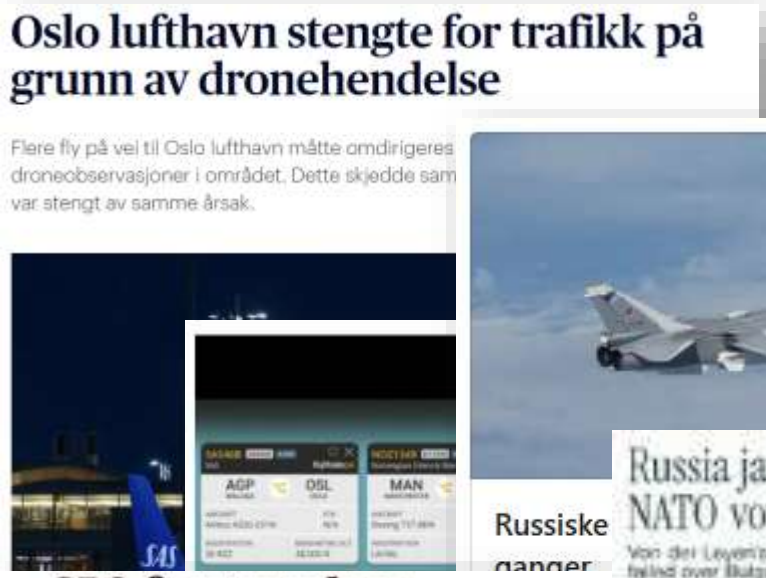
Cyberslagmark 2026
- med kommunen som frontlinje

Eirik Gulbrandsen | Spesialrådgiver seksjon Teknologi, Sikkerhet og Tilsyn

Datatilsynet

Kilde til SVT: Dronene over Kastrup skal ha vært flylignende droner med lang rekkevidde

Russerne anklages for å stå bak mistenkelig droneflyvning i Danmark. Dronene skal ha hatt vinger.



Flere titalls sabotasjeaksjoner mot fiber og mobilmaster i Sverige siden påske

Global Connect-direktør tror vi har grunn til å være bekymret også i Norge. – Hvorfor dette bare skjer i Sverige, er det ingen som vet, sier han.

– Dette er
Torvildse
skjøtebok
er blitt tru
over på b
fjernet. Fo

Flere kabelbrudd i Østersjøen

- Som nåla i høystakken

Kabelbruddene i Østersjøen kan være ledd i den russiske hybride krigføringen, mener ekspert. Han ber Norge være forberedt.

Den mest omtalte hendelsen er ødeleggelser av **et 30-talls mobilmaster** langs E22 ved påsketider. SVT skriver at politiet etterforsker dette som mulig sabotasje.

Omtrent samtidig ble **fiberkabler og fiberskap ødelagt i Julita** i Södermanland.

I september ble **flere skap med fiberkabler ødelagt i Eskilstuna**, og en representant for fibereieren sier til SVT at det har skjedd flere ganger tidligere i år at utstyret deres har blitt ødelagt.

Dagen før skjedde en lignende hendelse **mot fiberkabler i Kvicksund** i Västmanaland.

Ifølge Sveriges Radio har det statseide selskapet Teracom, som leverer infrastruktur for TV- radio- og annen kommunikasjon i løpet av de fire første månedene av 2025 **anmeldt rundt 50 hendelser** mot deres utstyr, inkludert sabotasje og forsøk på uautorisert tilgang.

10-15 personer skal ha blitt pågrepet ved i forbindelse med slike hendelser, og Teracoms sikkerhetssjef Stefan Steijnick utelukker ikke at det i noen tilfeller kan dreie seg om en fremmed stat som foretar en kartlegging.

PST-sjefen: Mener russere sto bak norsk dam-sabotasje

Kortversjonen

- I april tok hackere over styringssystemet til en dam i Bremanger.
- PST peker på pro-russiske hackere som de ansvarlige.
- PST-sjefen advarer mot økende cyberoperasjoner fra Russland, som tar sikte på å skape frykt og ustabilitet i Vesten.
- Flere slike aksjoner siste tiden.

«Passord123» -angrepet...

– Dette er virkemidler og metoder som Russland benytter for å påvirke sikkerhetssituasjonen i andre land. Målet er å påvirke det norske samfunnet, spre uro og ustabilitet, samt kartlegge våre styrker og svakheter, sier PST-sjefen.

Hva har dette med personvern å gjøre?

Konvergens

IT og OT benytter i økende grad samme infrastruktur

- Samme kabler og nettverk
- Samme servere og operativsystemer
- Samme brukere og påloggінger

Dårlig OT-sikkerhet = dårlig IT-sikkerhet = dårlig personopplysningssikkerhet ❓

God personopplysningssikkerhet avhenger av god informasjonssikkerhet

Fra fysiske til digitale demninger…

Bekreftar at personsensitiv data er lekka etter dataangrep i Østre Toten

Etterforskinga dei siste dagane har vist at data ligg ute på det mørke nettet. Kommunen seier persondata har hamna på «det mørke nettet».

GJENOPPRETTING: Alle desse datamaskinene måtte gjenopprettast etter angrepet. Kommunen var framleis utan alle system på plass ein månad etterpå.
FOTO: ANDERS BAKKERUD LARSEN / NRK

Marte Iren Noreng Trøen
Journalist

Line Fosser Vogt
Journalist

Dag Kessel
Journalist

Publisert 30. mars 2021 kl. 14:33
Oppdatert 31. mars 2021 kl. 22:07

Artikkelen er flere år gammel.

Oppdatert 31/3 kl. 22.00:

Kommunedirektøren i Østre Toten kommune seier ein stikkprøve som er gjort bekreftar at kriminelle har lagt ut personopplysningar på nett.

Østre Toten: Prislapp på over 32 millioner for å rette opp hacker-skadene

I januar ble Østre Toten kommune utsatt for et dataangrep fra en internasjonal hackergruppe. Skadene har hittil kostet over 32 millioner kroner å reparere – og likevel er ikke alt i orden ennå. Nå håper kommunen at deres åpenhjertighet kan være forebyggende for andre.

En ny virkelighet

...hevder åtti hackergrupper konstant angriper Ukraina.

– Hver dag opplever vi forskjellige former for cyberangrep. Vi ser direkte angrep mot vår finanssektor, energisektor, telekommunikasjon og logistikk, og selvfølgelig i den offentlige sektor.

