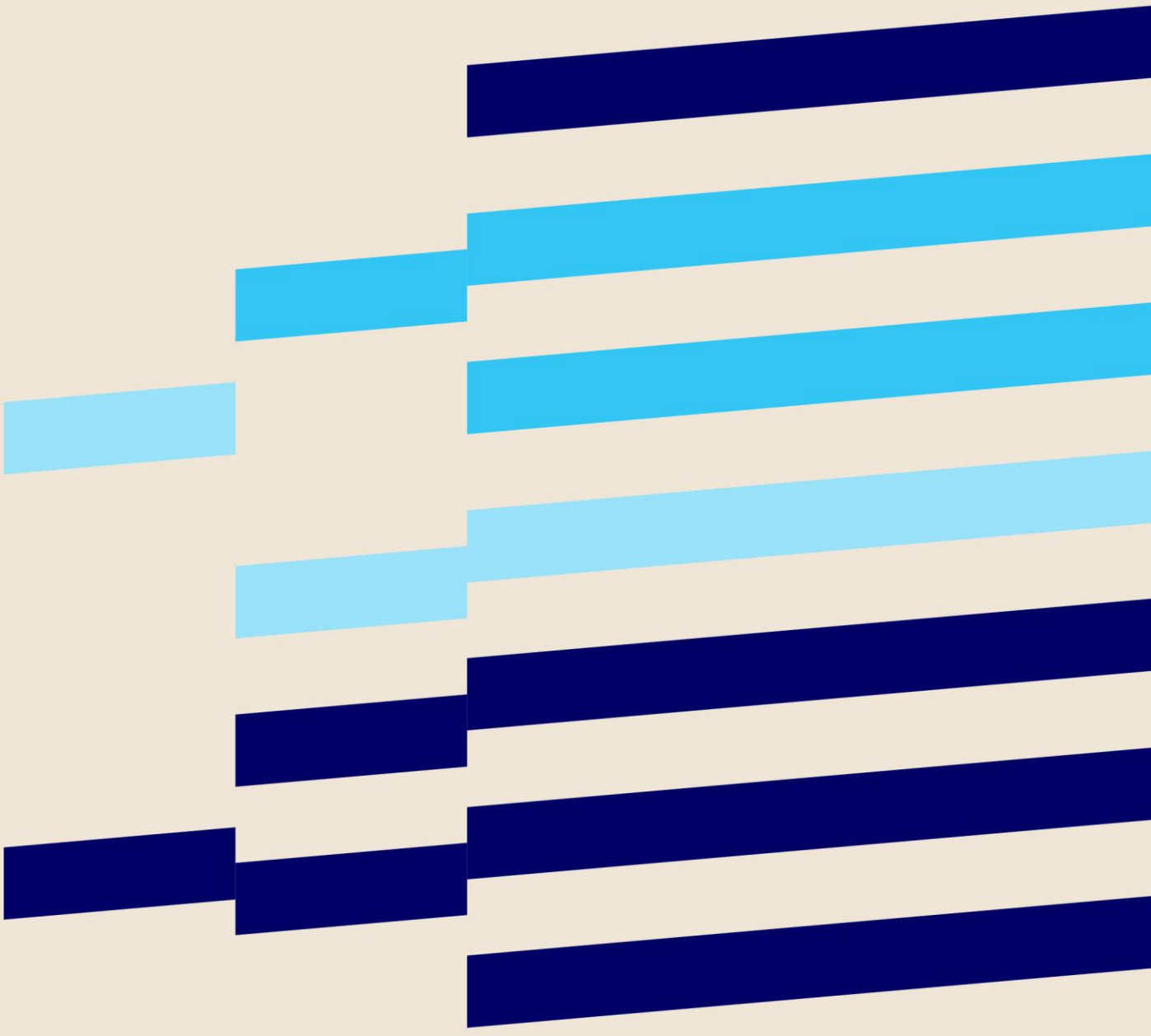
Difi
Direktoratet for forvaltning og ikt

Difi-notat
2017:4
ISSN 1892-1728

Samarbeid og koordinering på informasjonssikkerhetsområdet i nasjonale felleskomponenter

Status og anbefalte tiltak



Forord

Nasjonale felleskomponenter er gjenbrukbare løsninger som dekker typiske behov på digitaliseringsområdet og er en viktig del av den nasjonale digitale infrastrukturen. De eksisterende nasjonale felleskomponentene forvaltes av virksomheter underlagt forskjellige fagdepartementer.

For at innbyggere og forvaltningen skal ha tillit til felleskomponentene er det viktig at de utvikles og forvaltes på en trygg måte. Informasjonssikkerhet er derfor et sentralt tema i utvikling og forvaltning av felleskomponentene.

Dette notatet oppsummerer resultatene fra en kartlegging av status på koordinering, samarbeid og helhetlig tilnærming til informasjonssikkerhet i nasjonale felleskomponenter.

Notatet inneholder også forslag til tiltak der hvor vi har sett at det kan være hensiktsmessig.

Difi har ikke kartlagt hvor god informasjonssikkerheten er i virksomhetene som forvalter nasjonale felleskomponenter.

Difis kompetansemiljø for informasjonssikkerhet er ansvarlig for kartleggingen, med seksjonssjef Øyvind Grinde som leder av arbeidet.

Arbeidet er gjennomført av Remi Longva og Svanhild Gundersen. Katrine Aam Svendsen har bistått med kvalitetssikring av notatet.

Difi takker felleskomponentforvalterne som har deltatt i kartleggingen.

Oslo, 18.12.2017

Grete Orderud

avdelingsdirektør

Innhold

Sammendrag

Difis kompetansemiljø for informasjonssikkerhet gjennomførte i 2017 en kartlegging av status på samarbeid, koordinering og helhetlig tilnærming på informasjonssikkerhetsområdet i utvikling og forvaltning av nasjonale felleskomponenter.

Dette notatet oppsummerer resultatene fra kartleggingen og inneholder forslag til tiltak der hvor vi har sett at det kan være hensiktsmessig.

Nasjonale felleskomponenter[1] er gjenbrukbare løsninger som dekker typiske behov på digitaliseringsområdet og er en viktig del av den nasjonale digitale infrastrukturen. De eksisterende nasjonale felleskomponentene forvaltes av virksomheter underlagt forskjellige fagdepartementer.

Kartleggingen har undersøkt status på flere temaer innen informasjonssikkerhet. I hvilken grad, på hvilken måte, og for hvilke formål pågår det samarbeid, kunnskaps- og erfaringsdeling mellom felleskomponentforvalterne? Hvilke områder har de felles eller koordinert tilnærming til, f.eks. styring og kontroll, utvikling av sikkerhetstiltak og risikoforståelse? Hvordan kommuniserer felleskomponentforvalterne rundt risiko med de som utvikler tjenester som benytter komponentene?

Difi har ikke kartlagt hvor god informasjonssikkerheten er i virksomhetene som forvalter nasjonale felleskomponenter.

Felleskomponentforvalterne samarbeider en god del på flere områder, i ulike grupperinger og også med andre aktører, men kartleggingen viser at det er liten grad av helhetlig koordinering og samarbeid på informasjonssikkerhetsområdet.

Felleskomponentforvalterne er enige om at tettere samarbeid på informasjonssikkerhetsområdet vil være hensiktsmessig.

