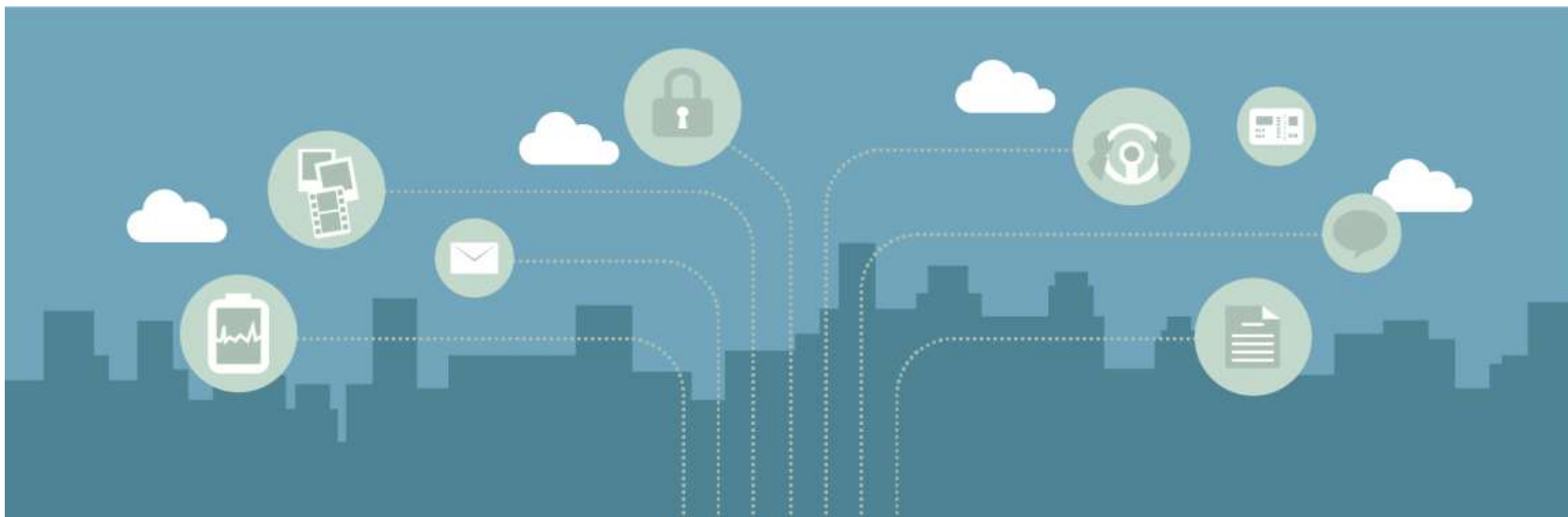




Sikkert.no

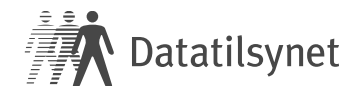
hva trenger vi i den nasjonale sikkerhetsverktøykassa?

KiNS - tech konferansen 2026

Eirik Gulbrandsen | spesialrådgiver

Alvilde Ryan Pharo, rådgiver

Seksjon Teknologi, Sikkerhet og Tilsyn



Varsler tilsyn med alle Norges kommuner

Som en del av Totalforsvarsåret 2026, har Datatilsynet satt i gang et omfattende tilsyn med hvordan norske kommuner sikrer personopplysninger.

Denne uken er det derfor sendt ut brev til alle landets 357 kommuner for å kartlegge kommunenes arbeid med personopplysningssikkerhet og sikkerhetshendelser.

– Målet med tilsynene er å bidra til at norske kommuner blir bedre rustet til å både forebygge og håndtere sikkerhetshendelser. De tiltakene vi nå skal kontrollere, er tett knyttet til beredskap, sier direktør i Datatilsynet, Line Coll.



Pressekontakt

Camilla Nervik
seksjonsjef for offentlige tjenester



Kontor: (+47) 22 39 69 29
E-post: csn@datatilsynet.no



Gjennomføring i tre faser

Kontrollen er delt opp i tre trinn som vil gjennomføres i løpet av 2026, hvor første fase er i gang:

- 1 Kartlegging:** Alle norske kommuner må svare på spørsmål om hvordan de ivaretar personopplysningssikkerheten. Svarfristen for tilbakemelding fra kommunene er 20. februar 2026.
- 2 Dokumentasjon:** Et utvalg kommuner må sende inn utfyllende dokumentasjon om sine systemer og rutiner.
- 3 Kontroll på stedet:** Vi gjennomfører stedlige tilsyn med et utvalg kommuner.

