Undersøkelse om informasjonssikkerhet i Nasjonale felleskomponenter – Spørreskjema *Vedlegg til Difi-notat 2017:4*

ID	Spørsmål	Svar
A Styring og kontroll i virksomheten		
A.1	Hvilke standarder, rammeverk og veiledninger baserer dere styring og kontroll med informasjonssikkerhet i felleskomponentene på?	
A.2	Hvilke roller har ansvaret for å ta beslutninger om risiko (f.eks. akseptere eller behandle risiko, inkludert iverksettelse av sikkerhetstiltak)?	
A.3	Hvordan går dere fram for å følge opp beslutninger om risikohåndtering (inkludert iverksettelse av sikkerhetstiltak)?	
B Sikkerhetsarkitektur		
B.1	Har dere beskrevet en sikkerhetsarkitektur for de nasjonale felleskomponentene?	
B.2	Hva legger dere i begrepet sikkerhetsarkitektur?	
B.3	Benytter dere etablerte rammeverk for sikkerhetsarkitektur? Eventuelt hvilke?	
B.4	Er det rammeverk som dere har vurdert å bruke, men ikke bruker i dag? Eventuelt hvorfor?	

C Anskaffelser og leverandøroppfølging		
C.1	Hvilken sourcingstrategi (valg av intern eller ekstern produksjon av tjenester til organisasjonen) har dere for utvikling og drift av felleskomponentene?	
C.2	Hvis dere har satt ut enkelte av disse tjenestene til eksterne leverandører, hvilke mekanismer benytter dere for å skaffe dere innsikt i styring og kontroll og sikkerhetstiltak hos leverandører (relatert til utvikling og drift av felleskomponentene)?	
C.3	Benytter dere eksterne bekreftelser av tjenesteleverandørers styring og kontroll og/eller sikkerhetstiltak (f.eks. SOC2-rapporter)?	
D Måling		
D.1	Arbeider dere med måling eller «benchmarking» av informasjonssikkerhet? Eventuelt hvordan?	
E Samarbeid mellom felleskomponentforvalterne		
E.1	Hvordan samarbeider felleskomponentforvalterne om informasjonssikkerhet i dag?	
E.2	Hvilke møteplasser og kanaler (for eksempel nettverk, faggrupper, samlinger, sosiale media, nyhetsbrev), hvor informasjonssikkerhet i felleskomponenter er et tema, deltar dere på?	

E.3	Er det møteplasser/kanaler knyttet til informasjonssikkerhet i felleskomponenter som dere kjenner til men ikke deltar på? I så fall hvorfor?	
E.4	Hvilke tema tas opp på disse møteplassene/i disse kanalene?	
E.5	Hvilke virksomheter og roller deltar på disse møteplassene?	
E.6	Samarbeider dere om utforming og koordinering av sikkerhetstiltak på tvers av felleskomponenter og på tvers av felleskomponentforvaltere? I hvilken grad og på hvilken måte gjennomføres slikt samarbeid?	
E.7	Benytter felleskomponentforvalterne en felles referanse for organisering eller kategorisering av sikkerhetstiltak (f.eks. tiltaksbanker/rammeverk som ISO/IEC 27002, NIST SP 800-53 e.l.)?	
E.8	Hvordan vurderer dere nytte og negative sideeffekter ved å ha et felles sett med grunnleggende sikkerhetstiltak for nasjonale felleskomponenter?	
E.9	Samarbeider dere med andre felleskomponentforvaltere om felles tilnærming til måling eller «benchmarking» av informasjonssikkerhet? Hvis ja, hvordan?	

	Hvis nei, hvilken nytte kunne dere eventuelt hatt av det?	
E.10	Samarbeider dere med andre felleskomponentforvaltere om planlegging eller gjennomføring av øvelser tilknyttet informasjonssikkerhetshendelser?	
F Eksterne føringer – Etatsstyring og regelverk		
F.1	Er det føringer, eller mangel på sådanne, fra overordnede departement som påvirker koordinering og samarbeid mellom felleskomponentforvalterne på informasjonssikkerhetsområdet? Hvilke føringer er det eventuelt snakk om?	
F.2	Er det regelverk som påvirker koordinering og samarbeid mellom felleskomponentforvalterne på informasjonssikkerhetsområdet? Hvilket regelverk er det eventuelt snakk om?	
F.3	Noen nasjonale felleskomponenter kan være utpekt som skjermingsverdig objekt iht. sikkerhetsloven, andre ikke. Gir dette spesielle utfordringer eller er det til nytte for koordinering eller samarbeid mellom felleskomponentforvaltere på informasjonssikkerhetsområdet? Hvilke utfordringer eller nytte?	
F.4	Informasjon om enkelte felleskomponenter, inkludert dokumentasjon av sikkerhetstiltak, kan	

	være gradert iht. til sikkerhetsloven. Gir dette spesielle utfordringer eller er det til nytte for koordinering eller samarbeid mellom felleskomponentforvaltere på informasjonssikkerhetsområdet? Hvilke utfordringer eller nytte?	
G Tverrgående utfordringer og løsninger		
G.1	Opplever dere tverrgående utfordringer knyttet til informasjonssikkerhet for forvaltere av nasjonale felleskomponenter?	
G.2	Hva kan gjøres for å bidra til å løse felles problemstillinger og hindringer i informasjonssikkerhetsarbeidet for nasjonale felleskomponenter?	
H Kundene		
H.1	Hvordan tilrettelegger dere for å bidra til at kundene kan vurdere og håndtere risiko knyttet til sin bruk av felleskomponenten[e]?	
H.2	Hvordan tilrettelegger dere for dette før en kunde tar i bruk felleskomponenten, og hvordan tilrettelegger dere for dette for kunder som er brukere av felleskomponenten?	
H.3	Hva er det kundene etterspør i forbindelse med vurdering og håndtering av risiko?	
H.4	Samarbeider felleskomponentforvaltere om risikokommunikasjon, inkl. samkjørt form og innhold, til kundene? Eventuelt hvordan?	

H.5	Stiller dere krav til kundene om vurdering og håndtering av risiko? (Vis gjerne til, eller legg ved, eksempel på slike krav.)	
H.6	Er dere tydelige og klare overfor kundene om ansvarsforhold rundt vurdering og håndtering av risiko ved bruk av felleskomponenten? (Vis gjerne til, eller legg ved, eksempel på slik dokumentasjon.)	
H.7	Gir dere kundene innsikt i informasjonssikkerheten tilknyttet utvikling og drift av felleskomponenten[e]? Eventuelt hvordan?	
I Samfunnsrisiko		
I.1	Det kan argumenteres for at felleskomponentforvaltere i praksis gjør risikovurderinger på samfunnets vegne. Hvordan forholder dere dere til samfunnets grad av avhengighet av en felleskomponent og den konsentrasjon av risiko på ett sted dette kan utgjøre?	
I.2	Arbeider felleskomponentforvaltere med felles forståelse av risiko og kritiske avhengigheter på tvers av virksomheter og sektorer? Eventuelt hvordan?	

J Forbedringsforslag		
J.1	Har dere forslag til hvordan man kan forbedre informasjonssikkerheten i nasjonale felleskomponenter?	
Kontaktpersoner		
	Navn, e-post og telefon til personer som kan kontaktes for et intervju	