Digdir

Felles sikkerhet i forvaltningen

Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning

Forord

Dette notatet er utarbeidet av Digitaliseringsdirektoratet (Digdir) for å se på hva som bør gjøres de neste årene i arbeidet for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning. Notatet gir oversikt over utfordringer, anbefaler strategisk retning for de neste årene, og peker på mulige tiltak for forvaltningen.

Digdirs anbefaling

Digitaliseringsdirektoratet anbefaler at det startes et arbeid for å utvikle felles sikkerhet i forvaltningen, inkludert en felles referanseramme (eller norm) for arbeidet med informasjonssikkerhet i offentlige virksomheter. Det bør gjøres i samarbeid mellom ulike aktører, inkludert de sentrale myndighetsorganene som veileder virksomhetene om informasjonssikkerhet og styring og kontroll. Virksomheter på ulike forvaltningsnivåer bør være involvert.

Dersom tiltakene som beskrives skal ha full effekt, bør det tas sikte på at det etter hvert skal dekke hele forvaltningen. Under utvikling og utprøving vil det likevel være fornuftig å fokusere på behovene til virksomheter med lav modenhet og lite ressurser til arbeidet med informasjonssikkerhet. Kommunene har likeartede oppgaver og tjenester, og det vil bli viktig å ivareta deres behov.

Konsepter og mulige tiltak

Det faglige innholdet er utarbeidet av statens kompetansemiljø for informasjonssikkerhet i Digdir.

Vi gjør oppmerksom på at notatet er skrevet for å danne utgangspunkt for videre arbeid. Det beskriver foreløpige vurderinger og konsepter som ikke er klare til å iverksettes i forvaltningen, men som bør videreutvikles i samarbeid.

Respons på initiativet

Sommer og høst 2022 ble versjon 0.9 av dette notatet sendt til sentrale aktører og departementene for å innhente synspunkter på initiativet.

Tilbakemeldingene er positive. Det er stor enighet om utfordringsbildet, og at noe bør gjøres for å få et informasjonssikkerhetsløft i forvaltningen, inkludert digital sikkerhet. Mange ser nytten med å få på plass en felles referanseramme med anbefalinger, og at veiledningstilbudet bør bli enda mer samordnet og helhetlig. Det er også stor grad av enighet om at bredt samarbeid vil være helt nødvendig for å lykkes med dette.

Dette notatet beskriver muligheter for å samkjøre anbefalinger og veiledning om informasjonssikkerhet og personvern. KS og Datatilsynet er spesielt tydelige på at dette bør samkjøres, og peker på nytten det kan gi for virksomhetene. I NOU 2022: 11 kom det fram at personvernkommisjonen også anbefaler slik samkjøring[1].

[1] NOU 2022: 11 Ditt personvern – vårt felles ansvar s. 83 og 227.

En sak om tilstand på fagområdet og initiativet om felles sikkerhet i forvaltningen ble behandlet av det strategiske samarbeidsrådet Skate i møte 23. mars 2022. Saksnummer er 2/22. Referat fra møtet er tilgjengelig på Skates nettsider[2].

I et orienteringsmøte for virksomheter i forvaltningen ble det gitt uttrykk for at beskrivelsen av utfordringsbildet er basert på en god forståelse av utfordringene kommuner og andre møter, og at dette fokuset har vært savnet. Det ble også gitt uttrykk for at det er bra at det blir satt søkelys på kompleksiteten i dette.

Leseveiledning

Del 1 er en innledning som beskriver formål og målsetninger. Den setter innholdet i notatet inn i en større sammenheng og forklarer avgrensningen som er gjort.

Del 2 beskriver utfordringer, og del 3 beskriver mulige tiltak og anbefalinger om hvordan vi kan gå fram for å løse utfordringene.