- ✓ Tidligere tilsyn og rapporterte avvik viser at det er stor forskjell på i hvilken grad norske kommuner ivaretar personopplysninger på en sikker måte.
- ✓ Mange sikkerhetsbrudd skyldes svake løsninger for pålogging (*autentisering*). Dette er et av områdene som vi vektlegger i kontrollen.
- ✓ Datatilsynet erfarer også at konsekvensene av digitale angrep blir unødvendig store om kommunene mangler gode rutiner for gjenoppretting av data.

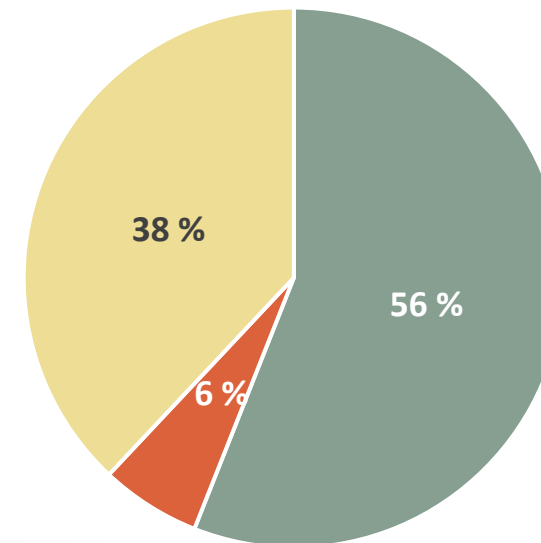


Styringssystem – forutsetning for å lykkes på sikt

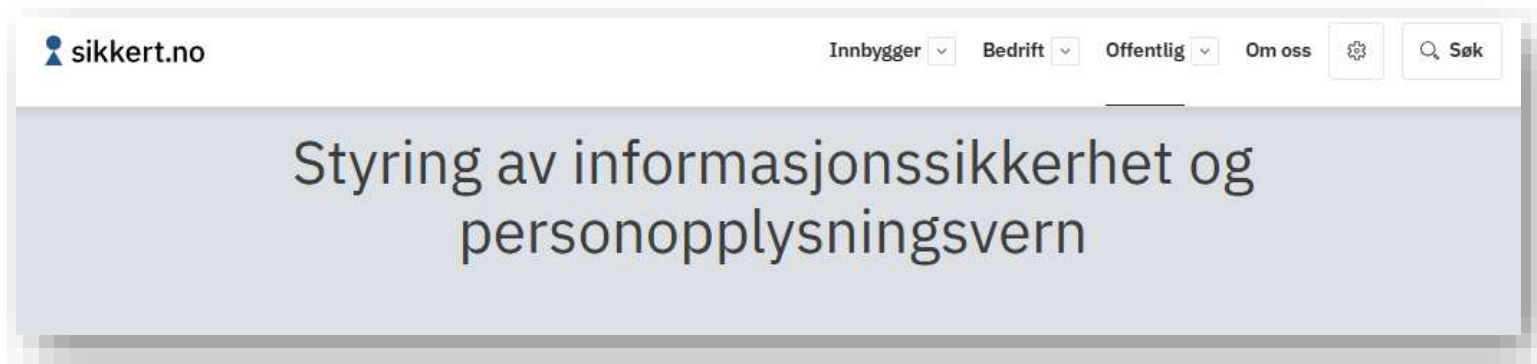


- De fleste kommunene har et styringssystem.
- Flere små kommuner (10 prosent) enn snittet mangler et styringssystem.

Har kommunen et etablert styringssystem for å ivareta arbeidet med informasjonssikkerhet og personvern?