Det er hovedsakelig ett tiltak alle felleskomponentforvalterne er enige om vil være hensiktsmessig, og det er «faglig møteplass». De fleste andre tiltakene som foreslås i kapittel 0 er det naturlig at felleskomponentforvalterne tar opp til diskusjon og vurdering på den «faglige møteplassen», slik at de sammen kan gå i gang med aktivitetene de anser for å være mest nyttige.

Vi anbefaler at felleskomponentforvalterne prioriterer en diskusjon av følgende tiltak:

- Styring og kontroll
- Informasjon til kunder
- Objektsikkerhet

[1] https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/felleskomponenter/id2342598/

1 Innledning

1.1 Handlingsplan for informasjonssikkerhet i statsforvaltningen

Kartleggingen ble gjennomført i tilknytning til tiltaksområdet *Sikkerhet i Nasjonale felleskomponenter* i Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017[2]. Tiltaksområdet skal bidra til en bedre koordinering av informasjonssikkerheten i de nasjonale felleskomponentene. Det er et mål at virksomhetene som forvalter nasjonale felleskomponenter har en felles risikoforståelse, og dermed også en felles forståelse av kritiske avhengigheter på tvers av virksomheter og sektorer.

Som en del av arbeidet med tiltaksområdet ønsket vi å undersøke status på samarbeid, koordinering og helhetlig tilnærming til informasjonssikkerhet i felleskomponentene – og å få fram forslag til forbedringer. Kunnskap og innsikt fra en slik kartlegging vil gjøre det mulig å vurdere tiltak for å styrke området i samarbeid med felleskomponentforvalterne.

1.2 Difis roller

Difis kompetansemiljø for informasjonssikkerhet er KMDs utøvende organ for informasjonssikkerhet i statsforvaltningen, og er ansvarlig for denne kartleggingen.

Difi er også en felleskomponentforvalter. Kompetansemiljøet for informasjonssikkerhet er uavhengig av avdelingen som forvalter Difis felleskomponenter. Difis avdeling med ansvar for felleskomponenter deltok i kartleggingen på lik linje med de andre felleskomponentforvalterne.

Når vi henviser til Difi som felleskomponentforvalter i notatet så er dette presisert i teksten. Vi benytter «Direktoratet for forvaltning og IKT» når vi henviser til hele Difis virksomhet.

1.3 Gjennomføring av undersøkelsen

Kartlegging av status ble gjennomført i form av en undersøkelse som ble besvart av forvalterne av nasjonale felleskomponenter.

Vi samlet inn informasjon i undersøkelsen i to deler:

- En skriftlig undersøkelse - hvor vi mottok svar i fritekst
- Separate intervjuer med hver enkelt felleskomponentforvalter – hvor vi fikk tilleggsinformasjon og oppklarte eventuelle uklarheter eller misforståelser

[2] https://www.regjeringen.no/no/dokumenter/handlingsplan-for-informasjonssikkerhet-i-statsforvaltningen/id2440093/

Spørsmålene i undersøkelsen var delt inn i forskjellige områder, eller temaer. Resultatene som presenteres i dette notatet er strukturert etter temaer på samme måte, men ikke helt identisk med undersøkelsen.

Ved utsending av undersøkelsen la vi vekt på at det var viktig at ansatte med relevant kompetanse og innsikt besvarte den, for eksempel fagansvarlig for informasjonssikkerhet og systemeiere for felleskomponentene. Felleskomponentforvalterne oppga kontaktinformasjon til kandidater for det oppfølgende intervjuet som et av svarene i den skriftlige undersøkelsen. Representanter fra alle felleskomponentforvaltere besvarte den skriftlige undersøkelsen og deltok på intervju.

Vi sammenstilte svarene fra den skriftlige undersøkelsen og intervjuene og analyserte svarene for hvert område i undersøkelsen. Vi så etter likheter og forskjeller i tilnærmingen hos de forskjellige felleskomponentforvalterne, og samlet forslag til forbedringer.

1.4 Begreper

1.4.1 Nasjonale felleskomponenter

Når vi skriver **felleskomponenter** og **felleskomponentforvaltere** i denne notatet mener vi **nasjonale felleskomponenter** og **forvaltere av nasjonale felleskomponenter** iht. regjeringens definisjon av disse.

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

Tabell 1 Felleskomponenter

1.4.2 Kunder

Når vi skriver **kunder** i dette notatet mener vi virksomhetene som benytter felleskomponentene – offentlige virksomheter som benytter felleskomponentene i sine tjenester. Noen felleskomponentforvaltere kaller dem **tjenesteeiere**.

1.4.3 Styring og kontroll

Vi skriver gjennomgående **styring og kontroll** når vi mener de sentrale aktivitetene som normalt inngår i internkontroll på informasjonssikkerhetsområdet. Vi benytter det synonymt med **styringssystem**, **ledelsessystem** eller **internkontroll**. Jf. ISO 27001[3] kapittel 4-10.

1.4.4 Sikkerhetstiltak

Vi skriver gjennomgående **sikkerhetstiltak**[4] når vi mener de varige tiltakene som iverksettes for å ivareta konfidensialitet, integritet eller tilgjengelighet i informasjonsbehandlingen. Dette er normalt tiltak som velges og iverksettes ved bruk av aktivitetene risikovurdering og risikohåndtering. Det er synonymt med det engelske begrepet **security control**. For eksempler, se innholdet i tiltaksbanker[5] som ISO 27002[6] (eller ISO 27001 Annex A) og NIST SP 800-53 Appendix F.

1.5 Temaer

Vi har valgt å dele opp undersøkelsen i forskjellige temaer i tilknytning til informasjonssikkerhet i nasjonale felleskomponenter.

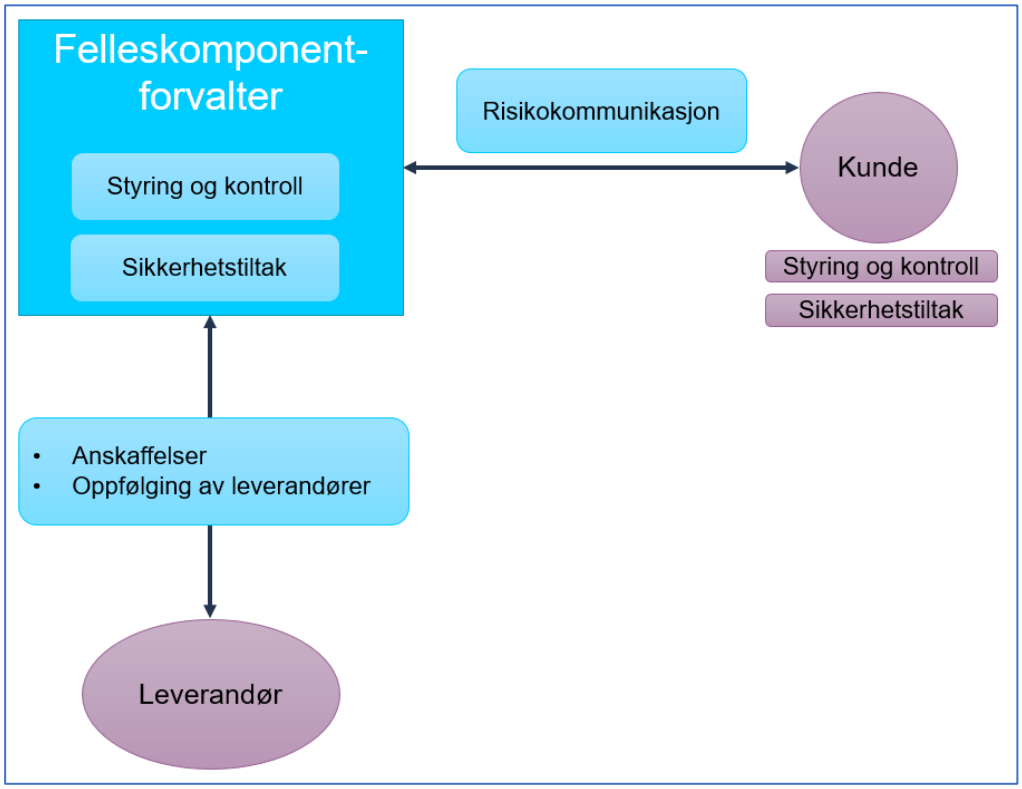
Figur 1 viser hvordan felleskomponentforvalterne og kundene har ansvar for styring og kontroll og sikkerhetstiltak i sine respektive virksomheter. Kundene er avhengig av informasjon om og kommunikasjon rundt informasjonssikkerhet og risiko fra felleskomponentforvalterne for å kunne ivareta sitt ansvar. De fleste felleskomponentforvalterne benytter eksterne leverandører i forbindelse med utvikling og drift av felleskomponentene.

