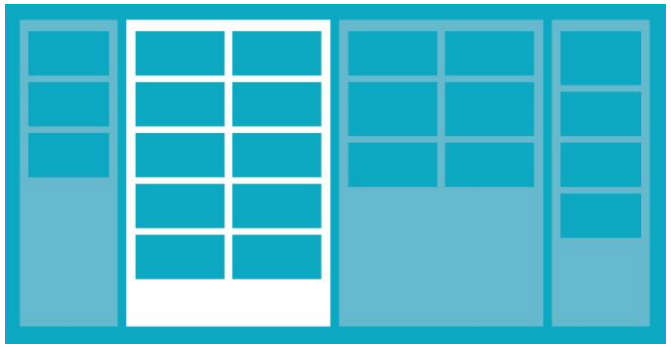
1. IDENTIFISERE OG KARTLEGGE



- opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere.

«Å, lå de dataene der!»

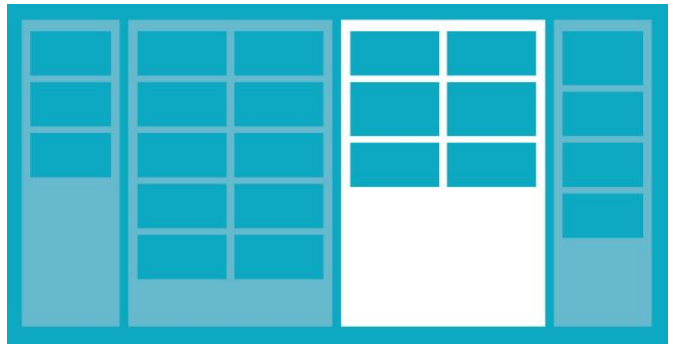
2. BESKYTTE



- ivareta en forsvarlig sikring av IKT-miljøet.

«Forrige torsdag fikk jeg informasjon om at 16 bulgarere hadde tilgang til sensitiv informasjon»

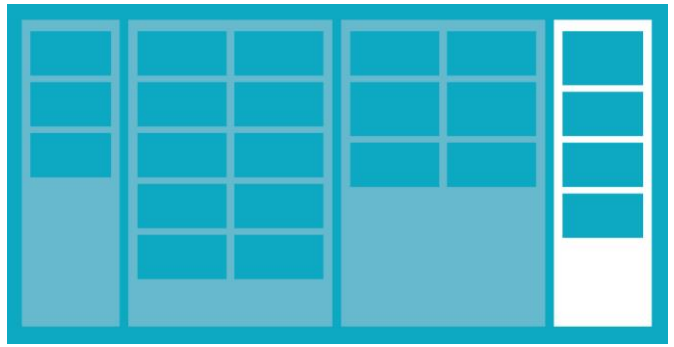
3. OPPRETTHOLDE OG OPPDAGE



- opprettholde den sikre tilstanden over tid og ved endringer, og oppdage sikkerhetstruende hendelser.

Ofte er det bare timer fra en sikkerhetsoppdatering slippes fra en leverandør, til det første angrepet oppdages hos NSM NorCERT

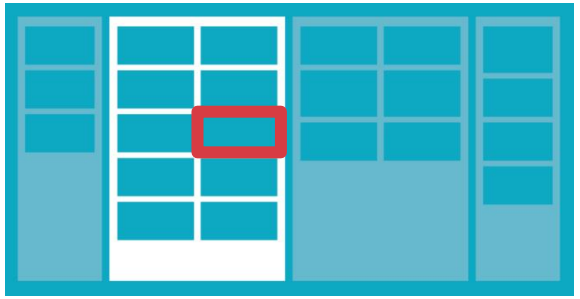
4. HÅNDTERE OG GJENOPPRETTE



- håndtere sikkerhetstruende hendelser effektivt.

Hva gjør man hvis et dataangrep blir oppdaget klokka 18 på en fredag? Har man betalt for at underleverandører og støttepersonell kan trå til på kort varsel?