Swedish cyberattack exposes 1.5 million citizens' data

Supply Chain Attacks

Leverandørkjedeangrep

the personal data of an es

Ransomware crooks knock Swedish municipalities offline for measly sum of $168K

: Miljödata meltdown leaves 200 local authorities scrambling over

Hackers dump 1M+ Swedes' data on darknet after ransom fails

Personal data of over one million Swedes has been published on the darknet following a major ...

Flere kommuner rammet av dataangrep

Flere norske kommuner er rammet av datainnbrudd. Tyver skal blant annet ha stjålet personopplysninger.

Malin Therese Strand
Journalist

Dag Kessel
Journalist

Publisert 7. juli kl. 20:40
Oppdatert 9. juli kl. 18:06

RAMMET: Ringsaker kommune er en av kommunene som har blitt rammet av dataangrepet.
FOTO: KNUT RØSRUD / NRK

Fredag ble det klart at Extend AS hadde vært utsatt for et dataangrep med løsepengevirus.

Extend leverer datatjenester til flere kommuner.

Daglig leder i Extend AS, Christine Våpenstad Holm, opplyser at fire kommuner er berørt av dataangrepet.

Oppdatering om dataangrep mot Extend AS

Fredag 4.juli ble det klart at Extend AS var utsatt for et dataangrep med løsepengevirus. Det har ført til at kriminelle har stjålet kundedata fra noen av våre kunder og det har vært driftsforstyrrelser i tjenesten. Siden angrepet ble oppdaget har vi jobbet med å gjenopprette systemene på en trygg måte, øke sikkerheten ytterligere og kommunisere direkte med berørte kunder. De fleste systemene er nå tilbake i normal drift, og vi vil bruke tiden fremover på å sikre dem ytterligere med hjelp fra eksperter. Angrepet er meldt til datatilsynet og politiet.

Databehandler vs behandlingsansvarlig

Databehandlere har et selvstendig ansvar, men også behandlingsansvarlige har et ansvar for å stille krav til leverandører.

Krav til leverandør
(forutsetter)
bestillerkompetanse

Artikkel 28. Databehandler

1. Dersom en behandling skal utføres på vegne av en behandlingsansvarlig, skal den behandlingsansvarlige bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter

Krav til leverandør: Kryptering

Artikkel 32.Sikkerhet ved behandlingen

1. a. pseudonymisering og kryptering av personopplysninger

- Lover, forskrifter og rammeverk setter krav til Å kryptere, men spesifiserer i liten grad hvordan den bør implementeres

- Riktignok sier ISO 27002 / 8.24 Use of cryptography:

8.24 Use of cryptography

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control

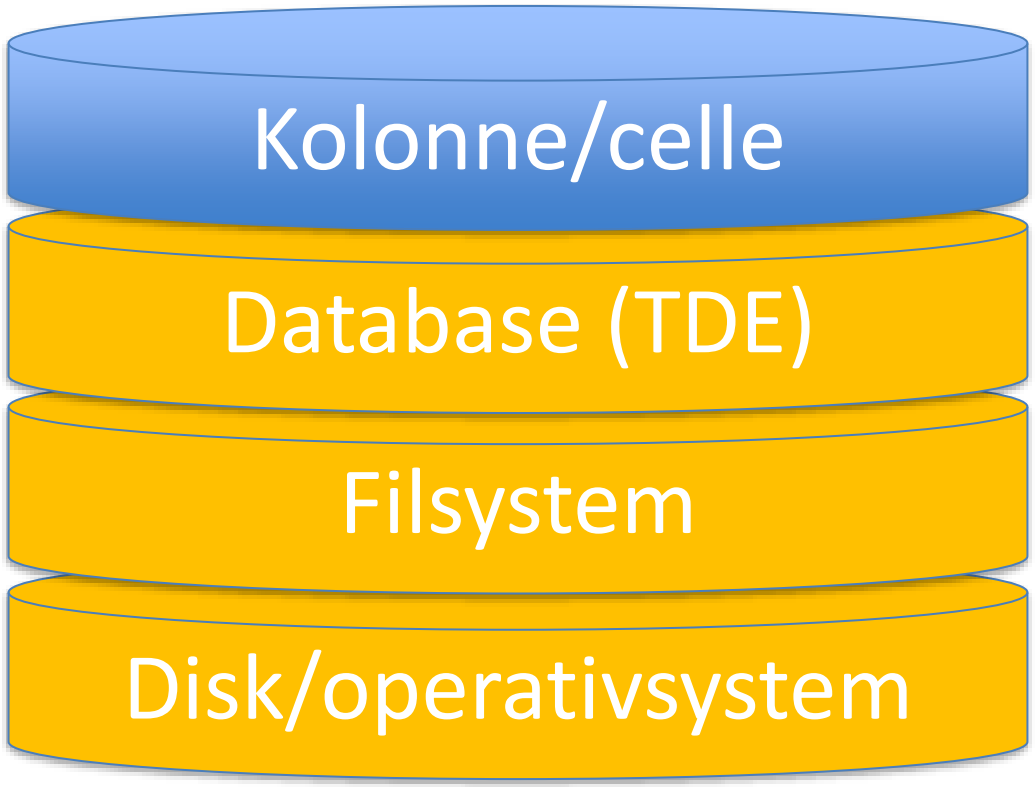
Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.