Det er en fordel om du har grunnleggende forståelse for hvordan fagområdet informasjonssikkerhet henger sammen med oppgaveløsningen i offentlig forvaltning. Begreper og konsepter som benyttes i resten av notatet er beskrevet i vedlegg. I vedleggene kan du også lese mer om sammenheng med personvern, digitale tjenester i felles økosystem, offentlige anskaffelser og skytjenester. Vi anbefaler alle som ønsker fullt faglig utbytte å lese vedleggene.

Dersom du ønsker en oversikt over innholdet kan du hoppe direkte til sammendraget som ligger i vedlegg. Du vil også ha glede av å lese innledningen i del 1.

Leveranseområdeansvarlig Informasjonssikkerhet

Kjetil Korslien

Oslo, 06.12.2022

[2] https://www.digdir.no/skate/skate-mote-23-mars-2022-referat/3451

1 Del 1 – Innledning 2

2 Del 2 – Utfordringsbildet 7
2.1 Problembeskrivelser 7

3 Del 3 – Tiltak og anbefalinger 17
3.1 Et nasjonalt løft for informasjonssikkerhet 17
3.2 Føringer for nye tiltak i forvaltningen 17
3.3 Mulige tiltak 17
3.4 Anbefalinger 24
3.5 Mulige gevinster 27
3.6 Vurdering av effekt 28
3.7 Økonomiske og administrative konsekvenser 30

4 Vedlegg 31
4.1 Vedlegg 1 – Viktige sammenhenger 31
4.2 Vedlegg 2 – Begreper og konsepter 36
4.3 Vedlegg 3 – Krav, anbefalinger og veiledning 45
4.4 Vedlegg 4 – Trusler og farer 46
4.5 Vedlegg 5 – Nasjonale strategier 47
4.6 Vedlegg 6 – Sammendrag 49
4.7 Vedlegg 7 – Figurer 55
4.8 Vedlegg 8 – Kilder 55

1 Del 1 – Innledning

Bakgrunn og formål

De langsiktige målsetningene som ligger til grunn for initiativet er en styrket og mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning, herunder:

- Alle virksomheter i forvaltningen har velfungerende styring og kontroll av informasjonssikkerhet.
- Virksomhetene i offentlig forvaltning har gode rammebetingelser for arbeidet med informasjonssikkerhet, inkludert digital sikkerhet. Dette inkluderer et helhetlig og brukerorientert veiledningstilbud.

Initiativet understøtter målsetninger i nasjonale strategier. Sammenhengen med disse er beskrevet i vedlegg.

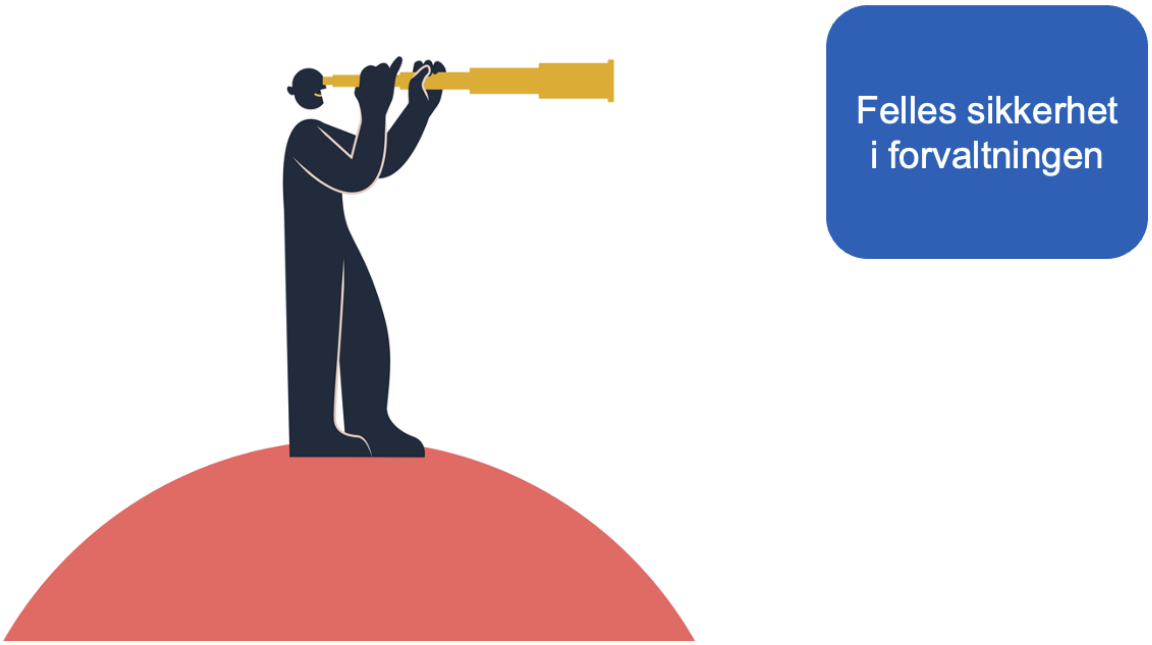
Digdir ønsker å skape forståelse for utfordringene og interesse for et tverrsektorielt samarbeid for å få en helhetlig, felles retning på arbeidet med informasjonssikkerhet i offentlig forvaltning.