■ Ja ■ Nei ■ Delvis

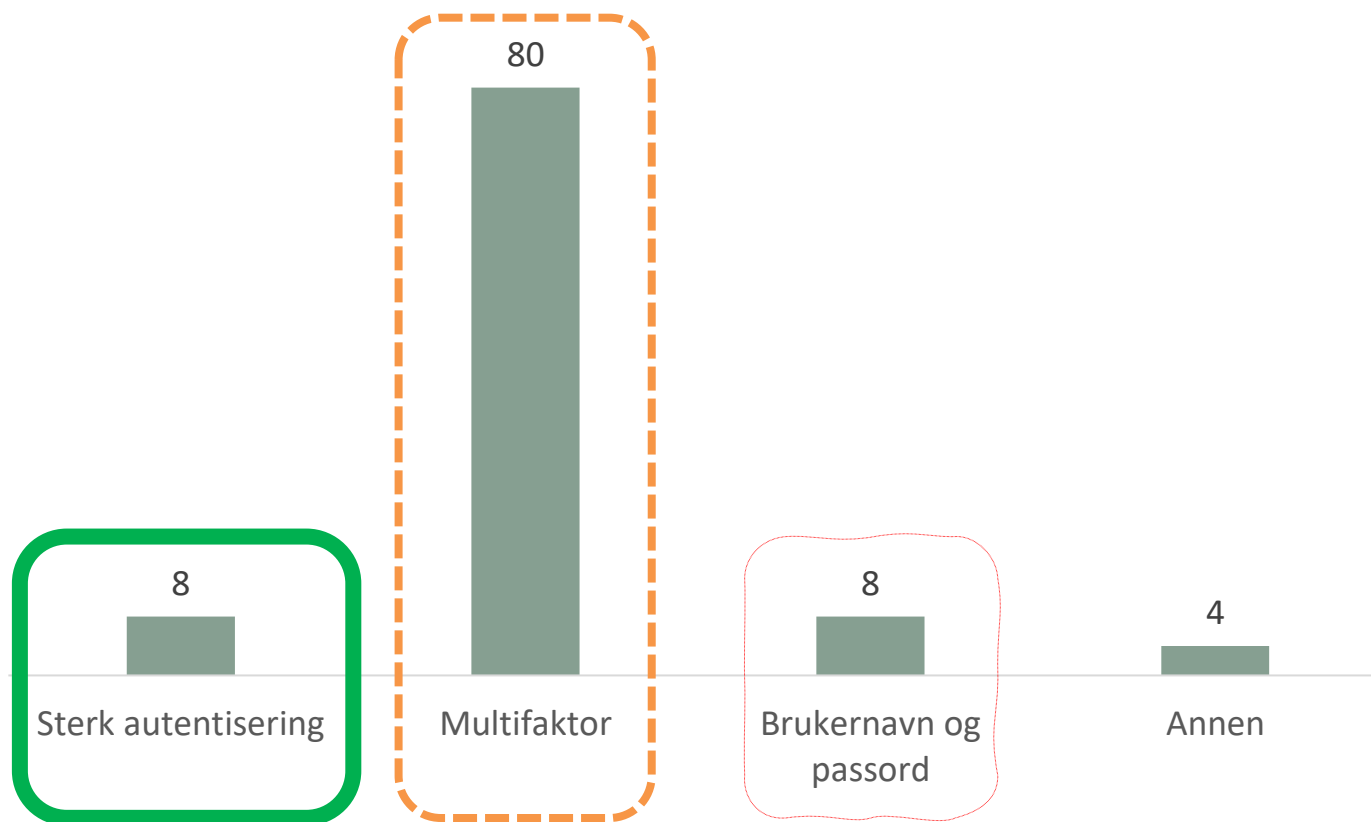


Sterk autentisering – bidrar redusere sannsynlighet



- 80 prosent bruker **multifaktor** som primær sikkerhetsmekanisme
- Ingen nevneverdige forskjeller mellom små, mellomstore og store kommuner
- 59 prosent har ikke gjennomført ROS før valg av autentiseringsløsning

Oppgi kommunens **primære** sikkerhetsmekanisme for autentisering av brukere og systemer (prosent)





PASSORD ALENE KAN IKKE LENGER REGNES SOM ET «TILSTREKKELIG» TILTAK

- Svak autentisering er primær angrepsvektor i mange avviksmeldinger
- **Mange 2-faktor / multifaktor-løsninger er ikke gode nok og blir også omgått**
- «vi har slått på MS365 MFA og skjønner ikke hvordan angriper kom seg inn»
- Microsofts «legacy» 2-faktor er det mest omgåtte MFA-løsningen
- Microsoft «tvinger» selv overgang til **Passkeys** = Tilgangsnøkler = **Fido2**/Webauth
= **«Phishingresistent autentisering»**