[3] ISO/IEC 27001:2013 (NS-EN ISO/IEC 27001:2017)

[4] http://internkontroll.infosikkerhet.difi.no/godt-vite/risikohandtering/sikkerhetstiltak

[5] Rammeverk med beskrivelser av sikkerhetstiltak
http://internkontroll.infosikkerhet.difi.no/godt-vite/risikohandtering/tiltaksbanker

[6] ISO/IEC 27002:2013 (NS-EN ISO/IEC 27002:2017)



Figur 1 Samhandling felleskomponentforvaltere – kunder - leverandører

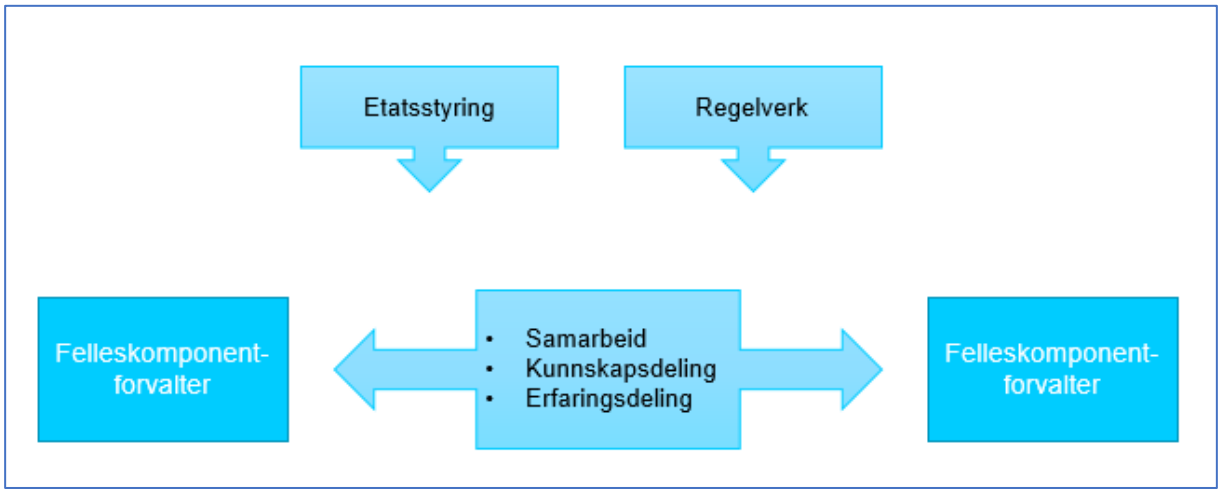
Figur 1 viser konseptuelle sammenhenger. Med utgangspunkt i den har vi identifisert følgende temaer:

Tema	**Beskrivelse**
Styring og kontroll	Styring og kontroll (internkontroll) på informasjonssikkerhetsområdet hos hver enkelt felleskomponentforvalter.
Sikkerhetstiltak	Arbeidet med sikkerhetstiltak hos hver enkelt felleskomponentforvalter.
Kundene	Virksomheter som benytter felleskomponentene i sine løsninger (kundene) skal ha styring og kontroll med informasjonssikkerhet, og har behov for oversikt over sikkerhetstiltak for sine løsninger. For å kunne ivareta sitt ansvar er de avhengige av informasjon fra felleskomponentforvalterne. Dette er aktuelt før de tar i bruk en felleskomponent, og mens de er brukere av en felleskomponent. F.eks. informasjon om sikkerhet i komponenten, vurderinger av risiko, tilstand på sikkerhetstiltak, obs-punkter kundene bør vurdere, tjenestenivå

	og hendelser.
Anskaffelser og oppfølging av leverandører	Hvordan felleskomponentforvalterne arbeider med tjenesteutsetting, inkludert hvordan de styrer og følger opp risiko, og hvordan de skaffer seg innsikt i styring og kontroll og sikkerhetstiltak hos leverandører.

Tabell 2 Temaer fra Figur 1 Samhandling felleskomponentforvaltere – kunder - leverandører

Figur 2 illustrerer at overordnete departementer og regelverk gir føringer for felleskomponentforvalterne, som blant annet påvirker samhandlingen. Den illustrerer også samhandlingen mellom felleskomponentforvalterne.



Figur 2 Samhandling felleskomponentforvaltere

Med utgangspunkt i figur 2 har vi identifisert følgende temaer:

Tema	**Beskrivelse**
Eksterne føringer - etatsstyring og regelverk	Forvaltning av nasjonale felleskomponenter er lagt til flere forskjellige virksomheter, underlagt forskjellige departementer. Forskjeller i føringer fra respektive departement og forskjeller i regelverk, eller anvendelse av regelverk, kan påvirke samhandling mellom felleskomponentforvaltere og tilnærming til arbeidet med informasjonssikkerhet.
Tverrgående utfordringer	Felleskomponentforvalternes oppfatning av hvilke felles, tverrgående utfordringer de har.
Samfunnsrisiko	Felleskomponentforvaltere gjør i praksis

	vurderinger av risiko på samfunnets vegne. Samfunnsfunksjoner er avhengige av felleskomponentene, på tvers av sektorer.
Generelt om samarbeid og møteplasser	En del generelle ting omkring samarbeid som ikke er behandlet under et av de andre temaene.

Tabell 3 Temaer fra Figur 2 Samhandling felleskomponentforvaltere

Med bakgrunn i føringer i handlingsplanen har vi også valgt å se på disse tre temaene:

Tema	**Beskrivelse**
Måling	Måling eller «benchmarking» av informasjonssikkerhet.
Sikkerhetsarkitektur	Beskrivelse og bruk av sikkerhetsarkitektur og bruk av arkitekturrammeverk.
Øvelser	Planlegging og gjennomføring av øvelser for læring, forbedring av sikkerheten og testing av beredskap.

Tabell 4 Temaer fra handlingsplanen

2 Resultater fra undersøkelsen

Resultatene er basert på en skriftlig spørreundersøkelse etterfulgt av muntlige intervjuer.