I dette notatet beskriver vi utfordringene virksomhetene har med å få god styring på området. Vi peker på konsepter og løsninger som kan utvikles for å gi virksomhetene bedre forutsetninger for å lykkes, og legge til rette for

- effektivt arbeid med informasjonssikkerhet
- samstyring i sammenhengende tjenestekjeder
- god sikkerhet på tvers av hele forvaltningen

Dersom en felles retning på arbeidet med informasjonssikkerhet skal realiseres vil det kreve at relevante fagmyndigheter legger til grunn den samme tilnærmingen, og benytter den som utgangspunkt for sine ulike veiledningsansvar.

Resultatet vil være at virksomhetene på alle forvaltningsnivå får mer spesifikke og resultatorienterte anbefalinger. Det vil i tillegg være behov for samordning og konsolidering av eksisterende, hovedsakelig prosessorienterte, veiledning om hvordan de kan gå fram for å finne og dekke egne behov.



Figur 1 – Felles retning på arbeidet med informasjonssikkerhet i forvaltningen

Informasjonssikkerhet er viktig for alle oppgaver og tjenester

Offentlig forvaltning utfører en lang rekke ulike oppgaver og leverer ulike tjenester. Ansvaret for disse er fordelt på forvaltningsnivåene kommune, fylkeskommune og stat. I tillegg er det organisering i tjenestesektorer. Som regel er imidlertid ansvaret for oppgaver og tjenester til syvende og sist fordelt på virksomheter.

Informasjonsbehandling er kjernen i mange oppgaver og tjenester i offentlig forvaltning. De resterende tjenestene er avhengige av informasjonsbehandling i en eller annen form. I vår moderne verden har informasjonsbehandling svært stor betydning for offentlige virksomheters oppgaveløsing. Informasjonssikkerhet handler om å sikre denne informasjonsbehandlingen. Digital sikkerhet og sikkerhet i digitale tjenester er en viktig del av dette

Informasjonssikkerhetsbrudd kan få konsekvenser for virksomhetens leveranser, økonomi og evnen til å utføre oppgaver og yte tjenester. Slike brudd kan også få følger for innbyggere og ansatte, andre virksomheter, samfunnsfunksjoner eller nasjonale sikkerhetsinteresser. Informasjonssikkerhet på tvers av forvaltningen har stor betydning for samfunnssikkerheten.

Virksomhetenes ledelse har et selvstendig ansvar

En offentlig virksomhet trenger god informasjonssikkerhet for å være i stand til å utføre sine oppgaver og levere sine tjenester på en god måte – for å nå sine mål og ivareta lovpålagte forpliktelser.