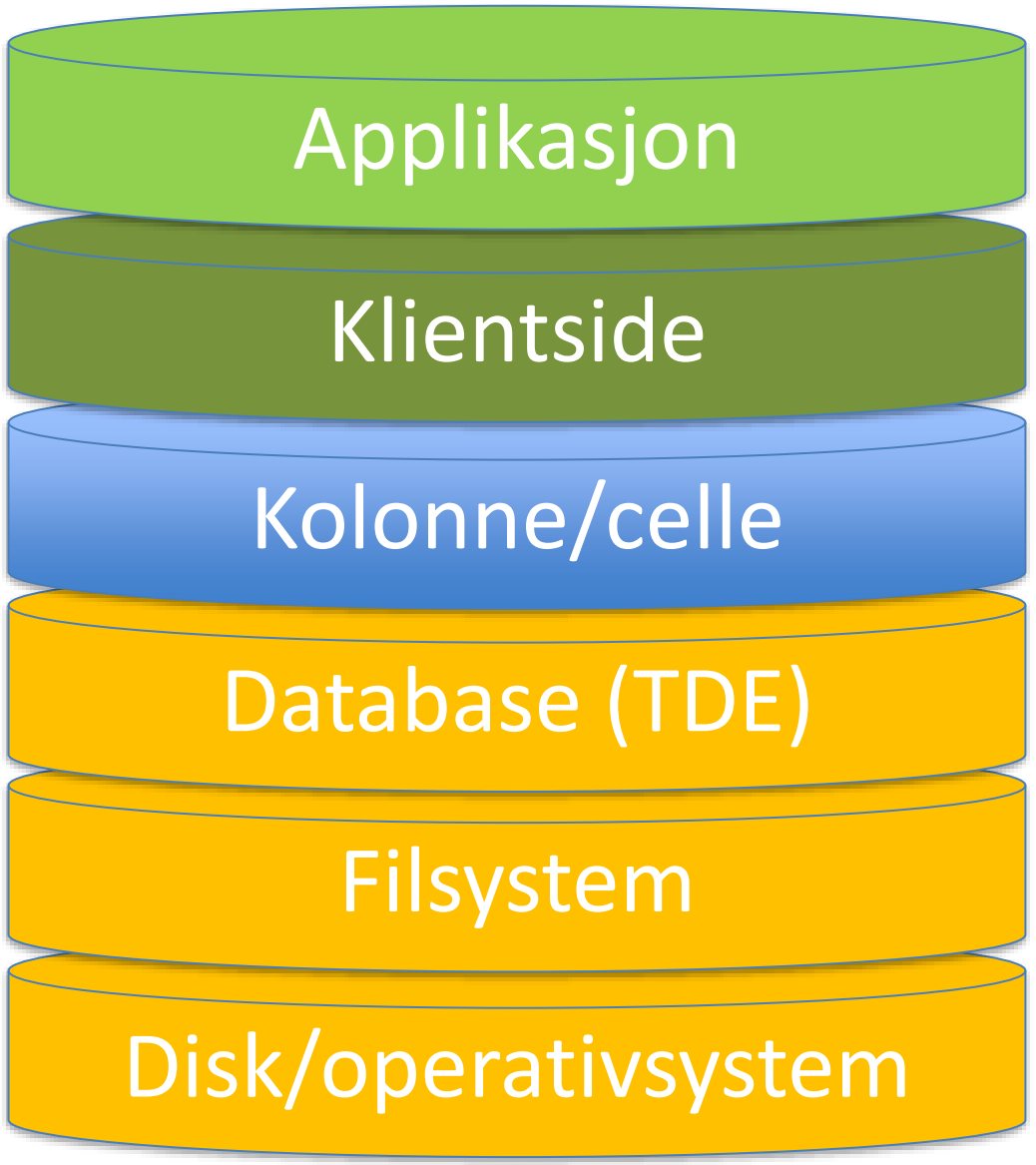
Krav til leverandør: Kryptering

- Kryptering: Ofte «ja» / «nei»
- Betyr som regel disk/OS, fil eller i beste fall databasekryptering
  - Beskytter mot…?
    - At noen fysisk stikker av med eller kopierer disker/filer/database
  - Beskytter ikke mot
    - Priviligerte brukere/admin med stjålne rettigheter, utro tjener, SQL-injeksjon, malware, uønskede søk
    - Tap av sikkerhetskopi?
- Kolonne/celle
  - Beskytter mot brukerangrep, men ikke adminangrep (aktør med admin-rettigheter), privilegert utro tjener



Krav til leverandør: Kryptering

- Klientside/applikasjon
  - Nøkkeladmin/kryptering er administrert/utført av klient
  - Beskytter mot…?
    - Alt de andre nivå gjør (og kan kombineres)
    - Angrep mot kjørende database
    - Priviligerte brukere/admin med stjålne rettigheter
    - Utro tjenere
    - Tap av sikkerhetskopi?
  - Beskytter ikke mot kompromitterte enkeltklienter, men kan beskytte alle andre klienter på samme database



Krav til leverandør: Kryptering

- Kryptering er ikke ja / nei
- Kryptering skal ikke være en «papirtiger»
- Kryptering skal være en faktisk effektiv beskyttelse mot faktiske trusler
- Forskjellige krypterings-tiltak er relevant for forskjellige beskyttelses-behov og konsekvens-scenarier

Artikkel 32. Sikkerhet ved behandlingen

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen

Informasjonssikkerhet og personvern: Fire elementer

Datatilsynet mottar 3000+ avviksmeldinger i året. For de som har en viss alvorlighetsgrad er det spesielt fire elementer som går igjen:

1) Hvis man hadde hatt effektiv, sterk autentisering, ville ofte konsekvensene av hendelser vært nesten fraværende eller sterkt redusert. Dette fordi effektiv, sterk autentisering fjerner mye av byrden fra den enkelte bruker og er krevende å omgå og utnytte

Hva er «sterk autentisering»?

- *Passord og brukernavn kan ikke lenger regnes som «egnet tiltak» for å oppnå «vedvarende konfidensialitet» for nesten enhver behandling av personopplysninger (PvF artikkel 32.1.b).*
- Mange kjente og utbredte 2-faktor/multifaktorløsninger omgås rutinemessig, inkludert «legacy» Microsoft 365
- Man trenger i praksis «phishingresistent autentisering» ofte realisert gjennom passordløs pålogging og passnøkler (FIDO2/Webauthn) → M365
- Dette eller tilsvarende tiltak må implementeres for ALLE typer brukere, også administratorer og tjenestekonti (*Grunnprinsipper 2.6 - Ha kontroll på identiteter og tilganger*)

nsm.no/regelverk-og-hjelp/rapporter/flerfaktor autentisering

Enable passkeys (FIDO2) for your organization

05/21/2025

For enterprises that use passwords today, passkeys (FIDO2) provide a seamless way for workers to authenticate without entering a username or password. Passkeys (FIDO2) provide improved productivity for workers, and have better security.

This article lists requirements and steps to enable passkeys in your organization. After you complete these steps, users in your organization can then register and sign in to their Microsoft Entra account using a passkey stored on a FIDO2 security key or in Microsoft Authenticator.

For more information about enabling passkeys in Microsoft Authenticator, see How to enable passkeys in Microsoft Authenticator.

For more information about passkey authentication, see Support for FIDO2 authentication with Microsoft Entra ID.

> **Note**
>
> Microsoft Entra ID currently supports device-bound passkeys stored on FIDO2 security keys and in Microsoft Authenticator. Microsoft is committed to securing customers and users with passkeys. We're investing in both synced and device-bound passkeys for work accounts.

