Spørreundersøkelse om informasjonssikkerhetsarbeidet i statsforvaltningen 2024

Vi gjennomfører en evaluering av arbeidet med informasjonssikkerhet i statsforvaltningen og trenger svar fra deg som er fagansvarlig informasjonssikkerhet/CISO/informasjonssikkerhetsleder i virksomheten.

Undersøkelsen består av totalt 26 spørsmål i fem deler. Svar etter beste evne basert på din opplevelse av status på informasjonssikkerhetsarbeidet i virksomheten.

Om respondenten

1. Virksomhetens navn:
2. Hvem svarer på undersøkelsen (angi rolle eller funksjon, ikke navn):

Del 1 - Om virksomheten

3. Omtrent hvor mange ansatte var det i din virksomhet 31. desember 2023 (antall personer som var ansatt i virksomheten, uavhengig av stillingstype eller stillingsprosent)?

Antall:
<tallet>

4. Hvor mange personer i virksomheten arbeider med fagområdet informasjonssikkerhet?

Antall:
<tallet>
Forklaring til spørsmål: Personer som har informasjonssikkerhetsarbeid som sin primæroppgave i hele eller deler av arbeidstiden. Dette inkluderer både egne ansatte og eksterne konsulenter.

5. Benytter virksomheten Digdirs veiledningsmateriell på informasjonssikkerhetsområdet? **70**

Ja	**Nei**	**Vet ikke**
52	**13**	**5**
Forklaring til spørsmål: Digdir sitt veiledningsmateriell er tilgjengelig på https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet/882		

Del 2 - Styring og kontroll på informasjonssikkerhetsområdet

6. I hvilken grad gir virksomhetsledelsen tydelige føringer for styring av informasjonssikkerhetsarbeidet? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
2	**5**	**35**	**28**	**0**	**0**

Forklaring til spørsmål:
Føringene vil normalt inkludere roller og ansvar, innhold i systematiske aktiviteter, hvordan risiko skal forstås og vurderes, med mer.

I informasjonssikkerhetsarbeidet kan aktivitetene være:

- ledelsens styring og oppfølging
- vurdering og håndtering av risiko
- måling, evaluering og revisjon
- overvåking og hendelseshåndtering
- kompetanse- og kulturutvikling

Se Digdirs veiledningsmateriell, jf. ISO/IEC 27001 kap. 4 til kap. 10:
https://www.digdir.no/informasjonssikkerhet/utforme-foringer/3159

7. Hvem har det formelle ansvaret for å vurdere og håndtere risiko innen informasjonssikkerhet? **70**

Alternativ	Sett kryss (bare ett kryss)
Ledere og mellomledere, som ledd i ordinær linjeledelse	**58**
Egen gruppe, fagansvarlig informasjonssikkerhet, eller lignende	**12**

Forklaring til spørsmål:
Dersom det formelle ansvaret for beslutninger om informasjonssikkerhetsrisiko er en del av det generelle ledelsesansvaret, velger du det første alternativet.

Dersom det formelle ansvaret for beslutninger om informasjonssikkerhetsrisiko tas av spesialfunksjoner eller andre, velger du det andre alternativet.

Vær oppmerksom på at ledere med ansvar for styring av risiko kan få støtte av spesialfunksjoner og fagpersoner, uten at de mister ansvaret for beslutninger om risiko.

8. I hvilken grad har virksomheten vurdert om informasjonssikkerhetshendelser vil kunne føre til utfordringer med virksomhetens evne til å levere sine tjenester? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**2**	**29**	**39**	**0**	**0**

9. I hvilken grad ser virksomheten risikostyring av informasjonssikkerhet i sammenheng med den øvrige risikostyringen i virksomheten?

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	8	30	31	0	0

Forklaring til spørsmål:
Øvrig risikostyring er for eksempel HMS, personvern, måloppnåelse og annen virksomhetsstyring.

10. I hvilken grad har virksomheten tydelige retningslinjer for å akseptere risiko? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	16	38	15	0	0

Forklaring til spørsmål:
Tydelige retningslinjer bør ta hensyn til
- hvor viktig oppgaven er for virksomheten
- hvor mye arbeidsinnsats som har vært lagt i å finne tiltak for å redusere risiko
- om man har vurdert alternative arbeidsmåter for å unngå risiko
- hvilke ledelsesnivåer som kan akseptere restrisiko av forskjellig størrelse

11. I hvilken grad opplever du at risikoeiere vurderer status på sitt ansvarsområde? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	10	43	16	0	1

Forklaring til spørsmål:

En risikoeier er stillingen som er pekt ut som ansvarlig for å nå ett eller flere mål for virksomheten og for å få utført tilhørende arbeidsoppgaver. I andre kontekster kalles de gjerne mål- og resultatansvarlig, oppgaveeier eller prosesseier.

En vurdering av status kan inkludere vurderinger av:

- om vedkommende selv og de personer risikoeier har ansvaret for
  - følger gjeldende lov- og regelverk
  - gjennomfører pålagte oppgaver i internkontroll- og sikkerhetsarbeidet på en tilfredsstillende måte
  - etablerer og følger opp vedtatte eller avtalte sikkerhetstiltak
  - etterlever innførte sikkerhetstiltak
- om sikkerhetstiltak man har ansvaret for fungerer som forutsatt

Se mer på https://www.digdir.no/informasjonssikkerhet/vurdere-status-pa-eget-ansvarsomrade/3049

12. Vurderer de som er ansvarlige for sikkerhetstiltak (tiltaksleverandører) systematisk status på sine ansvarsområder minst en gang i året? **70**

Ja	Nei	Vet ikke
36	22	12
Forklaring til spørsmål: Se forklaringen i forrige spørsmål.		