Lederne for offentlige virksomheter har et selvstendig ansvar for å styre risiko for de oppgavene og tjenestene som de har ansvaret for. De må ta ansvaret for å styre arbeidet med informasjonssikkerhet som en del av det å styre risiko for virksomhetens oppgaver og tjenester.

Ettersom informasjonssikkerhet er viktig for en virksomhets måloppnåelse er det mange regelverk som stiller krav til arbeidet med informasjonssikkerhet. Regelverkene har forskjellig formål og innretning, og retter oppmerksomheten mot ulike ting[3]. En virksomhet må likevel evne å jobbe helhetlig og effektivt.

Hva en virksomhet skal ha på plass for å ivareta ansvaret

Arbeidet med informasjonssikkerhet skal være risikobasert, med fleksibilitet og rom for tilpasning til en virksomhets størrelse, egenart og risiko. Dette skal gi tilstrekkelig og kostnadseffektiv informasjonssikkerhet for alle oppgaver og tjenester, inkludert digitale tjenester.

Ledelsens redskap for å få tilstrekkelig informasjonssikkerhet for virksomhetens oppgaver og tjenester er styringsaktiviteter og sikkerhetstiltak.

De delene av styringen som har spesiell oppmerksomhet på informasjonssikkerhet kalles gjerne «styringssystem for informasjonssikkerhet», og kan deles inn i to hoveddeler:

- Styringsaktiviteter
- Sikkerhetstiltak

Du kan lese mer om styringsaktiviteter, sikkerhetstiltak og hvilke krav og anbefalinger som gjelder for virksomhetene i vedlegg.

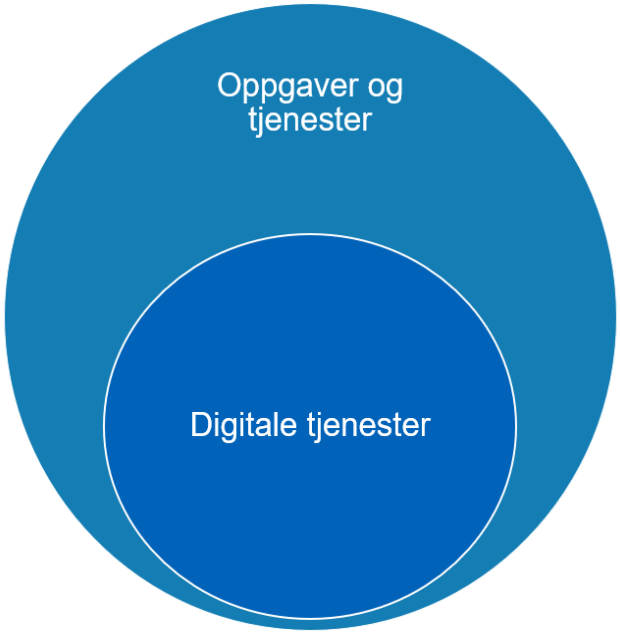
Figur 2 – Virksomheter har behov for styringsaktiviteter og sikkerhetstiltak for å få god informasjonssikkerhet

Digital sikkerhet er en viktig del av arbeidet med informasjonssikkerhet

[3] https://www.digdir.no/informasjonssikkerhet/ulike-perspektiver-gir-ulikt-fokus/2279

Digitale systemer og nettverk er viktig for de fleste oppgaver og tjenester i offentlig forvaltning. Offentlige virksomheter har også et stigende antall digitale tjenester. Digital sikkerhet er en svært viktig del av arbeidet med informasjonssikkerhet.

God informasjonssikkerhet er ikke bare en forutsetning for å kunne utføre oppgaver og tjenester generelt, men er også helt nødvendig for å lykkes med, og for kunne ta ut gevinstene fra digitalisering.