OPPBYGNING AV HVERT GRUNNPRINSIPP



2.6 KONTROLLER BRUK AV ADMINISTRATIVE PRIVILEGIER

- **Mål:** Kontrollere, korrigere, og spore tildeling, bruk og konfigurering av administrative rettigheter for å hindre misbruk av datamaskiner, nettverk og applikasjoner.

- **Begrunnelse(Hvorfor?)**
  - Misbruk av administrative privilegier
    - Blant de vanligste metodene
    - Eks 1: Infisert epostvedlegg, nedlastbar fil med skadevare fra ondsinnet nettside, nettside med skadevare
    - Eks 2: Eskalering av privilegier (gjette eller knekke passord)

Anbefalte tiltak:

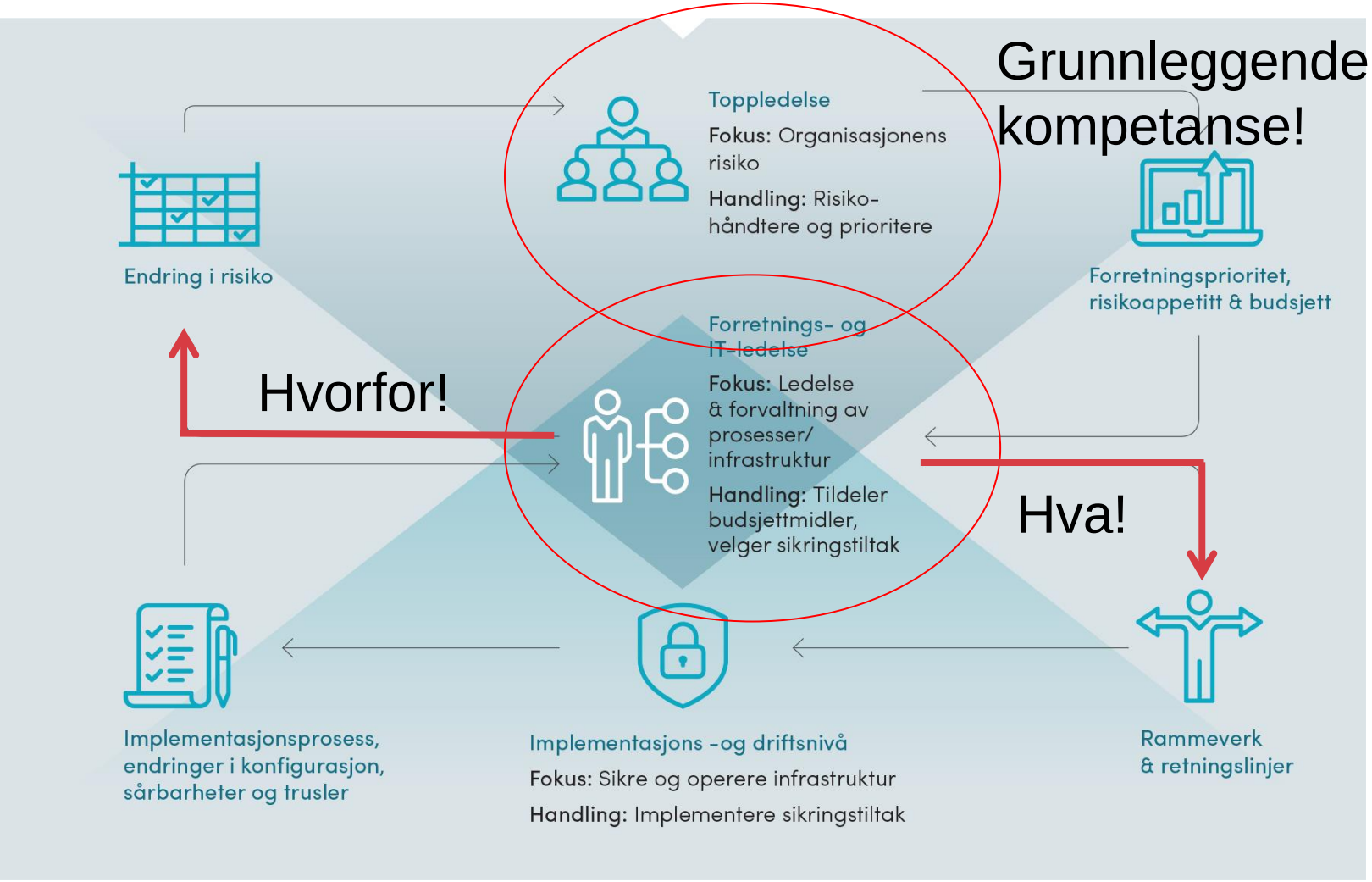
ID	BESKRIVELSE
2.6.1	Personer med administrative privilegier (operatører) bør bruke separate
2.6.2	Minimer bruken av administrative rettigheter og bruk administrative kont bruk av administrative privilegerte funksjoner og monitorer systemene fo I de tilfeller sluttbruker har behov for administrative privilegier, bør dette vurderes.
2.6.3	Administratorer bør påkreves å logge på systemer med en personlig, ikke administrative privilegier utføres.
2.6.4	Etabler ulike administratorkontoer til de ulike delene av IKT-infrastruktur administratorkonto ikke gir fulle rettigheter til å endre hele infrastruktur
2.6.5	Administratorer bør benytte dedikerte maskiner for alle administrative op tilganger. Maskinen bør isoleres fra virksomhetens primære nettverk. Ma utarbeide dokumenter eller ha mulighet til å surfe på internett.
2.6.6	Bruk multi-faktor autentisering for å autentisere administrative brukere.