2.1 Styring og kontroll

2.1.1 Felles utgangspunkt

E-forvaltningsforskriften § 15 stiller krav til styring og kontroll basert på anerkjent standard. Referansekatalogen anbefaler å basere seg på ISO 27001. I tillegg har Direktoratet for forvaltning og IKT veiledningsmateriell som gir grundig og praktisk hjelp til hvordan offentlige virksomheter kan gjøre dette i praksis. Veiledningsmateriellet er også anbefalt i referansekatalogen.

Sikkerhetsloven stiller krav til styring og kontroll, med forskrift for sikkerhetsadministrasjon som er basert på ISO 27001.

Alle virksomhetene sier de baserer seg på ISO 27001 i arbeidet med styring og kontroll med informasjonssikkerhet.

2.1.2 Ansvar for beslutninger om risiko

Flere av felleskomponentforvalterne sier at ansvaret for å ta beslutninger knyttet til vurdering og håndtering av risiko generelt følger linjen. Dvs. at linjeledere som er ansvarlig for mål og resultater også er ansvarlig for styring av risiko, inkludert informasjonssikkerhet. Virksomhetene har sikkerhetsfaglige personer som tilrettelegger, koordinerer og bidrar til å følge opp. Dette ansvaret kan også være knyttet opp mot en «systemeier»-rolle. Hos én av felleskomponentforvalterne er ansvaret knyttet opp mot prosjektgjennomføring, hvor beslutninger er konsensusdrevet, og gjøres i samarbeid med IT-sikkerhetsfaglige personer.

2.1.3 Oppfølging av iverksettelse av sikkerhetstiltak

Når det gjelder å følge opp beslutninger om iverksettelse av sikkerhetstiltak virker det som det er varierende praksis. Virksomhetene har bl.a. policy og retningslinjer for dette, oppfølging i ledermøter og «styringshjul». Ut fra svarene har det vært vanskelig å tolke i hvor stor grad dette er integrert i virksomhetsstyringen for øvrig; f.eks. i prosesser for finansiering og oppfølging av tiltak. Dette er et område hvor det i liten grad utveksles erfaringer.

2.2 Sikkerhetstiltak

2.2.1 Organisering og oppfølging av sikkerhetstiltak

Flere av felleskomponentforvalterne benytter ISO 27002 som tiltaksbank, eller baserer seg på strukturen i ISO 27002 for å sortere og holde oversikt over sikkerhetstiltakene sine. Det pågår ikke samarbeid om å benytte ISO 27002, eller andre tiltaksbanker som felles referanseramme for organisering og kategorisering av sikkerhetstiltak på tvers av virksomhetene.

En av felleskomponentforvalterne har en form for «fellessikring»[7] med tiltak som nye IT-løsninger skal benytte, bl.a. «komponenter for autentisering, autorisasjon og logging» og «godkjente kommunikasjonsmønstre».

Det pågår ikke et systematisk samarbeid om utforming og koordinering av sikkerhetstiltak på tvers av felleskomponenter og felleskomponentforvaltere. Samarbeidet som foregår er stort sett i forbindelse med prosjekter og er relatert til spesifikk integrasjon og samspill mellom tekniske løsninger, for eksempel datautveksling, autentisering og testing.

2.2.2 Felleskomponenter som er sikkerhetstjenester

I et litt større bilde kan felleskomponenter tilby sikkerhetstiltak til tjenester, og andre felleskomponenter, slik ID-porten leverer en autentiseringstjeneste. Hvordan slike sikkerhetstjenester skal utvikles og forvaltes som en del av en nasjonal arkitektur ble også nevnt. Skattedirektoratet ønsker at tilgangskontroll til tjenester løses ved hjelp av en egen felleskomponent, se omtalen av behov for bedre nasjonal oversikt i kapittel 2.6.

2.3 Kundene

2.3.1 Tilrettelegging for kundenes behov

Informasjonssikkerhet er viktig i et digitalisert samfunn, derfor pålegger Digitaliseringsrundskrivet[8] statlige virksomheter som skal ta i bruk felleskomponenter å vurdere risiko knyttet til informasjonssikkerhet. Det er viktig at felleskomponentforvalterne tilrettelegger slik at kundene får nødvendig informasjon for å gjøre dette.

Undersøkelsen viser at felleskomponentforvalterne tilrettelegger for dette på forskjellige måter for den enkelte felleskomponent. En forvalter gir kundene revisjonsinnsyn via samarbeidsavtaler. En annen publiserer sin vurdering av risiko for noen av felleskomponentene sine, arrangerer møteplasser for kunder og leverandører hvor informasjonssikkerhet er tema, og gir råd og veiledning i hvordan kundene kan vurdere risiko. Difi som felleskomponentforvalter publiserer rammeverk, metoder og eksempler på hvordan kundene kan vurdere risiko ved bruk av en av felleskomponentene.

Difi som felleskomponentforvalter stiller krav til risikovurdering hos kundene i bruksvilkår og kan kreve å få se kundenes vurderinger av risiko. Merk at kundekretsen er videre enn de virksomhetene som Digitaliseringsrundskrivet gir føringer til.

[7] Sikkerhetstiltak som inngår i et grunnleggende sikkerhetsnivå i en virksomhet http://internkontroll.infosikkerhet.difi.no/godt-vite/risikohandtering/fellessikring-og-tilleggssikring

[8] https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2569983/

2.3.2 Samkjøring av kommunikasjon

Felleskomponentforvalterne samarbeider ikke om hvordan de kommuniserer rundt risiko til kundene, unntatt en del varsling og oppfølging i forbindelse med hendelser. Virksomheter som benytter felleskomponenter i sine tjenester kan måtte forholde seg til flere forskjellige måter å fremstille slik informasjon på; med ulik detaljeringsgrad, begrepsbruk osv.

2.3.3 Hva kundene ber om

De fleste forvalterne gir kundene den informasjonen de etterspør om informasjonssikkerhet. Dersom kundene spør får de også grundig og detaljert informasjon om sikkerhetsegenskaper ved komponenten.

Eksempler på hva kundene etterspør er:

- Tilgjengelighet (oppetid)
- Datakvalitet
- Bistand til vurdering av risiko
- Sikkerhetsegenskapene til felleskomponenten
- Bruk av sikkerhetsfunksjonalitet, for eksempel hvordan sporing håndteres
- Generelt om informasjonssikkerhet i komponenten
- En form for «godkjenning» fra felleskomponentforvalteren
- Informasjon om hendelseshåndtering

2.3.4 Kundenes ansvar

Fordeling av ansvar mellom forvalter og kunde er hos noen håndtert i bruksavtaler, mens en forvalter henviser til gjeldende regelverk.

Difi som felleskomponentforvalter sier: «vårt inntrykk [..] er at tjenesteeiere ikke har gjort en tilstrekkelig grundig vurdering av hva konsekvensene ved et bortfall av ID-porten vil bety». Dette tyder på at de mener at kundene burde ha et mer bevisst forhold til risiko enn de har i dag. Det kan være mange grunner til at kundene eventuelt mangler tilstrekkelig oppmerksomhet på risiko i sine tjenester, men felleskomponentforvalterne besitter mye kunnskap og kompetanse som de kan benytte for å bidra til å heve nivået, slik at samfunnssikkerheten styrkes.