13. I hvilken grad gjennomfører dere regelmessige risikovurderinger for arbeidsoppgavene virksomheten har ansvar for? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**7**	**35**	**25**	**1**	**2**
Forklaring til spørsmål: Risikovurdering handler om å vurdere konsekvens og tilhørende sannsynlighet knyttet til uønskede informasjonssikkerhetshendelser som kan påvirke virksomhetens måloppnåelse.					

14. I hvilken grad har virksomheten en hensiktsmessig organisering av drift og forvaltning av sikkerhetstiltak? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**8**	**40**	**22**	**0**	**0**
Forklaring til spørsmål: En hensiktsmessig organisering fører til effektiv gjennomføring av risikovurderinger og kostnadseffektiv forvaltning av sikkerhetstiltak. Det vil normalt inkludere en beskrivelse av grunnleggende sikkerhetstiltak i virksomheten, slik at alle risikoeiere vet hvilke sikkerhetstiltak som allerede er på plass når de skal vurdere risiko på sine ansvarsområder. Se mer på https://www.digdir.no/informasjonssikkerhet/om-fellessikring-og-tilleggssikring/3043					

15. I hvilken grad godkjenner og iverksetter virksomheten sikkerhetstiltak på en systematisk måte? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	**9**	**40**	**20**	**0**	**0**

Forklaring til spørsmål:
Spørsmålet handler om ansvar for beslutninger om iverksetting av sikkerhetstiltak. Dette er normalt risikoeiers ansvar og bør dokumenteres.

Et sikkerhetstiltak er noe som etableres for å virke over tid. Det er relatert til sikkerhet og etablert for å redusere eller på annen måte modifisere risiko.

16. I hvilken grad er dere i stand til å etablere de sikkerhetstiltak som dere har vurdert at det er behov for? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**4**	**23**	**42**	**0**	**1**

17. I hvilken grad gjennomfører virksomheten regelmessig evaluering av etablerte sikkerhetstiltak for å finne ut om tiltakene virker etter hensikten? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**14**	**41**	**13**	**0**	**2**

Del 3 - Beredskap, øvelser og hendelseshåndtering

18. I hvilken grad arbeider virksomheten systematisk med øvelser på informasjonssikkerhetsområdet? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	15	29	25	0	0

Forklaring til spørsmål:
Øvelser på informasjonssikkerhetsområdet omfatter å trene på håndtering av hendelser som rammer digitale tjenester, IKT-infrastruktur eller andre utfordringer relatert til informasjonssikkerhet

19. Gjennomfører virksomheten minst én øvelse årlig på informasjonssikkerhetsområdet? **70**

Ja	Nei	Vet ikke
53	15	2

Forklaring til spørsmål:
Øvelser på informasjonssikkerhetsområdet omfatter å trene på håndtering av hendelser som rammer digitale tjenester, IKT-infrastruktur eller andre utfordringer relatert til informasjonssikkerhet

20. Virksomhetens håndtering av informasjonssikkerhetshendelser er basert på at:

Alternativer:	Sett kryss (flere kryss er tillatt)
Vi har definerte roller og ansvar	62
Vi har en egen funksjon for koordinering av håndtering av informasjonssikkerhetshendelser (eks: Security Incident Response Team)	55
Vi har oversikt over behov for kompetanse hos alle som er involvert i varsling, deteksjon og håndtering av hendelser	23
Vi har definerte prosedyrer for håndtering av hendelser	53
Vi har rapporteringsrutiner ved avvik	61
Annet	5

21. I hvilken grad har virksomheten oversikt over kostnadene som følge av informasjonssikkerhetshendelser? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
5	27	25	7	1	5

Del 4 - Kultur og kompetanse

22. I hvilken grad opplever du at informasjonssikkerhetsarbeidet har prioritet hos ledelsen? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	1	31	38	0	0

23. I hvilken grad kartlegger virksomheten behov for kompetanseheving på informasjonssikkerhetsområdet? **70**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	16	43	10	0	0

Forklaring til spørsmål:
Se beskrivelse av sikkerhetskultur og kompetanse- og kulturutvikling i Digdirs veileder for dette: https://www.digdir.no/informasjonssikkerhet/kompetanse-og-kulturutvikling-innen-informasjonssikkerhet/2187

24. Har virksomhetsledelsen i løpet av 2023 tatt initiativ til at det blir gjennomført tiltak for å styrke informasjonssikkerhetskulturen i virksomheten for noen av disse gruppene? **70**

For alle ansatte	For grupper av ansatte	For ledergruppen	Ikke gjennomført tiltak	Ikke relevant	Vet ikke
49	23	28	9	0	1

Del 5 - Avsluttende del

25. Har du noen ytterligere kommentarer til • deres arbeid med informasjonssikkerhet i virksomheten • arbeidet med informasjonssikkerhet i statsforvaltningen • informasjonssikkerhetsarbeid du ønsker å synliggjøre som du er spesielt fornøyd med • annet

26. Vi ønsker å gjennomføre korte intervjuer i etterkant av spørreundersøkelsen. Ønsker du å bli kontaktet for et intervju?

Ja	**Nei**

Skjema for utfylling ved ev. intervju

Vi ønsker å gjennomføre korte intervjuer i etterkant av spørreundersøkelsen. Ønsker du å bli kontaktet for et intervju, fyll ut skjemaet under.

Kontaktinformasjon for eventuell oppfølging av undersøkelsen:	
Navn	
E-post	
Telefonnummer	

Takk for ditt bidrag til undersøkelsen!