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



Digitalsikkerhetsforskriften § 10. Teknologiske sikkerhetstiltak

Teknologiske sikkerhetstiltak skal minst omfatte

- a. **sterk autentisering** for adgang til nettverk og informasjonssystemer

Overgang til phishingresistent autentisering

NSM anbefaler virksomheter å gå over til **passnøkler (passkeys) eller andre FIDO2-implementasjoner for autentisering**. Årsaken er at aktører i økende grad tar seg forbi tradisjonell flerfaktorautentisering. I 2024 har NSM og sektorvise responsmiljøer registrert en rekke phishingkampanjer der målet var økonomisk vinning, ofte via fakturasvindel. **Kampanjene lar seg gjennomføre fordi virksomheter ikke påkrever phishingresistent autentisering.**

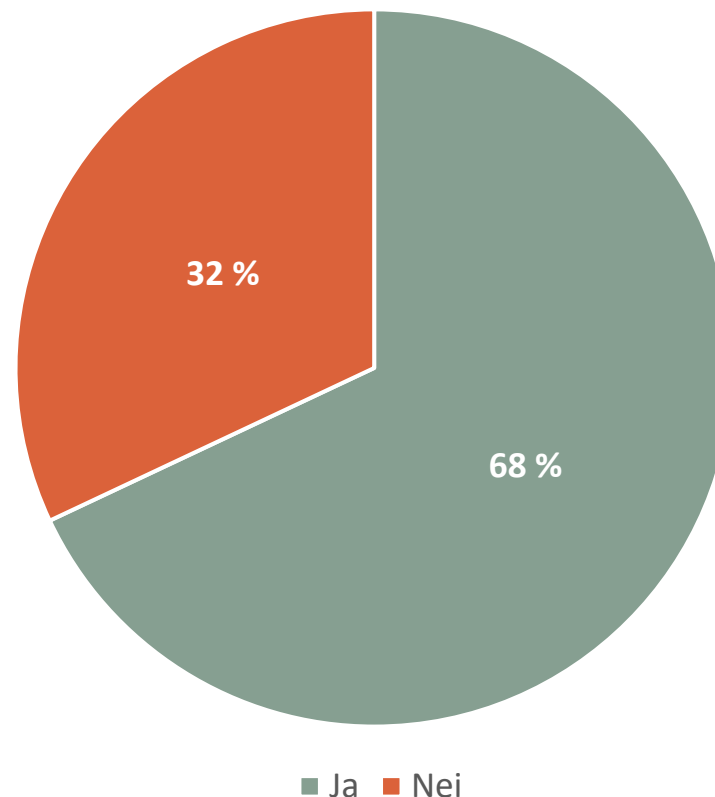


Evne til å **gjenopprette** data og systemer – tilgjengelighet



- De fleste kommunene har retningslinjer for gjenoppretting av data og systemer.
- Blant disse 68 prosentene har:
 - 77 prosent en vurdering av systemenes kritikalitet og prioritering av systemene
 - 90 prosent fordelt oppgaver og ansvar
 - 50 prosent krav til gjenopprettingstid

Har kommunen overordnede retningslinjer for gjenoppretting av data og systemer?





Hva er det viktigste å gjøre når det smeller?

Det samme som du gjorde i går!

*Pvf 32.1.c) evne til å **gjenopprette** tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,*

*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.***



Varsler tilsyn med alle Norges kommuner

Som en del av Totalforsvarsåret 2026, har Datatilsynet satt i gang et omfattende tilsyn med hvordan norske kommuner sikrer personopplysninger.

Denne uken er det derfor sendt ut brev til alle landets 357 kommuner for å kartlegge kommunenes arbeid med personopplysningssikkerhet og sikkerhetshendelser.

– Målet med tilsynene er å bidra til at norske kommuner blir bedre rustet til å både forebygge og håndtere sikkerhetshendelser. De tiltakene vi nå skal kontrollere, er tett knyttet til beredskap, sier direktør i Datatilsynet, Line Coll.



