Spørreundersøkelse om informasjonssikkerhet

Vi gjennomfører en evaluering av arbeidet med informasjonssikkerhet i statsforvaltningen og trenger svar fra deg som er fagperson for informasjonssikkerhet i virksomheten.

Om respondenten

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

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

Del 1 - Om virksomheten

1. Omtrent hvor mange ansatte var det i virksomheten 31. desember 2017 (antall personer som var ansatt i virksomheten, uavhengig av stillingstype eller stillingsprosent)?

Antall:
<tallet>

2. Hvor stor andel av arbeidsoppgavene for å ivareta informasjonssikkerheten i virksomheten utføres av eksterne tjenesteleverandører eller konsulenter? **76**

0 % av oppgavene	**< 30% av oppgavene**	**30 % - 70 %**	**> 70 % av oppgavene**	**Ikke relevant**	**Vet ikke**
15	**47**	**11**	**3**	**0**	**0**
Gi gjerne eksempel på typiske arbeidsoppgaver som settes ut til eksterne tjenesteleverandører eller konsulenter:					

3. 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.

4. Hvilken fagkompetanse har de som arbeider med informasjonssikkerhet i virksomheten? **76**

Alternativer:		**Sett kryss (flere kryss er tillatt)**
Informasjonssikkerhetsutdanning	**4a**	**44**
IKT-utdanning (generell)	**4b**	**72**
Militær- eller politifaglig utdanning	**4c**	**16**
Juridisk utdanning	**4d**	**32**
Økonomi-/lederutdanning	**4e**	**45**
Realkompetanse (ingen formell utdanning)	**4f**	**34**
Annen utdanning/kompetanse:		
	4g	**15**

5. Klarer virksomheten å dekke sitt behov for fagkompetanse på informasjonssikkerhetsområdet? **75**

Ja	Nei	Vet ikke
51	**20**	**4**
Hvis nei, hvorfor klarer ikke virksomheten å dekke sitt behov for fagkompetanse?		

6. Benytter virksomheten Difis veiledningsmateriell om internkontroll på informasjonssikkerhetsområdet? **76**

Ja	Nei	Vet ikke
56	**18**	**2**
Forklaring til spørsmål: Difis veiledningsmateriell er tilgjengelig på http://internkontroll.infosikkerhet.difi.no/		

Del 2 - Styring og kontroll på informasjonssikkerhetsområdet

7. I hvilken grad gir virksomhetsledelsen tydelige føringer for internkontroll og styringssystem for informasjonssikkerhet? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**4**	**35**	**37**	**0**	**0**
Gi gjerne noen eksempler på hvordan det er gitt tydelige føringer:					
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 de systematiske aktivitetene være: • ledelsens styring og oppfølging • vurdering og håndtering av risiko • måling, evaluering og revisjon • overvåking og hendelseshåndtering • kompetanse- og kulturutvikling Se Difis veiledningsmateriell, jf. ISO/IEC 27001 kap. 4 til kap. 10:					

http://internkontroll.infosikkerhet.difi.no/hjelp.

8. Hvem har det formelle **ansvaret** for å vurdere og håndtere risiko innen informasjonssikkerhet? **76**

Alternativ	**Sett kryss (bare ett kryss)**	
Ledere og mellomledere, som ledd i ordinær linjeledelse	**62**	**kryss for begge=2**
Egen gruppe, fagansvarlig informasjonssikkerhet, eller lignende	**12**	
Forklaring til spørsmål: Dersom det formelle ansvaret for beslutninger om informasjonssikkerhetsrisiko er en del av ledelsesansvaret for de ordinære virksomhetsprosessene, 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.		

9. I hvilken grad har virksomheten vurdert om informasjonssikkerhetshendelser vil kunne føre til utfordringer med virksomhetskontinuitet? **76**

I ingen grad	**I liten grad**	**I moderat grad**	**I stor grad**	**Ikke relevant**	**Vet ikke**
0	**4**	**35**	**37**	**0**	**0**
Forklaring til spørsmål: Spørsmålet handler om sammenhengen mellom arbeidet med informasjonssikkerhet og virksomhetskontinuitet.					