2.4 Anskaffelser og oppfølging av leverandører

Felleskomponentforvalterne har forskjellige, men avklarte strategier for tjenesteutsetting av arbeid knyttet til felleskomponentene. Dette varierer fra å utføre all utvikling, forvaltning og drift med egne ansatte (som for eksempel Brønnøysundregistrene med Enhetsregisteret), via å sette ut deler av arbeidet (for eksempel driften), til å kjøpe hele produkt i markedet (som for eksempel Difi med Digital postkasse til innbyggere). Alle forvalterne har satt ut en del av arbeidsoppgavene og utfører en del av arbeidsoppgavene internt.

Virksomhetene som har satt ut hele eller deler av arbeidet knyttet til felleskomponentene stiller sikkerhetskrav til leverandørene, som så følges opp i leveransene. Det benyttes også tekniske sikkerhetstester mot løsninger i leverandørers infrastruktur, og sikkerhetsgjennomganger med leverandørene.

En forvalter benytter selvdeklareringsskjemaer for leverandører.

Flere av felleskomponentforvalterne følger opp leverandørers ISO 27001-sertifisering ved å skaffe seg innsyn i rapporter fra sertifiseringsrevisjoner.

Det er ingen av felleskomponentforvalterne som benytter attestasjonstjenester eller rapporter av typen SOC2, ISAE 3402 e.l. for å skaffe seg innsikt i tilstanden på styring og kontroll og sikkerhetstiltak hos leverandører.

2.5 Eksterne føringer - etatsstyring og regelverk

2.5.1 Føringer er ikke til hinder for samarbeid

Noen av de nasjonale felleskomponentene er klassifisert som skjermingsverdige objekter iht. sikkerhetsloven § 17[9], andre ikke. Dette oppfattes ikke som problematisk for et velfungerende samarbeid om informasjonssikkerhet.

Det er en generell oppfatning at det heller ikke er annet regelverk som er til hinder for samarbeid på informasjonssikkerhetsområdet. Men det påpekes at det er regelverk som blir tolket og brukt forskjellig, f.eks. at bruken av personvernregelverket ikke er koordinert.

2.5.2 Objektsikkerhet

Felleskomponentforvalterne peker på arbeid med objektsikkerhet[10] som et område hvor det kan og bør være bedre samarbeid. Noen av virksomhetene forvalter skjermingsverdige objekter i dag, andre er involvert i periodiske vurderinger om behovet for å klassifisere felleskomponenter som skjermingsverdige objekter. De peker på mulighet for samarbeid i gjennomføring av slike vurderinger, og utveksling av erfaring med slike vurderinger. Dette kan typisk være hva som vektlegges i vurderingene, praktisk gjennomføring av vurderingene og kommunikasjon med ansvarlig departement. Det ble også pekt på at objektsikkerhetsforskriften stiller krav til undersøkelse av avhengigheter, noe som kan være egnet for samarbeid og koordinering.

2.5.3 Sektorregelverk

En forvalter nevnte at tverrfaglig samarbeid kan vanskeliggjøres av sektorspesifikt regelverk ved at noen er veldig opptatt av å styre etter sitt

[9] https://lovdata.no/lov/1998-03-20-10

[10] https://lovdata.no/dokument/SF/forskrift/2010-10-22-1362

regelverk. Vi oppfattet dette som en kommentar om et mulig problem med «silotenking» – ikke noe som er til hinder for å utvikle samarbeid.

Kartverket pekte på utfordringer med regelverksutviklingen, hvor det er tilfeller hvor fagmiljøene ikke er tilstrekkelig involvert og informert om utarbeidelse av nytt regelverk.

2.6 Tverrgående utfordringer

Det er mange av temaene i kartleggingen som inneholder tverrgående utfordringer. Her vil vi behandle det som felleskomponentforvalterne har brakt på banen når de har blitt spurt spesifikt om dette i undersøkelsen.

2.6.1 Ulik tolkning av regelverk

Det blir nevnt at rammebetingelser, inkludert lover og forskrifter, tolkes forskjellig, f.eks. ulik anvendelse av objektsikkerhetsforskriften. Se et ønske om mer koordinert oppfølging av regelverk som nevnt i andre avsnitt i 2.5. Forskjellige vurderinger fører til at forskjellige tiltak iverksettes av ulike felleskomponentforvaltere, noe som kan føre til økt kompleksitet for felles kunder og underleverandører. Se også ulik forståelse av risiko som nevnt i 2.7.

Difi som felleskomponentforvalter nevner et konkret eksempel, hvor de sier at håndteringen av spredning av informasjon fra Kontakt- og reservasjonsregisteret er forskjellig fra det Skattedirektoratet opererer med for Folkeregisteret, inkludert bruken av lokale kopier. Kartverket nevner som et annet eksempel håndtering av informasjon om personer med «fortrolig bostedsadresse», hvor tilgang til slik informasjon kan være styrt forskjellig i Folkeregisteret og Matrikkelen.

2.6.2 Unike – men med mange av de samme behovene

Det har blitt nevnt at felleskomponentene er ganske ulike, og har unike behov. For eksempel inneholder Altinn mye data, mens ID-porten er en autentiseringstjeneste. Det er likevel en kjensgjerning at felleskomponentforvalterne har mange felles og generelle problemstillinger som er helt uavhengig av komponentenes type og spesielle egenskaper. De skal også ofte samvirke i et nasjonalt tjenestelandskap og er utsatt for mange av de samme truslene, enten det er snakk om tilsiktede handlinger eller forskjellige typer uhell og uaktsomhet.

2.6.3 Økt behov for samhandling pga. kompleksitet og lange verdikjeder

NOU 2015:13 «Digital sårbarhet – sikkert samfunn» beskriver at dagens digitale tjenester er blitt avhengige av lange og uoversiktlige verdikjeder. Flere av felleskomponentforvalterne opplever dette som en tverrgående utfordring. Brønnøysundregistrene: «Utover dette blir det i stadig større grad krav til samhandling og kompleksitet i løsninger, noe som medfører at det kan være vanskelig […] å ha full oversikt i de svakheter eller sårbarheter som kan ramme

"kjeden" av komponenter som tjenesten består av.» Dette understøtter behovet for godt samarbeid mellom felleskomponentforvalterne.

2.6.4 Behov for bedre nasjonal oversikt

En bedre oversikt over det nasjonale landskapet av digitale tjenester og fellesløsninger ble etterlyst: «Hvilke komponenter skal inngå i en nasjonal arkitektur? Hva skal være prefererte løsninger fremover i tid?» Dette ble nevnt i sammenheng med samarbeid, hvor behovet for koordinert utvikling av felleskomponenter i en nasjonal arkitektur ble berørt. Koordinering kan bidra til å unngå dublerte eller overlappende tjenester, og sikre forutsigbarhet i utviklingen.

2.7 Samfunnsrisiko

I NOU 2015: 13 «Digital sårbarhet – sikkert samfunn» hevdes det at felleskomponentforvalterne i praksis gjør vurderinger av risiko på samfunnets vegne[11].

2.7.1 Tilgjengelighet på tjenester er i fokus

Det foregår ikke et spesifikt samarbeid om samfunnsrisiko, men felleskomponentforvalterne jobber hver for seg med å sikre at felleskomponentene er tilgjengelige. De er gjennomgående bevisst at mange tjenester er avhengige av deres komponent, og jobber internt i egen virksomhet med å sørge for god tilgjengelighet. Noen tar det med i egne vurderinger av risiko, noen bygger redundans i tekniske løsninger og personellplaner, og samfunnsaspektet kan være en del av rapporteringen til overordnet departement.