Pressekontakt

Camilla Nervik
seksjonsjef for offentlige tjenester



Kontor: (+47) 22 39 69 29
E-post: cmn@datatilsynet.no



Gjennomføring i tre faser

Kontrollen er delt opp i tre trinn som første fase er i gang:

1 **Kartlegging:** Alle norske kommuner ivaretar personopplysningssikkerhet. Kommunene er 20. februar 2026

2 **Dokumentasjon:** Et utvalg kommuner dokumentasjon om sine systemer

3 **Kontroll på stedet:** Vi gjennomfører kontroll på stedet i kommuner.

- ✓ Tidligere tilsyn og rapporterte avvik viser at det er stor forskjell på i hvilken grad norske kommuner ivaretar personopplysninger på en sikker måte.
- ✓ Mange sikkerhetsbrudd skyldes svake løsninger for pålogging (*autentisering*). Dette er et av områdene som vi vektlegger i kontrollen.
- ✓ Datatilsynet erfarer også at konsekvensene av digitale angrep blir unødvendig store om kommunene mangler gode rutiner for gjenoppretting av data.

Er kun kommuner som er med i fase 2 aktuelle for eventuelt stedlig tilsyn i fase 3?

Alle 357 kommunene fra fase 1 kan bli valgt for stedlig tilsyn i fase 3.

sikkert.no

Bedre digital sikkerhet for alle

For å bevare Norges digitale grunnmur må alle som er koblet til internett samarbeide. Her finner du råd og veiledning til hvordan du kan bidra. DNT kunnskap styrker vår felles motstandskraft.

[Trenger du hjelp?](#)[Er jeg godt nok sikret?](#)

Råd for digital sikkerhet

Her finner du gode råd om digital sikkerhet, enten du er innbygger eller ansatt i en bedrift eller offentlig myndighet.

[Innbygger](#)[Bedrift](#)[Offentlig](#)

Bedrift **Offentlig**

Digitalsikkerhetsloven og -forskriften

Digital sikkerhet for alle

Disse sidene drives av myndighetene i Norge for å gi viktig kunnskap om digital sikkerhet. Du finner råd og veiledning, enten du er innbygger, ansatt eller leder i en bedrift eller offentlig forvaltning.



NASJONAL
SIKKERHETSMYNDIGHET



POLITIET



Datatilsynet

Digdir

Styring av informasjonssikkerhet og personopplysningsvern

Hjem > Offentlig > Styring av informasjonssikkerhet og personopplysningsvern

**Offentlig**

Introduksjon

Offentlige virksomheter og deres ledere har ansvar for å styre risiko for sine oppgaver og tjenester. Å styre informasjonssikkerhet og personopplysningsvern er en del av dette, og bør være integrert i virksomhetsstyringen.

[→](#)

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretagelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

[→](#)

Ha oversikt og prioritere (OP)

Alle risikoeiere i virksomheten skal ha god oversikt over sine ansvarsområder, slik at arbeidet med styring av informasjonssikkerhet og personopplysningsvern gjøres effektivt.

[→](#)

Vurdering av risiko (RV)

Risikoeiere skal sørge for å ha tilstrekkelig oversikt over risiko knyttet til informasjonssikkerhet og personopplysningsvern på sitt ansvarsområde, og vite hvilke risikoer...

[→](#)

Håndtering av risiko

Måling, evaluering og digitalsikkerhetsloven

Virksomheter som omfattes av digitalsikkerhetsloven plikter å sørge for å oppfylle loven og forskriften. Les mer om hvordan og hvilke tiltak som gjelder.

[→](#)

Overvåking og tjenester

Virksomheter som tilbyr samfunnsnødvendige tjenester skal melde fra til både NSM og Datatilsynet om sikkerhet og datavern. Innretningen skal sikre at risikoen for å bli angrepet er lav.

[→](#)

Veileder i digitalsikkerhetsloven og -forskriften

NSM har utarbeidet veiledning i digitalsikkerhetsloven og -forskriften for virksomheter.

[→](#)

Cyberus er tilsatt til å følge opp sikkerhetsmyndighet. Formålet med Cyberus er å sikre at sikkerheten i Norge er god, med cyberikkerhet. Cyberus er et tett samarbeid med egen digitale sikkerhet og datavern. Sikkerhet i sikkerhet og datavern er en del av sikkerheten i Norge. Det er 30 minutter å gjennomføre undersøkelsen.

Slik fungerer tjenesten:

- Tjenesten er organisert i 11 kategorier
- Slett på alle eller de kategorier som er aktuelle for denne virksomheten.
- Basert på svarene oppgitt for denne tjenesten vil de viktigste utfordringene som...