Figur 3 - Oppgaver og tjenester i offentlig forvaltning

Felles økosystem og sammenhengende tjenester

Tjenester fra ulike virksomheter vil henge tettere sammen inn i de neste årene. Man er i stor grad avhengig av andre virksomheter, og at de har tilstrekkelig informasjonssikkerhet.

Digitale tjenester er en viktig del av oppgavene og tjenestene som leveres av offentlig forvaltning. Kommuner, fylkeskommuner og statlige virksomheter skal samhandle for å utvikle brukerrettede, sammenhengende og effektive digitale tjenester.

Virksomheter skal samarbeide og dele data i et felles økosystem for digital samhandling og tjenesteutvikling i større grad i fremtiden. Når tjenester fra ulike virksomheter henger tettere blir virksomhetene i større grad avhengig av andre virksomheter, og at de har tilstrekkelig informasjonssikkerhet.

Felles utfordringer på informasjonssikkerhetsområdet har betydning for digitale tjenester, og for tjenestekjeder i felles økosystem. Når tjenester henger sammen, kan en hendelse i én virksomhet kan få direkte konsekvenser for tjenester hos andre virksomheter. Det svakeste leddet kan bryte hele tjenestekjeden.

Når virksomheter skal utvikle og levere tjenester sammen, er det behov for samarbeid og samstyring for å håndtere risiko i tjenestekjeden. Slikt samarbeid vil inkludere samstyring av informasjonssikkerhet.

Det er derfor viktig å se på hvordan rammebetingelsene for informasjonssikkerhet kan legge til rette for dette på en god måte, slik at det er lett å gjøre rett.

Avgrensning

Det er en kjensgjerning at det er mye som er utenfor den enkelte virksomhets kontrollspenn. Det er blant annet viktig at det arbeides med digital sikkerhet i den grunnleggende infrastrukturen som alle er avhengige av, [4] og at det er samarbeid mellom responsmiljøer på tvers av EU/EØS[5].

Det er også viktig at offentlig forvaltning har tilgang til ulike typer kompetanse med betydning for informasjonssikkerhet. Det er blant annet snakk om kompetanse innen ledelse, virksomhetsstyring og -arkitektur, risikostyring, IKT- og IKT-sikkerhetskompetanse[6].

Dersom det for eksempel kommer en «nasjonal skyløsning»[7] eller løsninger for sentraldrift for offentlige tjenester, så vil noen av konseptene som beskrives i dette notatet, slik som basisnivåer med sikkerhetstiltak, kunne bidra til å få god forståelse for ansvarsdelingen mellom virksomhetene (tjenesteeier / kunde) og tilbydere av sentrale tjenester. De kan også benyttes til å gi virksomhetene god oversikt over hva de sentrale tjenestene tar ansvaret for, inkludert hvilke sikkerhetstiltak tilbyder av sentral løsning sørger for.

Det er vanskelig å dekke alt som kan inngå i informasjonssikkerhet og digital sikkerhet under én paraply. Dette notatet tar utgangspunkt i, og tar i hovedsak for seg, det selvstendige ansvaret hver virksomhet i forvaltningen har for å styre risiko for sine oppgaver og tjenester; hvordan anbefalinger og veiledning kan hjelpe dem med å lykkes med å ivareta det ansvaret, og hvordan det kan bli mer effektivt og gjøres mer likt på tvers av virksomhetene.

Det er likevel snakk om å se arbeidet med informasjonssikkerhet på tvers av forvaltningsnivåene og virksomhetene i forvaltningen, og hvordan de kan få en mest mulig felles referanseramme for arbeidet, og få gode rammebetingelser for samarbeid og samstyring.

Sammen med andre initiativer som drives fram på andre tverrgående områder, spesielt innen digital sikkerhet, kan dette arbeidet bidra til et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning.