MINIMUMSKRAV TIL LEVERANDØREN

- Et etablert **styringssystem** for informasjonssikkerhet og sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001:2017
- Innsyn i **sikkerhetsarkitekturen** som benyttes for å levere tjenesten
- **Utvikling av sikkerheten** i tråd med utvikling i teknologi og trusselbildet over tid
- En **oversikt over hvem som skal ha innsyn i virksomhetens informasjon**, hvor og hvordan denne skal behandles og lagres samt grad av mekanismer for segregering fra andre kunder
- **Tilgangsstyring** som inkluderer **kryptering**, aktivitetslogging, fysisk og logisk sikkerhet
- **Sikkerhetsovervåkning** egnet til å avdekke hendelser og handlinger i tråd med virksomhetens trusselbilde og relevante trusselaktører
- Rutiner for **hendelseshåndtering**, avviks- og sikkerhetsrapportering
- **Krise- og beredskapsplaner** som skal harmonisere med virksomhetens egne planer
- At bruk av underleverandører og deres bruk av **underleverandører** skal godkjennes før iverksetting
- Hvilke aktiviteter som skal utføres ved **terminering** av kontrakten, blant annet tilbakeføring/flytting/sletting av virksomhetens informasjon

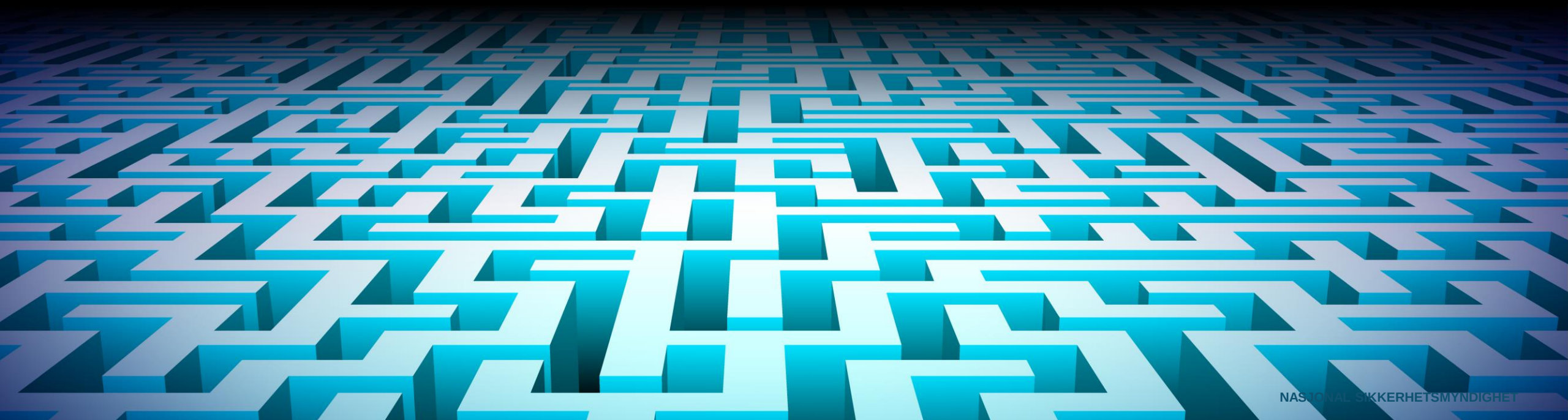
«Sikkerhet er for viktig til å overlates til sikkerhetsekspertene»

RIKTIGE BESLUTNINGER KREVER SIKKERHETSKOMPETANSE - I ALLE LEDD



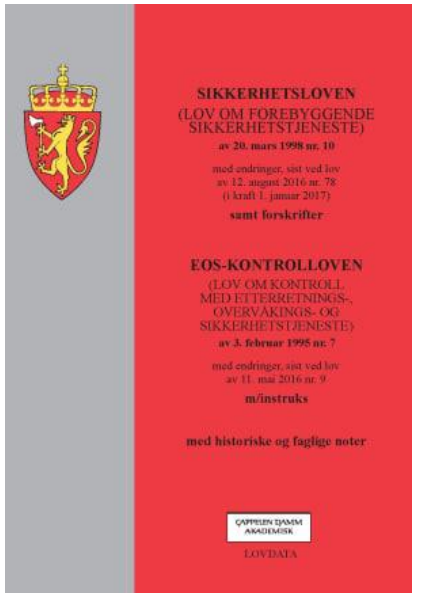
I realiteten vil virksomheter møte kommersielt attraktive og til dels sterke dominerende tjenesteleverandører som i liten grad er villige til å gi tilstrekkelig transparens til å verifisere samsvar med regelverk og anbefalinger

Der kravene ikke oppnås vil virksomheten ha en risiko og virksomheten må vurdere eventuelle kompenserende tiltak og hvorvidt tjenesten faktisk skal settes ut



LOVVERKET

Når en virksomhet velger å sette ut leveranser er det viktig å kartlegge hvilke lover, krav og regler som gjelder for egen virksomhet både nasjonalt og internasjonalt



NÅR DIGITALE SÅRBARHETER ER NASJONALE SÅRBARHETER

MODERNISERING MEDFØRER OFTE AT IKT-LØSNINGER FÅR ØKT NASJONAL BETYDNING OG ØKT BESKYTTELSESBEHOV

NSM er bekymret for….