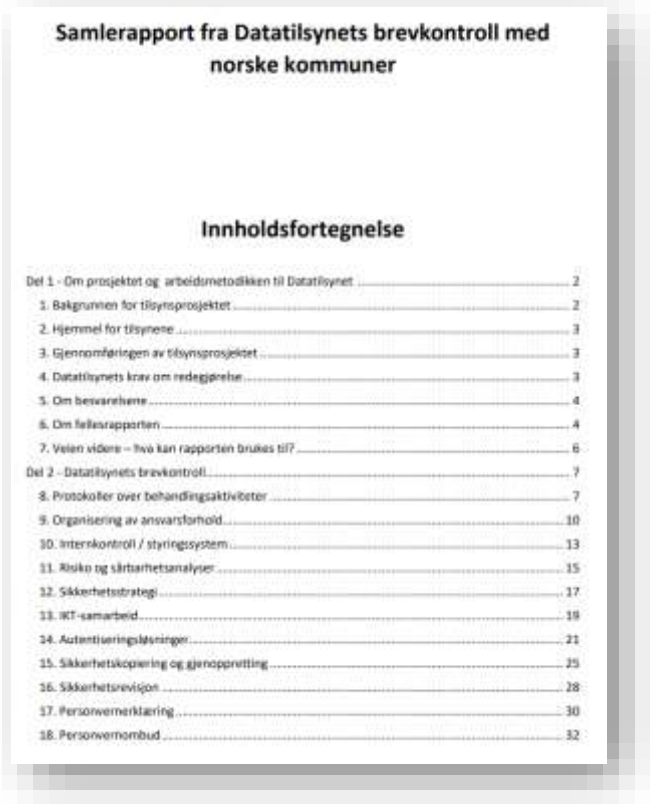
Informasjonssikkerhet og personvern: Fire elementer

Datatilsynet mottar 3000+ avviksmeldinger i året. For de som har en viss alvorlighetsgrad er det spesielt fire elementer som går igjen:

2) Hvis man hadde evne til effektivt å gjenopprette data og drift av løsninger (PvF artikkel 32.1.c), ville ofte konsekvensene av hendelser vært redusert (tid, penger, omdømme).

«Alle» tar sikkerhetskopier, men altfor mange har ikke (2023):

- Forretningsforankrede krav til funksjonell gjenopprettingstid i prioritert rekkefølge
- Godt dokumenterte prosedyrer for gjenopprettingsprosessen
  - Avhenger ofte av enkeltpersoner kompetanse og tilstedeværelse
- Har gjenopprettingsprosesser integrert i en overordnet beredskapsplan
- Øver og tester på prosesser og planer
  - Man tester kun at sikkerhetskopier teknisk kan leses


Samlerapport fra Datatilsynets brevkontroll med norske kommuner

Innholdsfortegnelse

www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/funn-fra-tilsyn-i-kommuner-og-fylkeskommuner/

Informasjonssikkerhet og personvern: Fire elementer

Datatilsynet mottar 3000+ avviksmeldinger i året. For de som har en viss alvorlighetsgrad er det spesielt fire elementer som går igjen:

3) Hvis man hadde evne til å analysere og dokumentere aktivitet inkludert datatrafikk (både mistenkelig og antatt vanlig trafikk), både inn og ut – gjennom brannmurlogger, systemlogger og applikasjonslogger, ville man i langt større grad raskt kunne fastslå om hendelser er alvorlige eller ikke.

I dag brukes ofte dager, uker og måneder på «famle i blinde» for å finne ut hva som skjedde og hvilke type data som kan være på avveie. Dette er dermed både tidkrevende, kostbasert og gir ofte uklare konklusjoner om mulige konsekvenser og manglende evne til å forebygge nye hendelser.

Dette reduserer også evne til å oppfylle kravet om raske og effektive tiltak for å håndtere konsekvenser for de registrerte, som f.eks. p beskytte mot identitetstyveri (72 timer).

PvF fortalepunkt 49.

Behandling av personopplysninger i det omfang som er strengt nødvendig og forholdsmessig for å sikre nett- og informasjonssikkerheten … utgjør en berettiget interesse for den berørte behandlingsansvarlige (PvF artikkel 6.1.f).

Informasjonssikkerhet og personvern: Fire elementer

Datatilsynet mottar 3000+ avviksmeldinger i året. For de som har en viss alvorlighetsgrad er det spesielt fire elementer som går igjen:

4) Hvis man hadde «en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er» vil man kunne tilpasse tiltakene til endrede rammevilkår og eventuelle endringer i trusselbilde.

PvF artikkel 32.1.d

F.eks.:

- Er kryptering fremdeles effektiv for formålet og truslene?
- Er gjenoppretting- og beredskapsplaner effektive?
- Kan vi effektivt analysere og dokumentere hendelser?
- …er gjennomførte ROS-vurderinger og DPIA og deres tiltak fremdeles relevante?