---

[4] Meld. St. 28 (2020–2021) *Vår felles digitale grunnmur — Mobil-, bredbånds- og internettjenester.* https://www.regjeringen.no/no/dokumenter/meld.-st.-28-20202021/id2842784/?ch=1

[5] https://digital-strategy.ec.europa.eu/en/activities/cybersecurity-digital-programme

[6] Nasjonal strategi for digital sikkerhetskompetanse https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/

[7] Nasjonalt digitalt risikobilde 2022 s.28 https://nsm.no/getfile.php/1312007-1667980738/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf

2 Del 2 – Utfordringsbildet

Offentlige virksomheter møter utfordringer med å ha tilstrekkelig systematisk og kostnadseffektivt arbeid med informasjonssikkerhet. Vi har delt det opp i ulike *problembeskrivelser*.

Problembeskrivelsene her i del 2 er korte, men er ment å være tilstrekkelig for å få oversikt over utfordringsbildet.

Generelle problemer med styringsaktiviteter og sikkerhetstiltak omtales først. Deretter beskrives mer detaljerte deler innenfor disse, og en del omkringliggende probemstillinger på tvers av virksomheter.

2.1 Problembeskrivelser

2.1.1 P1 Svake eller manglende styringsaktiviteter

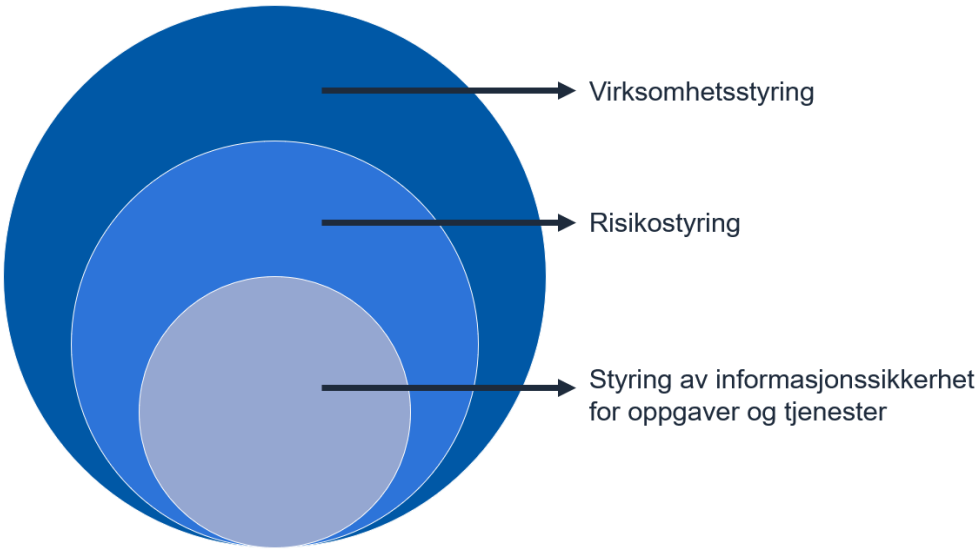
Virksomheter har svake eller manglende styringsaktiviteter.

Noen virksomheter har en ledelse som av ulike grunner ikke er i stand til å ivareta sitt ansvar innenfor informasjonssikkerhet. Dette fører til svak eller manglende gjennomføring av styringsaktiviteter[8].

Dette fører blant annet til svak vurdering og håndtering av risiko. Vurderingene kan for eksempel være delvis frikoblet fra oppgavene og tjenestene, eller være delvis frikoblet fra ledelsens prioritering av ressursbruk.

Anbefalinger og veiledning blir fulgt opp i varierende grad, og det er begrenset forståelse, spesielt blant ledere, om betydningen av sikkerhetsarbeidet.[9]

Informasjonssikkerhet er viktig for oppgaveløsningen, og ledelsen må styre aktivt. Det er ikke tilstrekkelig med «ledelsesforankring».



Figur 4 - Informasjonssikkerhet inngår i styringen av en virksomhet

https://www.riksrevisjonen.no/rapporter/

[9] Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden*, s. 80.