Ettersom mange tjenester er avhengige av felleskomponenten er det også forvaltere som legger vekt på god endringsstyring, inkludert tidlig varsling av endringer til kundene.

Samfunnets avhengighet av felleskomponenten tas med i vurderingene av om komponenten skal være skjermingsverdig objekt. En av felleskomponentforvalterne peker også på at de må holde orden på hva deres komponent er avhengig av fordi den er et skjermingsverdig objekt.

2.7.2 Felles forståelse av risiko

Felleskomponentforvalterne jobber ikke sammen om felles forståelse av risiko og avhengigheter på tvers av virksomheter og sektorer. Noen ser at det kan være behov for dette. Noen av dem gir uttrykk for at det er forskjellig oppfatning av og vurdering av risiko, samt at det gjøres ulike vurderinger av hvor kritiske komponentene er. Se 2.5 om samarbeid om objektsikkerhet.

[11] 22.5.2 «Utvalget merker seg at etatene i praksis gjør risikovurderinger på samfunnets vegne.»

2.8 Samarbeid og møteplasser

En god del av det eksisterende samarbeidet i dag er knyttet til spesifikke prosjekter på mer teknisk nivå, fra sak til sak, f.eks. større endringer knyttet til skattemeldingen (tidligere selvangivelsen) eller nettverksforbindelser for sikker utveksling av data.

Felleskomponentforvalterne har som oftest samarbeidsforum og møteplasser tilknyttet komponentene, og de møtes på hverandres forum og møteplasser, hvor informasjonssikkerhet kan være et tema. Alle er deltakere på Direktoratet for forvaltning og IKTs nettverk for informasjonssikkerhet (NIFS), og alle felleskomponentforvalterne deltar i arbeid i regi av Skate. Ingen av disse møteplassene har informasjonssikkerhet i felleskomponenter som primæroppgave.

Felleskomponentforvalterne stiller seg positive til å samarbeide tettere om informasjonssikkerhet, og ser opprettelsen av en faglig møteplass som et naturlig sted å starte.

2.9 Måling

Felleskomponentforvalterne driver i varierende - men liten - grad med måling eller «benchmarking» av informasjonssikkerhet.

Skattedirektoratet benytter ISF Benchmark fra Information Security Forum jevnlig, og også Gartner benchmark. ISF Benchmark brukes til å måle utviklingen fra år til år, samt å måle seg mot sektor, mot virksomheter i EMEA-området og globalt. Dette gir grunnlag for vurdering av sikkerhetstiltak. Analyser av målingene blir også rapportert til virksomhetens ledelse.

Difi som felleskomponentforvalter benytter en form for modenhetsmåling med en tilpasset variant av en Gartner-skala.

Det nevnes også eksempler som tilgjengelighetsmålinger på systemer og tall fra systemer for håndtering av feil og avvik, men det foregår lite strukturert måling av informasjonssikkerhet – hverken av aktiviteter for styring og kontroll eller sikkerhetstiltak.

Felleskomponentforvalterne samarbeider i dag ikke om måling eller benchmarking av informasjonssikkerhet. Flere sier at dette kan være nyttig for å se hvor de er i forhold til de andre felleskomponentforvalterne og for å lære av hverandre. Bedre samhandling og felles forståelse er nevnt som mulig gevinst.

2.10 Sikkerhetsarkitektur

Felleskomponentforvalterne ser på sikkerhetsarkitektur som *et sett av komponenter, løsninger og prosesser som bidrar til sikkerhet*.

Bruken av sikkerhetsarkitektur varierer mellom felleskomponentforvalterne, men også internt hos felleskomponentforvalterne.

Eksempelvis har Brønnøysundregistrene definert en sikkerhetsarkitektur for Altinn som en del av de generelle arkitekturdokumentene. Sikkerhetsarkitekturen følger «beste praksis» på utviklingstidspunktet og oppdateres når endringer påvirker sikkerhetskonseptet. De ser på muligheten for å beskrive sikkerhetsarkitektur for Enhetsregisteret med nye rammeverk ved videreutvikling av plattform.

Difi som felleskomponentforvalter har publisert sikkerhetsarkitekturen for Digital postkasse til innbyggere på Github[12].

Flere felleskomponentforvaltere ser på muligheten for å benytte SABSA[13] i kombinasjon med TOGAF[14] i videre arbeid med sikkerhetsarkitektur.

2.11 Øvelser

Alle felleskomponentforvalterne har gjennomført øvelser sammen med andre virksomheter. Det finnes flere eksempler på øvelser hvor flere felleskomponentforvaltere har deltatt eller hvor to felleskomponentforvaltere øver sammen. Kartverket har arrangert øvelser i «Norge digitalt»[15]-samarbeidet.

Det er ikke formelt samarbeid om planlegging og gjennomføring av øvelser mellom felleskomponentforvalterne i dag.

2.11.1 Håndtering av hendelser på tvers av aktører

Skattedirektoratet trekker fram hendelseshåndtering på tvers av offentlige aktører som et område med potensial for mer samarbeid, men ikke nødvendigvis begrenset til forvaltere av nasjonale felleskomponenter. De påpeker også hvor viktig det er med enda bedre kommunikasjon «når det brenner». De deltar i NorCERT VDI[16]-samarbeidet, men anser ikke dette for å være tilstrekkelig for dagens behov.

I denne forbindelse er det verdt å nevne at Nasjonal sikkerhetsmyndighet (NSM) har et pågående arbeid med «Rammeverk for digital hendelseshåndtering».

Det vil være fornuftig for felleskomponentforvalterne å utforske mulighetene for mer samarbeid og deling av erfaringer på disse områdene. De kan også se på

---

[12] https://github.com/difi/begrep-SikkerDigitalPost/blob/master/innledning/Sikkerhetsarkitektur.pdf

[13] Rammeverk for sikkerhetsarkitektur http://www.sabsa.org/

[14] Rammeverk for virksomhetsarkitektur http://www.opengroup.org/subjectareas/enterprise/togaf

[15] Norge digitalt https://www.geonorge.no/Geodataarbeid/geografisk-infrastruktur/Norge-digitalt/

[16] Varslingssystem for digital infrastruktur https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/

hvordan de i fellesskap kan jobbe sammen med andre aktører. Se kapittel 2.13 om drøfting av nasjonale felleskomponenter som basis for samarbeid.

2.12 Forslag fra felleskomponentforvalterne

2.12.1 Faglig møteplass

Flere av felleskomponentforvalterne nevner at et godt sted å starte er å møtes periodisk, med informasjonssikkerhet som det primære tema. Møtene bør ha en planlagt og forberedt agenda, slik at det blir mest mulig effektivt. Målet bør være å knytte gode kontakter og få diskutert temaer og problemstillinger fritt og åpent.

Det ble også nevnt aktuelle temaer som kan tas opp på en slik møteplass:

- Generell utveksling av erfaringer med informasjonssikkerhetsarbeid
- Vurdering og håndtering av risiko
- Kunnskap om og forståelse av trusselbildet
- Applikasjonssikkerhet
- Problemstillinger knyttet til sammenstilling av datasett fra flere etater
- Objektsikkerhet
- Anskaffelser og leverandøroppfølging, inkludert skytjenester
- Hendelseshåndtering
- Fokuset nasjonalt har vært tilgjengelighet. Integritet og andre temaer har vært mindre belyst

2.12.2 Samordning og standardisering

Flere peker på at felleskomponentene er ulike og har unike behov. Likevel tar flere til orde for større grad av samordning eller standardisering av informasjonssikkerhetsarbeidet.