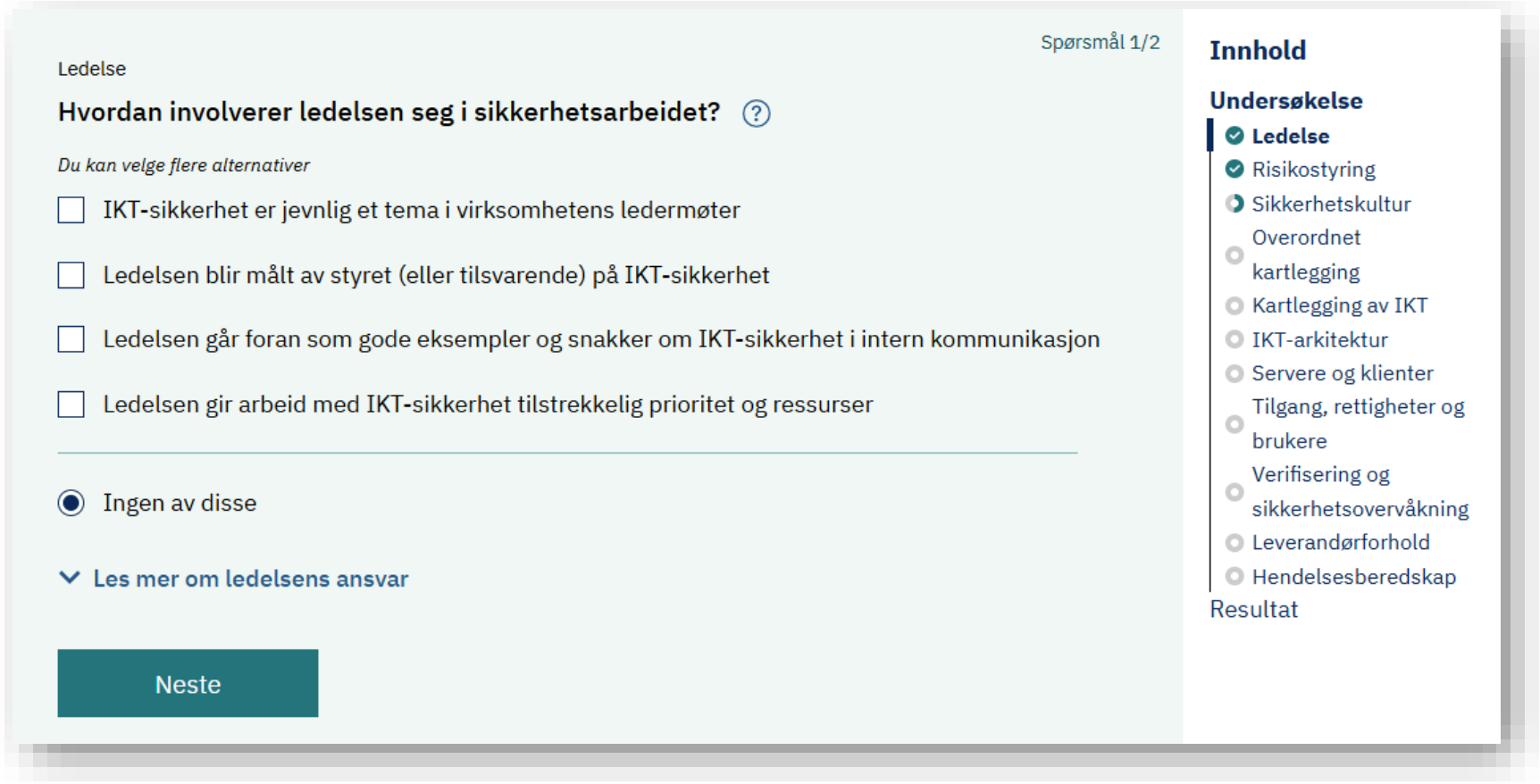
Hvordan bli mer motstandsdyktig

Vi må være bedre forberedt på at Norge kan rammes av mer alvorlige sikkerhetstruende hendelser enn vi har erfart så langt. Offentlige myndigheter, frivilligheten, næringsliv og andre virksomheter **må kartlegge egne verdier, kjenne egne sårbarheter og utvikle planer for bedre å motstå alvorlige hendelser.** Det er særlig viktig å raskt kunne gjenopprette drift.

Økt systematikk i arbeidet med sikkerhet Kommunal, frivillig og privat sektor har en viktig rolle i arbeidet med norsk sikkerhet.

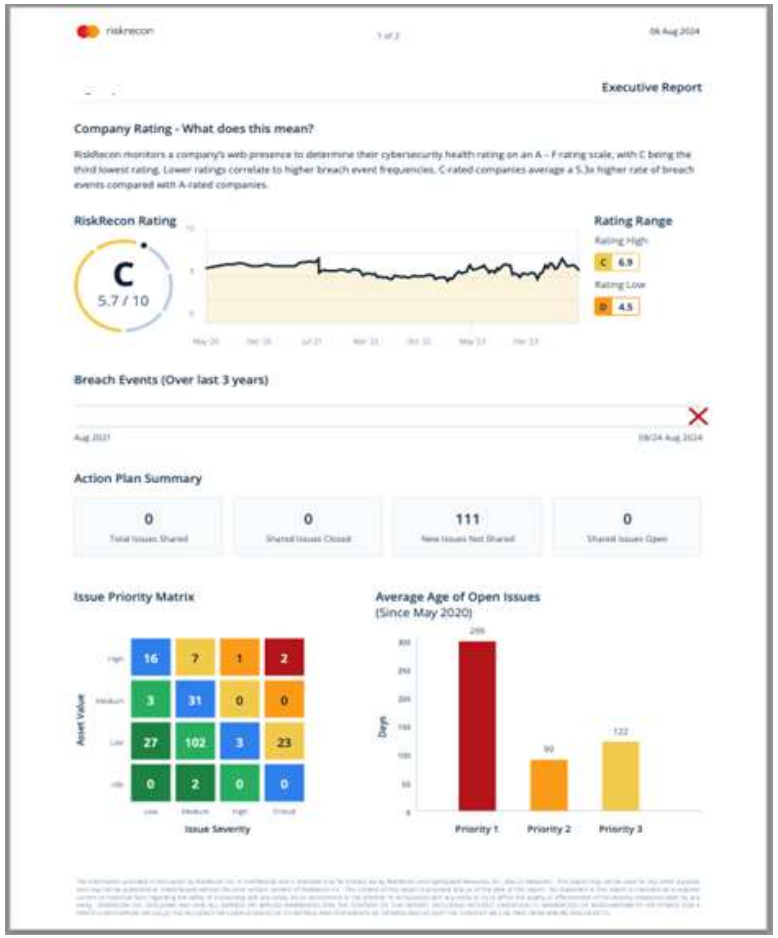
Verktøy og hjelpemidler

- Ikke bare «bedre» og mer tilgjengelige, men også i økende grad samordnet
- cybersjekk.no:



Verktøy og hjelpemidler

- Ikke bare «bedre» og mer tilgjengelige, men også i økende grad samordnet
- cybersjekk.no (NSM)
- Cyber Risk Score (DFØ):



Hva gjør Cyber Risk Score for virksomhetene?