2.1.2 P2 Mangler grunnleggende sikkerhetstiltak

Virksomheter mangler grunnleggende sikkerhetstiltak.

Anbefalinger og veiledning om effektive sikkerhetstiltak har vært tilgjengelig i lang tid. Det er tilgjengelig fra flere internasjonale kilder, og i Norge har for eksempel NSM god veiledning om tekniske IKT-sikkerhetstiltak for kritisk infrastruktur.

Når hendelser inntreffer, eller tilsynsmyndigheter gjør grundige undersøkelser, viser det seg at helt grunnleggende sikkerhetstiltak ikke er etablert, eller ikke fungerer etter hensikten.

Riksrevisjonen viser til at et flertall av statlige virksomheter har store svakheter i informasjonssikkerheten og mangler grunnleggende tiltak som tilgangsstyring og overvåking av systemer.[10]

Selv om bevisstheten rundt informasjonssikkerhet øker, tar ikke virksomhetene nødvendige grep for å bedre deres arbeid med informasjonssikkerhet.[11] Flere offentlige virksomheter, [12] og spesielt kommuner, mangler grunnleggende sikkerhetstiltak som kan bidra til å gi tilstrekkelig sikkerhet.[13]

Det er en del grunnleggende sikkerhetstiltak man vet kan ha god effekt. NSM viser blant annet til dette innen IKT-sikkerhet.[14]

Virksomheter som mangler grunnleggende sikkerhetstiltak, har delvis mistet evnen til å levere primære oppgaver og tjenester til sine innbyggere på grunn av informasjonssikkerhetsbrudd[15]. Det har også resultert i økonomiske konsekvenser på grunn av ressursbruk på håndtering av hendelser og gjenoppretting av tjenester[16].

Datatilsynet peker på mangler i grunnleggende sikkerhetstiltak i sitt varsel om overtredelsesgebyr til Stortinget[17] med hjemmel i personopplysningsloven.

2.1.3 P3 Utilstrekkelig oversikt over informasjonsbehandlingen

Virksomheter har utilstrekkelig oversikt over informasjonsbehandlingen.

Mange virksomheter mangler tilstrekkelig oversikt over:

- oppgaver og tjenester
- informasjonstyper som behandles i disse

---

[10] Riksrevisjonen (2018) *Riksrevisjonens årlige revisjon og kontroll – budsjettåret 2017. Dokument 1 (2018–2019)*.
[11] Nasjonal sikkerhetsmyndighet (2021) *Nasjonalt digitalt risikobilde 2021,* s. 10.
[12] Ibid, s.10.
[13] KPMG, *IKT-sikkerhet I Østre Toten kommune forut for dataangrepet 9. januar 2021*, s. 25. https://www.ototen.no/_f/p1/i5689ceb7-72b4-44d0-970c-a5c4828047e5/endelig-rapport-26082021-kpmg_sladdet.pdf
[14] Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden*, s. 33.
[15] Østre Toten kommunes nettside 10.1.21 Dataangrepet – slik blir våre innbyggere berørt
[16] Østre Toten kommune: – Dataangrepet har kostet oss mer enn 32 millioner https://www.aktuellsikkerhet.no/cybersikkerhet-datainnbrudd-it-sikkerhet/ostre-toten-kommune-dataangrepet-har-kostet-oss-mer-enn-32-millioner/700321
[17] Datatilsynet. *Vedtak om overtredelsesgebyr - Bergen kommune - Melding om avvik i Vigilo*. 03.09.2020. https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/varsel-om-overtredelsesgebyr-til-stortinget/

- informasjonssystemene (inkl. digitale systemer) de benytter
- hva konsekvensene kan bli ved informasjonssikkerhetsbrudd

For eksempel mangler flere kommuner oversikt over egne data og systemer.[18]

Det fører til at virksomhetene ikke er tilstrekkelig i stand til å prioritere ressursinnsatsen og ha oversikt over risiko og behovet for sikkerhetstiltak, og sørge for tilstrekkelig informasjonssikkerhet.