10. I hvilken grad har virksomheten tydelige retningslinjer for å **akseptere** risiko? **75**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	**13**	**34**	**26**	**0**	**1**

Gi gjerne noen eksempler på hva retningslinjene inneholder:

Forklaring til spørsmål:

Tydelige retningslinjer bør ta hensyn til

- hvor viktig oppgaven risikoen er knyttet til 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 har virksomheten en hensiktsmessig organisering av drift og forvaltning av sikkerhetstiltak? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**7**	**43**	**25**	**1**	**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 http://internkontroll.infosikkerhet.difi.no/godt-vite/risikohandtering/fellessikring-og-tilleggssikring

12. Vurderer **risikoeiere** systematisk status på sine ansvarsområder minst en gang i året? **75**

Ja	Nei	Vet ikke
42	**25**	**8**

Forklaring til spørsmål:
En risikoeier er en leder 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 http://internkontroll.infosikkerhet.difi.no/systematiske-aktiviteter/maling-evaluering-og-revisjon#Vurdere status paa eget ansvarsomraade

13. Vurderer de som er ansvarlige for sikkerhetstiltak (tiltaksleverandører) systematisk status på sine ansvarsområder minst en gang i året? **76**

Ja	Nei	Vet ikke
47	**22**	**7**

Forklaring til spørsmål:
Se forklaringen i spørsmål 12.

Se mer på http://internkontroll.infosikkerhet.difi.no/systematiske-aktiviteter/maling-evaluering-og-revisjon#Vurdere status paa eget ansvarsomraade

14. I hvilken grad ser virksomheten styring av informasjonssikkerhet i sammenheng med den øvrige risikostyringen i virksomheten? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	7	30	36	0	2
Gi gjerne eksempler på hvordan risikostyringen sees i sammenheng:					
Forklaring til spørsmål: Øvrig risikostyring er for eksempel HMS, personvern, måloppnåelse og annen virksomhetsstyring.					

15. I hvilken grad har virksomheten et relevant og oppdatert risikobilde på informasjonssikkerhetsområdet? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	5	29	42	0	0

16. I hvilken grad vurderer dere informasjonssikkerhetsrisiko ved oppstart og gjennomføring av utviklings- og anskaffelsesprosjekter? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	5	34	34	2	1

17. I hvilken grad gjennomfører dere regelmessige risikovurderinger for arbeidsoppgavene virksomheten har ansvar for? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	7	46	23	0	0
Forklaring til spørsmål: Risikovurdering handler om å vurdere konsekvens og tilhørende sannsynlighet knyttet til uønskede informasjonssikkerhetshendelser som kan påvirke virksomhetens måloppnåelse.					

18. I hvilken grad er dere i stand til å etablere de sikkerhetstiltak som dere har vurdert at det er behov for? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**0**	**30**	**46**	**0**	**0**

19. Hva skyldes eventuelle forskjeller mellom behov for sikkerhetstiltak og etablerte sikkerhetstiltak? **75**

Svar		Sett kryss (flere kryss er tillatt)
Manglende kompetanse	**19a**	**29**
Økonomiske prioriteringer	**19b**	**37**
Uklare ansvarsforhold	**19c**	**23**
Annet:		
	19d	**tekst=26**

20. Hvilke av de fire sikkerhetstiltakene som er anbefalt av Nasjonal sikkerhetsmyndighet (NSM) har virksomheten innført? **76**

NSMs anbefalte tiltak:		Sett kryss (flere kryss er tillatt)
Oppgrader program- og maskinvare	**20a**	**74**
Installer sikkerhetsoppdateringer så fort som mulig	**20b**	**74**
Ikke tildel sluttbrukere administratorrettigheter	**20c**	**64**
Blokker kjøring av ikke-autoriserte programmer	**20d**	**49**
Ikke relevant	**20e**	**1**
Vet ikke	**20e**	**1**

Forklaring til spørsmål:
For mer informasjon, se https://www.nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/

Vi tar høyde for at virksomheter kan ha enkelte systemer som av ulike grunner må holdes utenfor et eller flere av de over nevnte tiltakene.

21. I hvor stor grad vektlegges følgende faktorer ved beslutninger om iverksettelse eller videreføring av sikkerhetstiltak?

Faktor		Vektlegges ikke	I liten grad	I moderat grad	I stor grad
Kostnader	21a (74)	6	9	30	29
Estimert effekt	21b (75)	2	2	20	51
Negative sideeffekter	21c (75)	2	6	38	29
Annet:					

Forklaring til spørsmål:
Spørsmålet handler om vurderingene som gjøres i forbindelse med beslutninger om å redusere risiko ved etablering av sikkerhetstiltak. Dette gjelder også vurderinger om videreføring av allerede etablerte sikkerhetstiltak.