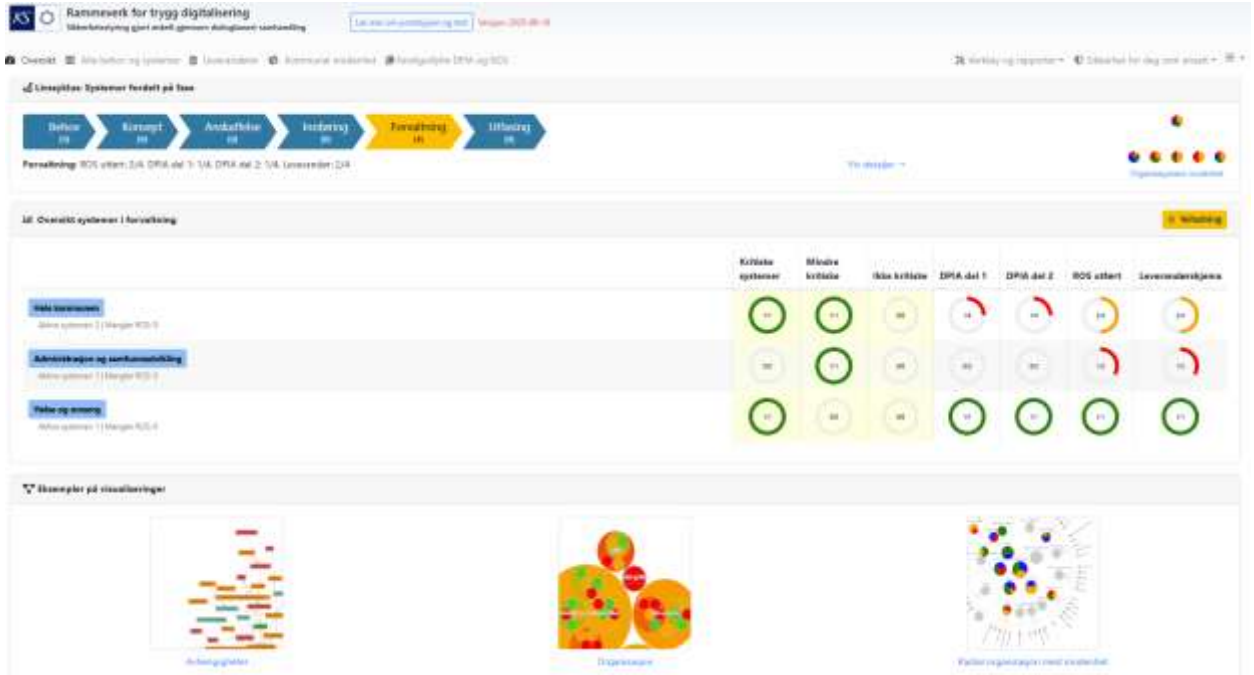
Voldsom interesse for nytt skyprogram: – Kjipt å være flagget rødt når naboen er grønn, mener IT-sjef

Markedsplassen for skytjenester (MPS) er er i gang med å sjekke interessen for en ny skytjeneste som kartlegger cyberriskofaktorer i offentlig og statlig sektor. Styreleder i offentlig sikkerhetsforening mener programmet er et «must».

- Kartlegger virksomhetens systemer, risiko og sårbarhet på Internett
- Beregner en risikoscore som kan følges opp over tid og sammenlignes med andre
- Verktøy for oppfølging av identifiserte risiko og sårbarheter
- Funksjonalitet for dashboards, varsling og rapporter for virksomhetsledelse og operativt bruk hos IT og sikkerhet
- Oppfølging av leverandører og tredjeparter med tilsvarende funksjonalitet som virksomheten selv
- Merk at verktøyet krever en systematisk tilnærming, og det er bare et av flere verktøy i verktøykassa!

Verktøy og hjelpemidler

- Ikke bare «bedre» og mer tilgjengelige, men også i økende grad samordnet
- cybersjekk.no (NSM)
- Cyber Risk Score (DFØ)
- Rammeverk for Trygg Digitalisering (KS)



Verktøy og hjelpemidler

- Ikke bare «bedre» og mer tilgjengelige, men også i økende grad samordnet
- cybersjekk.no (NSM)
- Cyber Risk Score (DFØ)
- Felles Myndighetsportal
  - Samarbeid:
    - NSM
    - Digdir
    - Datatilsynet
    - Politiet

Hva er den viktigste forutsetningen for god sikkerhet?

Forståelse av digital risiko og konsekvenser
Tilstrekkelig prioritet og ressurser

Hva er den viktigste faktoren for dette?
De som har ansvaret for økonomien = ledelsen

Hva er verktøyet for å sikre at ledelsen jobber systematisk med sikkerhet?

Bøter og sanksjoner

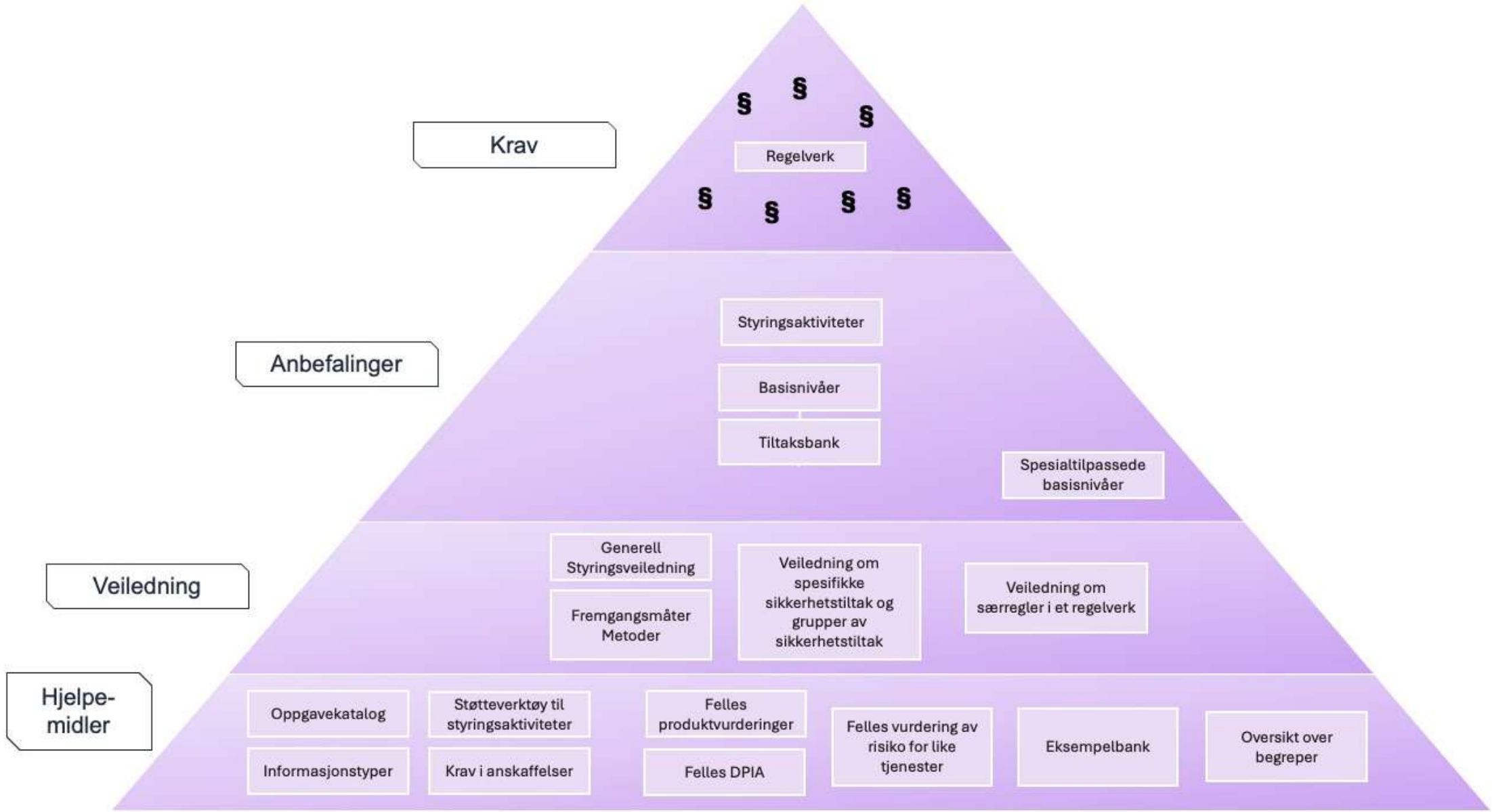
GLEM ~~lederforankring~~ – etabler lederansvar!