Eksempler:

- Å gå lenger i å standardisere på krav og felles vurdering av risiko
- Besluttede felles standarder for informasjonssikkerhet
- Felles trusselvurdering, ikke for hver enkelt felleskomponent
- Standardisering på hvordan man rapporterer om risiko og arbeidet med informasjonssikkerhet og sikkerhetstilstanden til overordnet departement

Noen av felleskomponentforvaltere peker på at de i hovedsak møter det samme trusselbildet, og har behov for en mer samordnet vurdering av risiko.

2.13 Om nasjonale felleskomponenter

En av felleskomponentforvalterne reiste tvil om *nasjonale felleskomponenter* er en god logisk mengde å organisere arbeid og samarbeid rundt. Vi fulgte derfor dette opp, og spurte alle om dette temaet.

Flere av felleskomponentforvalterne samarbeider mye og godt med andre aktører, som NAV og politiet. Kartverket har «Norge digitalt»-samarbeidet. Difi som felleskomponentforvalter ser *fellesløsninger* i en større sammenheng, og

behandler stort sett de *nasjonale felleskomponentene* som sine andre fellesløsninger. Samarbeid er ofte konsentrert rundt de virksomhetene felleskomponentforvalteren har tette tekniske integrasjoner med.

Vi mener at mange av områdene det vil være naturlig å samarbeide om ikke er spesielle for forvaltere av nasjonale felleskomponenter, slik de er definert i dag. Dette ble også nevnt i minst ett av intervjuene. Velfungerende aktiviteter for styring og kontroll, slik som ledelsens styring og oppfølging og vurdering og håndtering av risiko, god organisering og oppfølging av sikkerhetstiltak, oppfølging av leverandører mv. er noe alle må forholde seg til.

Det felleskomponentforvalterne har til felles er at de er forvaltere av kritisk digital infrastruktur og kritiske digitale tjenester, men dette har de til felles med mange andre aktører – inkludert aktører i det private næringsliv.

Noe annet de har til felles er at mange virksomheter må forholde seg til dem som leverandører av komponenter og tjenester inn i digitale tjenester. Informasjon, risikokommunikasjon, kontraktsvilkår, rolleforståelse og ansvarsavgrensning mv. tilpasset kundenes behov kan samordnes og koordineres. Kundene får da en enhetlig måte å forholde seg til felleskomponenter på, og slipper å forholde seg til kompleksiteten med flere forskjellige regimer.

Vi tror det kan være fornuftig å se utover nasjonale felleskomponenter, og se flere aktører og fellesløsninger i sammenheng i en nasjonal arkitektur, når man vurderer behovet for samarbeid og koordinering av informasjonssikkerhetsarbeidet.

3 Forslag til tiltak

På bakgrunn av resultatene fra undersøkelsen og forslag fra felleskomponentforvalterne skisserer vi her noen mulige tiltak for å få større grad av kunnskapsdeling og erfaringsutveksling mellom felleskomponentforvalterne, og tettere koordinering av informasjonssikkerhet i nasjonale felleskomponenter.

Det er hovedsakelig ett tiltak alle er enige om at vil være fornuftig, og det er «faglig møteplass». Mange av de andre tiltakene er det naturlig å ta opp til diskusjon på den «faglige møteplassen», slik at felleskomponentforvalterne sammen kan gå i gang med aktivitetene de anser for å være mest hensiktsmessige.

Vi anbefaler at felleskomponentforvalterne prioriterer følgende tiltak:

- Styring og kontroll
- Informasjon til kunder
- Objektsikkerhet

Bakgrunnen for prioriteringen er at god ledelse og systematiske aktiviteter for styring og kontroll er fundamentet for alt sikkerhetsarbeidet i virksomhetene. Mer helhetlig tilnærming til informasjon til kundene er et lite ressurskrevende tiltak, som hurtig kan gi positive effekter. Objektsikkerhet har vært nevnt som en utfordring av de fleste felleskomponentforvalterne.

3.1 Faglig møteplass

Vi anbefaler at felleskomponentforvalterne samarbeider systematisk i et faglig nettverk om informasjonssikkerhet. Formålet bør være å få samordnet og tilstrekkelig styring og kontroll på informasjonssikkerheten i nasjonale felleskomponenter. De bør dele kunnskap og erfaringer og koordinere initiativ.

Møter bør ha en planlagt og forberedt agenda, slik at samarbeidet blir effektivt. Målet bør være å få diskutert temaer og problemstillinger man er opptatt av, men også å knytte gode kontakter.

Det bør være minst én fast deltaker fra hver virksomhet, for å sikre kontinuitet og oppfølging. For øvrig kan deltakelse variere fra gang til gang, alt etter hvilke temaer som tas opp.

Det faglige arbeidet bør koordineres med andre instanser dersom det er behov for det.

3.2 Styring og kontroll

Alle felleskomponentforvalterne har behov for gode, systematiske aktiviteter for styring og kontroll med informasjonssikkerhet. De forvalter viktige nasjonale løsninger hvor svikt i informasjonssikkerhet kan få alvorlige konsekvenser, og skal også følge de samme føringene om god styring og kontroll basert på anerkjente standarder.

Vi anbefaler at de samarbeider om felles tilnærming til aktiviteter for styring og kontroll, basert på Direktoratet for forvaltning og IKTs veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet». Denne gir praktisk veiledning til aktiviteter basert på ISO 27001, og er anbefalt å bruke som støtte i dette arbeidet.

De bør legge vekt på å dele kunnskap og erfaringer på området.

Ettersom alle felleskomponentforvalterne allerede baserer arbeidet sitt på ISO 27001 burde alt ligge til rette for god samordning på dette området. Erfaringsutveksling og tettere koordinering kan oppnås ved hjelp av tiltak 3.1 Faglig møteplass.

3.3 Sikkerhetstiltak

Vi anbefaler at felleskomponentforvalterne samarbeider om utforming, organisering og oppfølging av sikkerhetstiltak.

De bør vurdere å bruke en felles referanseramme for sikkerhetstiltak for felleskomponenter og sentrale tjenester, f.eks. en anerkjent tiltaksbank.

Etter at vi gjennomførte denne undersøkelsen har NSM publisert første utgave av «Grunnprinsipper for IKT-sikkerhet»[17]. Dette er en tiltaksbank med grunnleggende sikkerhetstiltak, med hovedvekt på IKT-nære tiltak. Tiltakene er i hovedsak inspirert av og hentet fra ISO 27002, men er strukturert mer i tråd med NIST Cybersecurity Framework[18]. Det er frivillig å bruke disse grunnprinsippene. Felleskomponentforvalterne bør ta denne tiltaksbanken med i vurderingen av felles referanseramme – men være klar over at den ikke dekker alle tiltaksområder.

3.4 Informasjon til kunder

Vi anbefaler at felleskomponentforvalterne innleder et samarbeid om hvordan de tilbyr informasjon relatert til informasjonssikkerhet til kundene. De bør samordne informasjonen slik at kundene kan ivareta sitt ansvar og ha tilstrekkelig styring og kontroll på informasjonssikkerheten i sine tjenester.