… datasikkerheten når virksomheter setter ut tjenestene

… at økt kritikalitet ikke blir risikovurdert og identifisert

… sikkerhetsvurderingene ved konsolidering av data

… manglende nasjonal kontroll på kritisk infrastruktur

… at kritisk infrastruktur tjenesteutsettes til risikoland

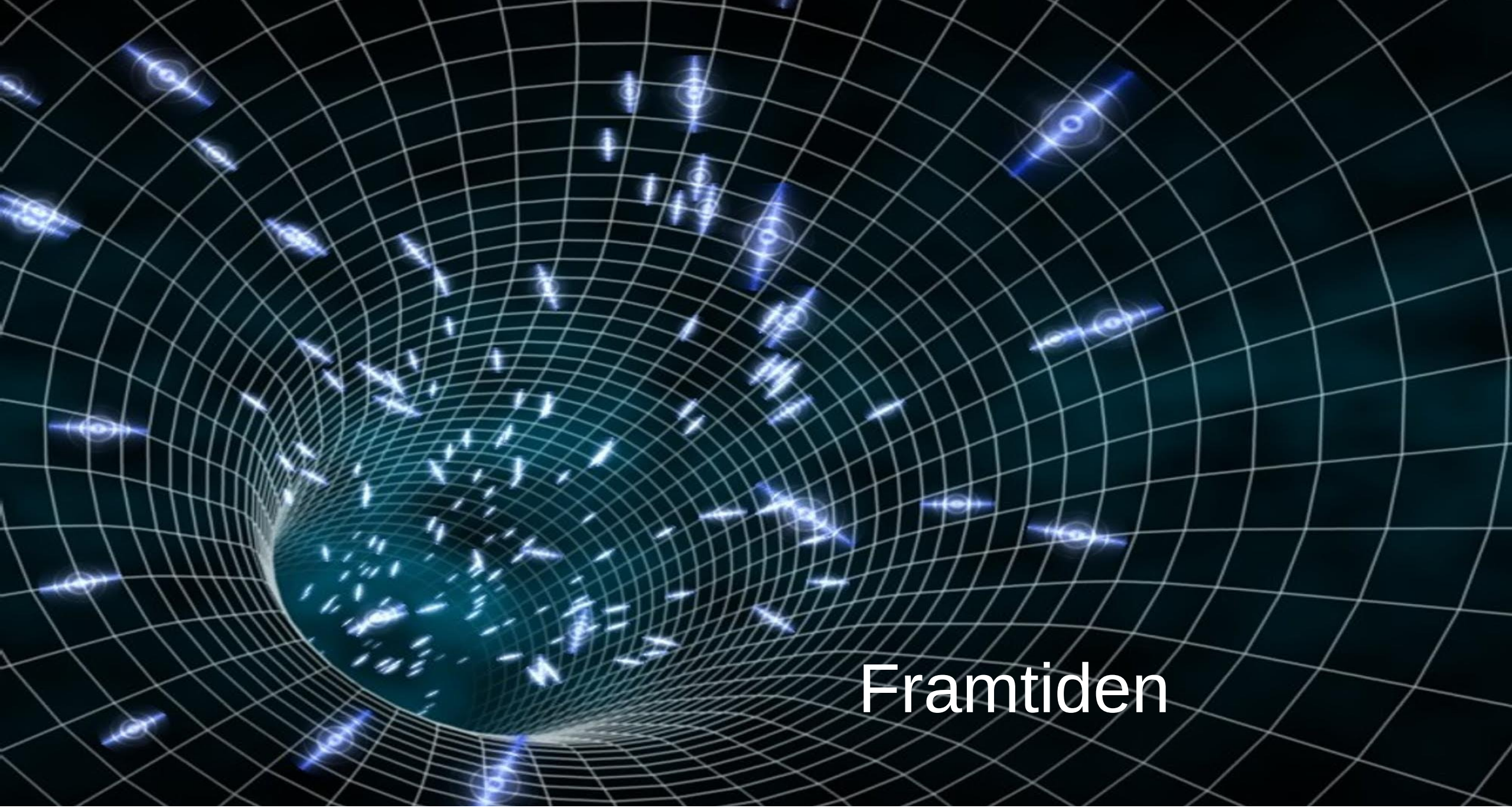
Nasjonal sikkerhetsmyndighet (NSM) er bekymret for at tjenesteutsetting gjøres uten at virksomheter vurderer sikkerhetsaspektet godt nok Foto: Istockphoto/Getty Images

Meninger Innlegg

Bekymret over at tjenester settes ut

Vi er bekymret for datasikkerheten når virksomheter setter ut tjenestene. Datalagring og -prosessering utenfor landets grenser krever særlig aktsomhet.

Kjetil Nilsen, direktør, Nasjonal sikkerhetsmyndighet



Framtiden


Spørsmål?
NSM sikrer samfunnsverdier
NSM