- velfungerende styringssystemer er en forutsetning
- etablere styringssystemer med indikatorer som betyr noe for de som styrer
- skape bestillerkompetanse!

Felles sikkerhet i forvaltningen

Felles anbefalinger gir samordnet hjelp

NSM Datatilsynet Digdir KS dfø Helsedirektoratet


Krav
§ § § § § § §
Regelverk
Anbefalinger
Styringsaktiviteter
Basisnivåer
Tiltaksbank
Spesialtilpassede basisnivåer
Veiledning
Generell Styringsveiledning
Fremgangsmåter Metoder
Veiledning om spesifikke sikkerhetstiltak og grupper av sikkerhetstiltak
Veiledning om særregler i et regelverk
Hjelpe-midler
Oppgavekatalog
Informasjonstyper
Støtteverktøy til styringsaktiviteter
Krav i anskaffelser
Felles produktvurderinger
Felles DPIA
Felles vurdering av risiko for like tjenester
Eksempelbank
Oversikt over begreper

KS

NSM

HDir

Datatilsynet

Økonomireglementet i staten

Digdir

DFØ

Personopplysningsloven

Sikkerhetsloven

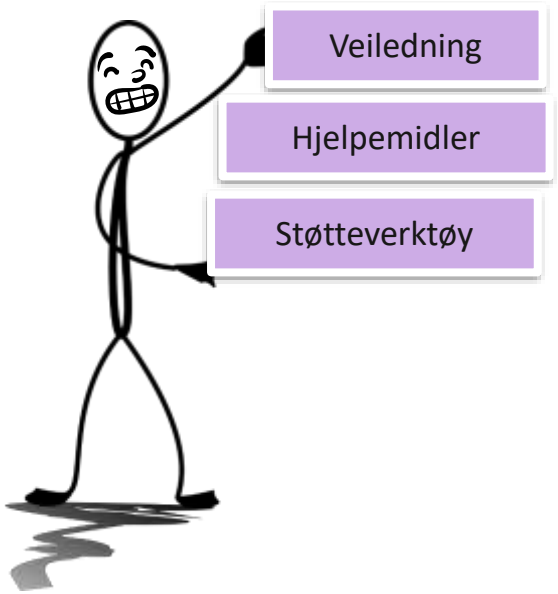
eForvaltningsforskriften § 15.2

Kommuneloven

Digitalsikkerhetsloven

Felles anbefalinger

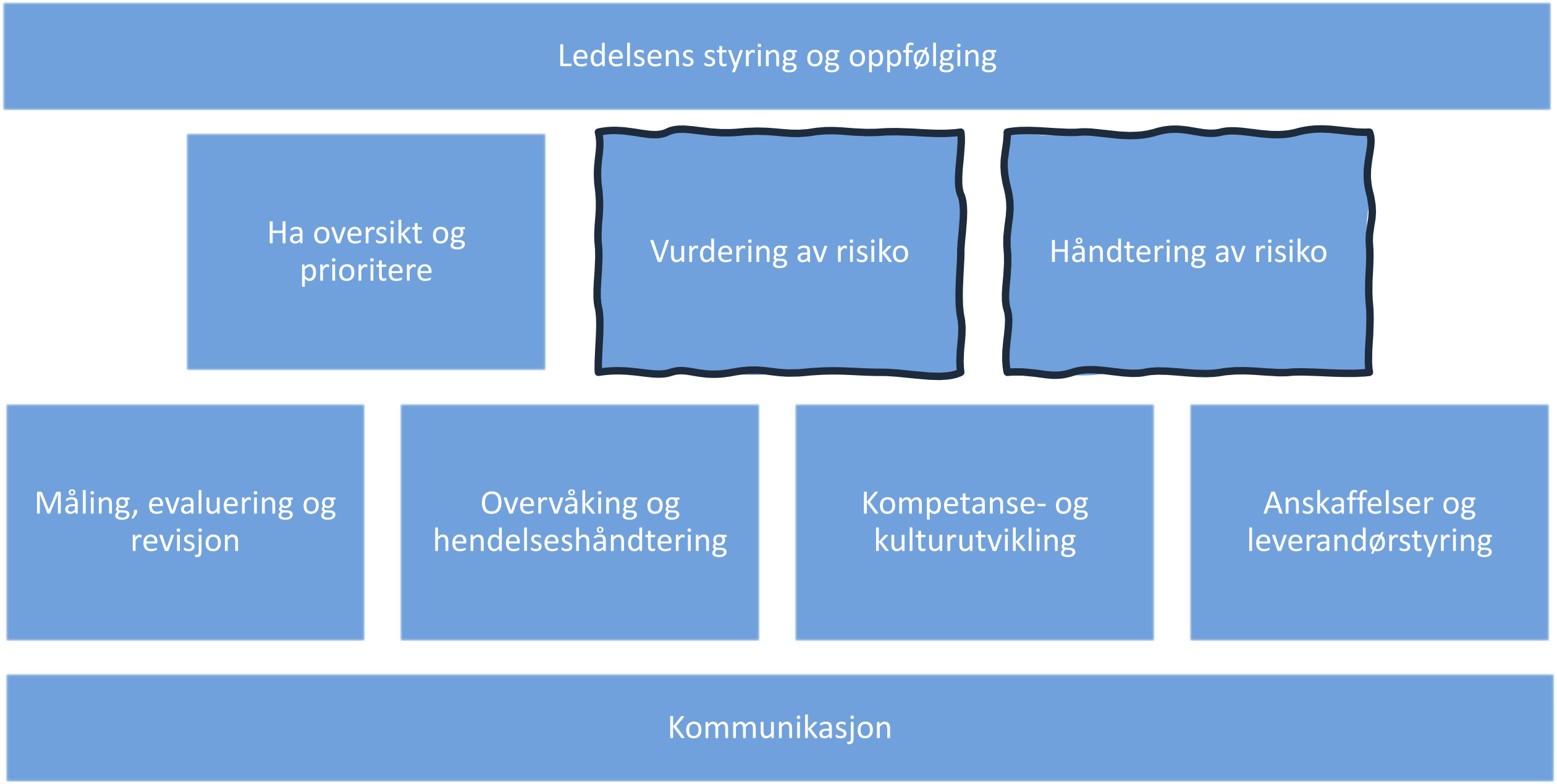
Styringsaktiviteter



Veiledning

Hjelpemidler

Støtteverktøy


Ledelsens styring og oppfølging
Ha oversikt og prioritere
Vurdering av risiko
Håndtering av risiko
Måling, evaluering og revisjon
Overvåking og hendelseshåndtering
Kompetanse- og kulturutvikling
Anskaffelser og leverandørstyring
Kommunikasjon

§ 4-2. *Vurdering av risiko*

Sikkerhetsloven

Virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.

§ 7. *Krav om sikkerhet for tilbydere av samfunnsviktige tjenester*

Digitalsikkerhetsloven

En tilbyder av en samfunnsviktig tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

§ 10. *Krav om sikkerhet for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Artikkel 32. *Sikkerhet ved behandlingen*

GDPR

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisat
sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

Artikkel 24. *Den behandlingsansvarliges ansvar*

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

Vurdering av risiko

Risikoeiere skal sørge for å ha tilstrekkelig oversikt over risiko på sitt ansvarsområde, og å vite hvilke risikoer som må håndteres.

Risikoeiere planlegger og gjennom
Vurderinger gjøres på oppgaver, t
disse.

Vurdering av risiko gjennomføres
risikovurderinger), men også når d
hendelser eller i forbindelse med e
og utvikling av digitale systemer.

RV1 - Planlegge risikovurdering

Risikoeier skal sørge for at det legges en plan før en risikovurder

Planleggingen bør som minimum inneholde:

- Beskrivelse av omfang og avgrensninger
- Valg av deltakere
- Valg av framgangsmåte, inkludert hensiktsmessige metoder
- Estimat av ressursbruk
- Hvordan arbeidet skal dokumenteres

Gir evne til

- Effektiv nnomfø g av ovurder ger, som gir et g beslutn sgrunnlag
- A rge fo t perso ed riktig kompetanse deltar og

RV-2 - Gjennomføre risikovurdering