Med kostnader menes utgifter til iverksettelse og forvaltning av sikkerhetstiltak. Estimert effekt er i hvor stor grad tiltaket er egnet til å endre risiko. Negative sideeffekter er for eksempel at arbeidsoppgaver blir mindre effektive.

22. I hvilken grad gjennomfører virksomheten systematisk godkjenning og iverksetting av sikkerhetstiltak? 76

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	13	31	30	0	2

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.

23. I hvilken grad har virksomheten definert tydelig ansvar for forvaltning og oppfølging av alle sikkerhetstiltak? 76

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	6	28	40	0	1

24. I hvilken grad gjennomfører virksomheten regelmessig evaluering av etablerte sikkerhetstiltak for å finne ut om tiltakene virker etter hensikten og ikke har utilsiktede negative sideeffekter? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
3	**21**	**36**	**14**	**1**	**1**

Del 3 - Beredskap, øvelser og hendelseshåndtering

25. I hvilken grad arbeider virksomheten systematisk med øvelser på informasjonssikkerhetsområdet? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
7	**23**	**31**	**14**	**1**	**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					

26. Hva blir erfaringer fra øvelser i virksomheten benyttet til? **72**

Alternativer		Sett kryss (flere kryss er tillatt)
Forbedre og oppdatere beredskapsplan(er)	**26a**	**60**
Vurdere effekten av- og behovet for sikkerhetstiltak	**26b**	**57**
Forbedre sikkerhetstiltak	**26c**	**63**
Vurdere behovet for kompetansetiltak i virksomheten	**26d**	**44**
Annet:		

27. Gjennomfører virksomheten minst én årlig øvelse på informasjonssikkerhetsområdet? **75**

Ja	**Nei**	**Vet ikke**
34	**40**	**1**
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		

28. Er IKT-beredskapsplanen evaluert og oppdatert i løpet av de siste to år? **75**

Ja	**Nei**	**Vet ikke**
54	**19**	**2**
Forklaring til spørsmål: Med IKT-beredskapsplan mener vi planer for etablering av midlertidige tiltak og håndtering av blant annet informasjonssikkerhetshendelser.		

29. Virksomhetens håndtering av informasjonssikkerhetshendelser er basert på at: **76**

Alternativer:		**Sett kryss (flere kryss er tillatt)**
Vi har definerte roller og ansvar	**29a**	**67**
Vi har en egen funksjon for koordinering av håndtering av informasjonssikkerhetshendelser (eks: Security Incident Response Team)	**29b**	**47**
Vi har oversikt over behov for kompetanse hos alle som er involvert i varsling, deteksjon og håndtering av hendelser	**29c**	**29**
Vi har definerte prosedyrer for håndtering av hendelser	**29d**	**64**
Vi har rapporteringsrutiner ved avvik	**29e**	**71**
Annet:		

30. I hvilken grad benytter virksomheten erfaringene fra hendelseshåndteringen til kontinuerlig forbedring av informasjonssikkerhetsarbeidet? **76**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
1	**5**	**26**	**42**	**2**	**0**
Gi gjerne eksempler på hvordan hendelseshåndteringen brukes til forbedring:					
Forklaring til spørsmål: Eksempler på oppgaver og områder som kan forbedres ved hjelp av resultatet fra hendelseshåndteringen er risikovurderinger, sikkerhetstiltak og kompetanseheving.					

31. I hvilken grad har virksomheten oversikt over kostnadene som følge av informasjonssikkerhetshendelser? **74**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
4	**36**	**21**	**6**	**6**	**1**
Gi gjerne eksempler på hvordan kostnadsberegninger har blitt brukt:					

32. Hvor mange av virksomhetens informasjonssikkerhetshendelser i 2017 ble oppdaget av:

Alternativer:		**Antall:**
Virksomheten selv	**32a**	**<tallet>**
Eksterne partnere/leverandører	**32b**	**<tallet>**
Eksterne, uavhengige parter (for eksempel kunder eller brukere av virksomheten, journalister eller sikkerhetseksperter)	**32c**	**<tallet>**
Ukjent	**32d**	**<tallet>**
		Sett kryss
Vi har ikke systematisk registrering av slik informasjon om hendelser	**32e**	**26**

Del 4 - Nasjonale felleskomponenter

33. Har virksomheten vurdert om den er avhengig av nasjonale felleskomponenter? **76**

Ja	Nei	Vet ikke
68	**7**	**1**

Forklaring til spørsmål:

Virksomheten er avhengig av en felleskomponent hvis måloppnåelsen blir påvirket dersom felleskomponenten ikke er tilgjengelig.