Styring av informasjonssikkerhet og personopplysningsvern

Hjem • Offentlig • Styring av informasjonssikkerhet og personopplysningsvern



Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretagelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

Ha oversikt og prioritering

Alle risikoer skal ha god oversikt slik at arbeidet med informasjonssikkerhet og personopplysningsvern gjøres effektivt...

ansvarsområde, og vite hvilke risikoer...

virksomhetens oppgaver og tjenester.

- ✓ ISO 27001 / 27002, CIS, NIST
- ✓ NSM Grunnprinsipper
- ✓ Normen
- ✓ KS veiledninger
- ✓ Digdir veiledninger
- ✓ DFØ veiledning anskaffelser
- ✓ Datatilsynets veiledninger (GDPR)
- ✓ Digitalsikkerhetsloven (NIS)

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretagelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

gjennomføres

Innhold

Introduksjon

Ledelsens styring og oppfølging (LS)

LS-1 Gi føringer

LS-2 Sørge for budsjett til arbeidet

LS-3 Kommunisere viktighet

LS-4 Løfte og håndtere problemstillinger gjennom linjen

LS-5 Virksomhetsledelsens gjennomgang

Ha oversikt og prioritere (OP)

Vurdering av risiko (RV)

Håndtering av risiko (RH)

Måling, evaluering og revisjon (ME)

Overvåking og hendelseshåndtering (OH)

Kompetanse- og kulturutvikling

Kommunikasjon (KO)



NSM



Datatilsynet



Digdir



Helsedirektoratet

Håndtering av risiko

Måling, evaluering og

Overvåking og

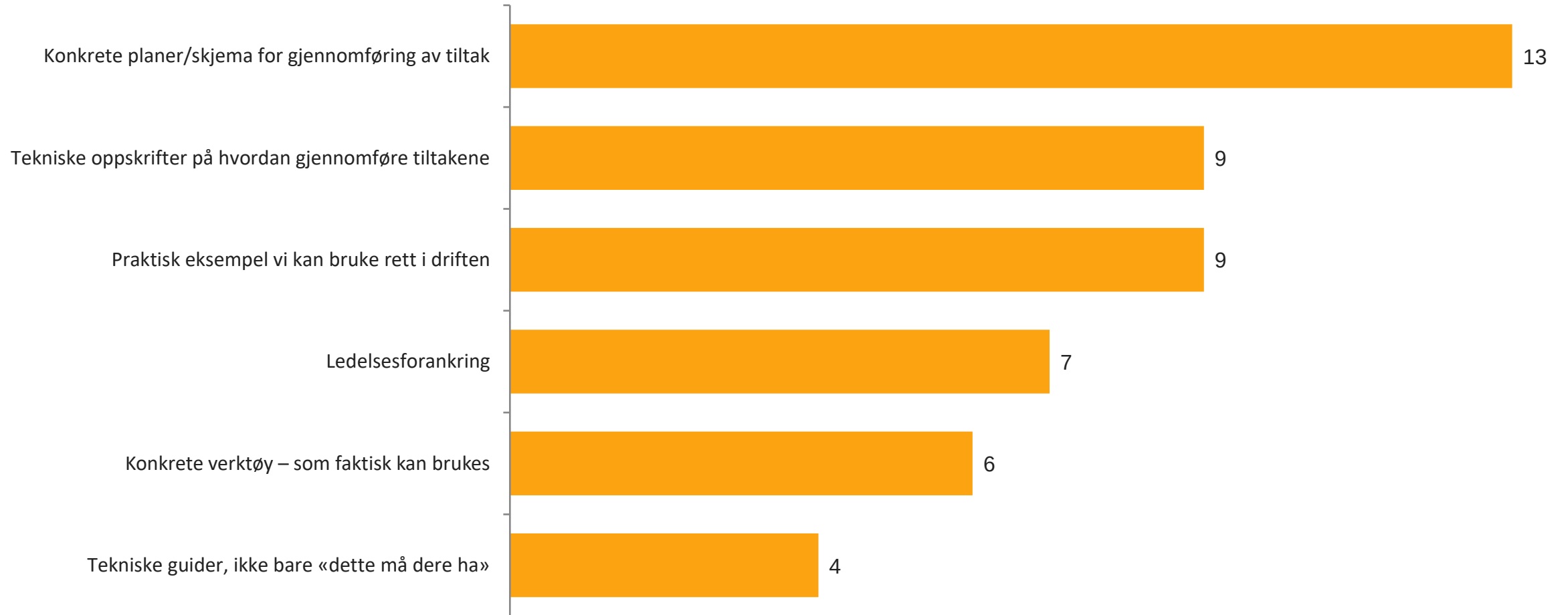
- delegering av oppgaver for å styre informasjonssikkerhet og

personopplysningsvern til ledere som er mål- og resultatansvarlige for et område (risikoeiere).