Informasjonen bør inkludere

- klargjøring av ansvar mellom felleskomponentforvaltere og kunder
- resultat av sårbarhetsvurderinger eller det kundene bør få vite om disse for å vurdere risiko i egne tjenester
- hvordan oppnå god sikkerhet ved bruk av felleskomponenten
- varsling om og oppfølging av sikkerhetshendelser

[17] https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

[18] https://www.nist.gov/cyberframework

3.5 Måling

Måling er viktig for å se om innførte sikkerhetstiltak fungerer og for å følge opp aktiviteter for styring og kontroll. Vi anbefaler at felleskomponentforvalterne innleder samarbeid om måling av informasjonssikkerhet. Det kan være nyttig å samarbeide om valg av måleindikatorer, samt hvordan data fra disse indikatorene skal analyseres, tolkes og presenteres.

En felles tilnærming til måling av informasjonssikkerhet vil gjøre det enklere for felleskomponentforvalterne å utveksle erfaringer og lære av hverandre.

3.6 Sikkerhetsarkitektur

Da flere av felleskomponentforvalterne vurderer å ta i bruk SABSA i utvikling av sikkerhetsarkitektur, vil det være naturlig å samarbeide og dele erfaringer om dette. Det kan gjerne være SABSA i kombinasjon med TOGAF, siden flere av felleskomponentforvalterne ser på muligheten for å benytte dette i sitt videre arbeid med sikkerhetsarkitektur.

3.7 Øvelser

Vi anbefaler at felleskomponentforvalterne drøfter mulighetene for økt samarbeid om øvelser. De kan samarbeide om planlegging og gjennomføring, samt hvordan de drar nytte av erfaringer fra øvelser. Samarbeidet kan gjerne omfatte andre aktører, dette har vi drøftet i kapittel 2.13 Om nasjonale felleskomponenter.

3.8 Hendelseshåndtering

Felleskomponentforvalterne bør samarbeide om hvordan de håndterer hendelser. NSMs pågående arbeid med «Rammeverk for digital hendelseshåndtering» vil være relevant for dette arbeidet.

3.9 Objektsikkerhet

Felleskomponentforvaltere bør samarbeide og dele erfaringer om vurderinger knyttet til utvelgelse og klassifisering av komponenter som skjermingsverdige objekter iht. forskrift om objektsikkerhet §2, samt beskyttelse av objektene og oppfølging av arbeidet med objektsikkerhet. De bør vurdere hvordan dette kan organiseres og prøves ut.

En samordnet dialog med NSM kan også effektivisere og styrke slikt arbeid.

3.10 Samordning av føringer

Felleskomponentforvalterne bør få føringer som legger til rette for samarbeid, koordinering og felles innsats på informasjonssikkerhetsområdet. Vi anbefaler at felleskomponentforvalterne tar opp samordning av føringer med sine departementer.

Slike initiativer kan koordineres via Skate.

3.11 Rapportering

Virksomheter rapporterer til overordnet departement om risiko, inkludert status på informasjonssikkerhetsområdet. En standardisert måte å rapportere på vil bedre evnen til å holde helhetlig oversikt på dette området.

En slik standardisering vil også bidra til å styrke virksomhetsledelsens oppmerksomhet om informasjonssikkerhetsarbeidet, og gjøre det lettere å samarbeide om å få til god rapportering.

Vi anbefaler at felleskomponentforvalterne tar opp rapportering med sine departementer, for å vurdere muligheten for samordning av innholdet i rapporteringen på området.

Direktoratet for forvaltning og IKT kan ved behov bidra med koordinering av slike initiativer.

3.12 Samordning – nasjonal arkitektur

I forbindelse med spørsmålene om tverrgående utfordringer og om nasjonale felleskomponenter (behandlet i kapitlene 2.6 og 2.13) nevnte felleskomponentforvalterne en del synspunkter og behov.

- Oversikt over det nasjonale landskapet av fellesløsninger og tjenester
- Forutsigbarhet i utviklingen
- Hvilke komponenter skal inngå i nasjonal arkitektur?
- Hvilke løsninger skal være prefererte fremover i tid?
- Unngå overlappende tjenester
- Sørge for at forvaltere av felleskomponenter og -løsninger møter kundene på en helhetlig måte (informasjon om sikkerhet i løsningene, risikokommunikasjon, ansvarsavgrensning, kontraktsvilkår, utforming og dokumentasjon av tekniske grensesnitt (API-er) mv.)

Vi anbefaler at disse behovene ivaretas i forbindelse med Direktoratet for forvaltning og IKTs pågående arbeid med tiltak knyttet til den tverrgående digitaliseringsstrategien[19], blant annet arbeidet med «Felles kjøreregler».

[19] Digitaliseringsstrategi i offentlig sektor https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/digitaliseringsstrategi

4 Deltakere på intervjuer

Brønnøysundregistrene

- Kristine Aasen, seksjonsleder, Forvaltning og Tjenesterealisering Altinn
- Arnt Kristiansen, underdirektør, Enhetsregisteret
- Christian Tesli, konsulent

Difi

- Arild Bjørk, seniorrådgiver, Drift og sikkerhet
- Tommy Harjo, seksjonssjef, Drift og sikkerhet

Kartverket

- Pål Arnesen, IT-sjef, drift
- Lars Elsrud, leder av matrikkelen
- Per Christian Haraldsen, stedfortreder for sikkerhetsansvarlig i Kartverket
- Knut Sælid, IT-sjef, utvikling

Skattedirektoratet

- Åsmund Sand, sikkerhetsarkitekt
- Kristoffer Stav, senioringeniør Sikkerhet

5 Referanseark for Difi

Tittel på notat:	Samarbeid og koordinering på informasjonssikkerhetsområdet i nasjonale felleskomponenter
Difis notatnummer:	2017:4
Forfatter(e):	Svanhild Gundersen og Remi Longva
Evt. eksterne samarbeidspartnere:	
Saksnummer:	17/00733-14
Prosjektnummer:	17-6
Prosjektnavn:	Sikkerhet i digitale tjenester
Prosjektleder:	Svanhild Gundersen
Prosjektansvarlig avdeling:	Avdeling for Digital Transformasjon
Oppdragsgiver(e):	Direktoratet for forvaltning og IKT
Resymé/omtale: Dette notatet oppsummerer resultatene fra en kartlegging av status på samarbeid, koordinering og helhetlig tilnærming på informasjonssikkerhetsområdet i utvikling og forvaltning av nasjonale felleskomponenter. Notatet inneholder også forslag til tiltak der hvor vi har sett at det kan være hensiktsmessig. Felleskomponentforvalterne samarbeider en god del på flere områder, i ulike grupperinger og også med andre aktører, men kartleggingen viser at det er liten grad av helhetlig koordinering og samarbeid på informasjonssikkerhetsområdet. Felleskomponentforvalterne er enige om at tettere samarbeid på informasjonssikkerhetsområdet vil være hensiktsmessig. Ett tiltak alle felleskomponentforvalterne er enige om er å ha en faglig møteplass hvor det primære temaet er informasjonssikkerhet.	
Emneord: Informasjonssikkerhet, felleskomponenter, felleskomponentforvalter	
Totalt antall sider til trykking:	
Dato for utgivelse:	18.12.2017
Utgiver:	**Difi** Postboks 8115 Dep 0032 OSLO www.difi.no