Risikoeiere skal sørge for nødvendige risikovurderinger blir gjennomført. Omfan metodebruk og hvordan vurderingen gjennomføres må tilpa es det som s vurderes.

Når risikoeiere vurderer risiko, skal de benytte resultatet fra for lysen *a oversikt og prioritere*, og blant annet ta hensyn til

- hvilke trusler og far nformasjonsbehandl en i o gaver og tj ster kan bli utsatt for, og hvilke i masj rhets ersonvernbrudd det kan føre til
- hvilke konsekvenser inf sjonssikke ets- d rsonvernbrudd kan få for virksomhetens gaver tjenester, v somhetens økonomi, individer, andre virksomhete mfunnsfun ner eller sjonale sikkerhetsinteresser

etable sikkerhets- p vernstiltak for å forebygge, oppdage og reage å hend er som kan før p vernbrudd

Nå rderi er oppdateres kan det v endri som påvirker eksisterende sårbarheter, hvilke hendelser som kan oppstå.

Risikovurderingen skal dokumenteres beslutningsgrunnlag for risikoeier for

Gir evne til

- Å få oversikt over risiko på et område (oppgave, tjeneste, digitalt system eller annen avgrensing)
- Å ta beslutninger om risiko, inkludert bruk av virksomhetens ressurser på håndtering av risiko

RV-3 - Vurdere risiko etter hendelser

Risikoeiere skal gjøre ny behovsvurdering og etter behov gjennomføre risikovurderinger når de blir kjent med informasjonssikkerhetshendelser eller hendelser som har påvirket personopplysningsvernet.

Gir evne til

- Å ha oppdatert oversikt over risiko når hendelser har tilført ny informasjon til bruk i vurderingene.

Cyberslagmark 2026 - Totalforsvarsåret 2026

Syv forventninger fra NATO:

1. Kontinuitet i nasjonale styringssystemer og kritiske offentlige tjenester
2. Robust kraftforsyning
3. Evne til å håndtere ukontrollert forflytning av mennesker
4. Robust mat- og vannforsyning
5. Evne til å håndtere masseskadesituasjoner
6. Robuste sivile kommunikasjonssystemer
7. Robuste transportsystemer.

CER og NIS2-direktivene

EU har vedtatt to direktiver med formål å styrke motstandskraften til virksomheter som leverer samfunnsviktige tjenester.

Hvordan lykkes over tid

Det å være digitalt forberedt handler ikke om å bli immun mot alle risikoer og hendelser— det handler om å stå støtt når truslene rammer.

Seks ting du kan gjøre

- Vurder tilstanden til virksomheten: Hva er kritisk, hva er sårbart?
- Sørg for at du har en tydelig plan for å oppfylle GDPR og NIS/DSL-kravene.
- Gå gjennom forsyningskjeden din: Hvilke avhengigheter finnes, og hvor sikre er de?
- Ledergruppen har ansvaret: Bidra til å gjøre risikoer og nødvendige investeringer synlige.
- Sørg for at du har riktige partnerskap på plass for å kunne reagere raskt ved hendelser.
- Etabler felles styringsaktiviteter på tvers av informasjonssikkerhet og personvern

Eirik Gulbrandsen

Datatilsynets seksjon for Teknologi, Sikkerhet og Tilsyn

eirik.gulbrandsen@datatilsynet.no

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no