- Har du benyttet **sikkert.no** for å finne informasjon?
- Hvordan var det å navigere på **sikkert.no**?
- Ga informasjon du fant på **sikkert.no** verdi?
- Hva vil gjøre **sikkert.no** til en nyttig ressurs for deg og din virksomhet?

sikkert.no: ønske om konkret informasjon



Mest likte fritekstsvar (likes). 29 av 55 deltakere, 22 svar.

- ✓ ISO 27001 / 27002, CIS, NIST
- ✓ NSM Grunnprinsipper

- ✓ Normen
- ✓ KS veiledninger
- ✓ Digdir veiledninger
- ✓ DFØ veiledning anskaffelser
- ✓ Datatilsynets veiledninger (GDPR)
- ✓ Digitalsikkerhetsloven (NIS)

Anbefalinger om styring av informasjonssikkerhet og personopplysningsvern

Utarbeidet av Digdir, Datatilsynet, NSM, KS, DFØ og Helsedirektoratet i programmet Felles sikkerhet i forvaltningen.

Oversikt over styringsaktivitetene

LS Ledelsens styring og oppfølging - LS-1 Gi føringer - LS-2 Sørge for budsjett til arbeidet - LS-3 Kommunisere viktighet - LS-4 Løfte og håndtere problemstillinger gjennom linjen - LS-5 Virksomhetsledelsens gjennomgang	OP Ha oversikt og prioritere - OP-1 Oversikt over ansvarsområde - OP-2 Kartlegge eksterne krav - OP-3 Vurdere behov for risikovurderinger - OP-4 Oppdatert oversikt over risikovurderinger	RV Vurdering av risiko - RV-1 Planlegge risikovurdering - RV-2 Vurdere personvernkonsekvensvurdering (DPIA) - RV-3 Gjennomføre risikovurdering - RV-4 Vurdere risiko etter hendelser
RH Håndtering av risiko - RH-1 Foreslå håndtering av risikoer - RH-2 Godkjenne forslag til risikohåndtering - RH-3 Iverksette godkjent håndtering av risiko - RH-4 Forvalte fellessikring og tilleggssikring	ME Måling, evaluering og revisjon - ME-1 Vurdere status på eget ansvarsområde - ME-2 Måle tilstanden på områder over tid - ME-3 Gjennomføre evalueringer /internrevisjon - ME-4 Vurdere effektivitet av sikkerhets- og personverntiltak	OH Overvåking og hendelseshåndtering - OH-1 Overvåking etter behov - OH-2 Følge opp hendelser og avvik - OH-3 Varsling ved hendelser - OH-4 Beredskap og krisehåndtering
KK Kompetanse- og kulturutvikling KK-1 Gi grunnopplæring til risikoeiere	AL Anskaffelser og leverandørstyring - AL-1 Identifisere behov - AL-2 Håndtere risiko og stille krav	KO Kommunikasjon - KO-1 Formidle føringer - KO-2 Dokumentere gjennomførte



- "Felles anbefalinger om styring av informasjonssikkerhet og personopplysningsvern"...
- Hva ville gjøre "Felles anbefalinger om styring av informasjonssikkerhet og personopplysningsvern" til en nyttig ressurs for deg og din virksomhet?

Felles anbefalinger treffer et behov



90 %

37 av 41

mener anbefalingene kan være aktuelle for å videreutvikle eller komplettere eksisterende veiledning og styringsarbeid.

Bare 4 av 41 mener eksisterende veiledning allerede dekker behovene.

Eirik Gulbrandsen Alvilde Ryan Pharo

Datatilsynets seksjon for Teknologi, Sikkerhet og Tilsyn

egu@datatilsynet.no
arp@datatilsynet.no



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

datatilsynet.no
personvernbloggen.no