Dette er de nasjonale felleskomponentene og deres forvaltere:

- ID-porten (Difi)
- Altinn (Brønnøysundregistrene)
- Digital postkasse til innbyggere (Difi)
- Kontakt- og reservasjonsregisteret (Difi)
- Det sentrale folkeregisteret (Skatteetaten)
- Enhetsregisteret (Brønnøysundregistrene)
- Matrikkelen (Statens kartverk)

34. Er virksomheten kritisk avhengig av en eller flere nasjonale felleskomponenter? **75**

Ja	Nei	Vet ikke
36	**34**	**5**

Forklaring til spørsmål:
Med «kritisk avhengig» menes det her at det vil oppstå alvorlige konsekvenser ved bortfall av felleskomponenten, slik at virksomheten i vesentlig grad ikke kan levere tjenester eller gjennomføre planlagte arbeidsoppgaver. Dette gjelder også når en kritisk avhengighet er midlertidig.

Hvis ja, har virksomheten etablert reserveløsning ved midlertidig bortfall av nasjonale felleskomponenter?

Ja	Nei	Vet ikke
7	**26**	**3**

35. Hvis virksomheten benytter en eller flere nasjonale felleskomponenter, har dere bedt om følgende informasjon fra en eller flere felleskomponentforvaltere?

Alternativer:	**Sett kryss (flere kryss er tillatt)**
Vet ikke **35a**	**25**
Informasjon som klargjør fordeling av ansvar mellom felleskomponentforvaltere og virksomheten **35b**	**22**
Informasjon om resultat av sårbarhetsvurderinger eller det virksomheten bør vite om disse i sine risikovurderinger **35c**	**17**
Informasjon om varsling og oppfølging av sikkerhetshendelser **35d**	**21**
Annen informasjon til nytte i virksomhetens arbeid med informasjonssikkerhet:	

Del 5 - Kultur og kompetanse

36. I hvilken grad opplever du at informasjonssikkerhetsarbeidet har fokus og prioritet hos ledelsen? **75**

I ingen grad	**I liten grad**	**I moderat grad**	**I stor grad**	**Ikke relevant**	**Vet ikke**
0	**0**	**36**	**39**	**0**	**0**

37. I hvilken grad har virksomheten kartlagt behov for kompetanseheving på informasjonssikkerhetsområdet? **75**

I ingen grad	**I liten grad**	**I moderat grad**	**I stor grad**	**Ikke relevant**	**Vet ikke**
2	**22**	**36**	**13**	**1**	**1**

Forklaring til spørsmål:
Se beskrivelse av sikkerhetskultur og kompetanse- og kulturutvikling i Difis veileder for dette: https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/kompetanse-og-kulturutvikling/hva

38. Har virksomhetsledelsen i løpet av 2017 tatt initiativ til at det blir gjennomført tiltak for å styrke informasjonssikkerhetskulturen i virksomheten for noen av disse gruppene? **73**

For alle ansatte	For grupper av ansatte	For ledergruppen	Ikke gjennomført tiltak	Ikke relevant	Vet ikke
24	4	1	6	0	0
5	5		To kryss		
	6	6			
12		12			
15	15	15	Tre kryss		
56	30	34	Total		
Gi ett eller flere eksempler på tiltak som er gjennomført og virkemidler som er benyttet:					

39. I hvilken grad er kompetansetiltak tilpasset til ulike målgrupper i virksomheten? **74**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	12	38	20	2	2
Forklaring til spørsmål: Eksempler på forskjellige målgrupper er toppledergruppen, ledere, systemforvaltere, nyansatte, alle ansatte, ansatte med spesielle arbeidsoppgaver mv. Se også http://internkontroll.infosikkerhet.difi.no/eksempel/2015/10/malgrupper-og-temaer-opplaering					

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

Tusen takk for ditt bidrag til undersøkelsen!