2.1.4 P4 Må til en viss grad gjøre de samme vurderingene

Virksomheter må til en viss grad gjøre de samme vurderingene.

Virksomheter må ofte gjøre de samme, eller tilsvarende, vurderinger. Det kan være stor variasjon i resultater fra vurderingene, uten at variasjonen er begrunnet i virksomhetenes ulike og unike behov.

Det at virksomhetene til en viss grad må gjøre de samme vurderingene gjelder særlig virksomheter som har tilsvarende oppgaver eller leverer de samme tjenestene, for eksempel en stor del av oppgaveløsningen i kommunene. En del støtteoppgaver er likeartede på tvers av virksomheter, for eksempel personalforvaltning eller anskaffelsesprosess.

Selv om oppgavene og tjenestene er de samme eller svært like, så vil ikke alle vurderinger være de samme. Det vil være andre forhold som varierer, blant annet hvordan tjenestene leveres med bruk av ulike typer støttesystemer.

En stor mengde separate vurderinger er ikke spesielt effektivt, og bidrar til sprikende sikkerhet i forvaltningen.

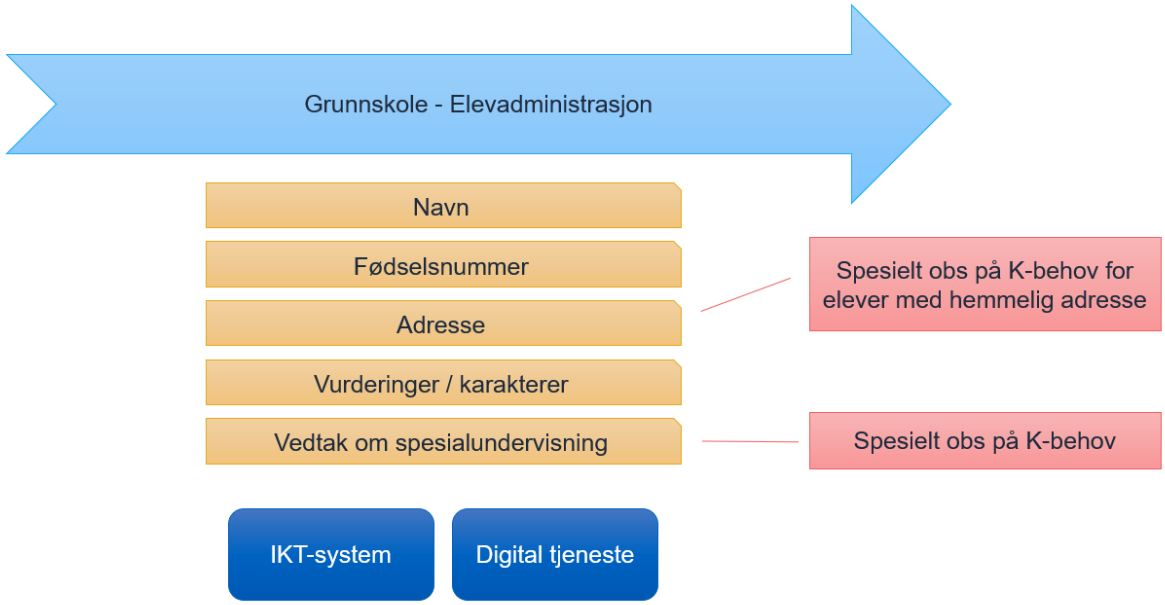
Elevadministrasjon i grunnskolen kan trekkes frem som et eksempel. Her behandles blant annet elever og foresattes navn og adresse. Mange kommuner bruker også mange av de samme støttesystemene. Etter at Bergen kommune tok i bruk digitale tjenester fra Vigilo, kom det i 2020 frem at kommunen ikke hadde gjort god vurdering og håndtering av risiko. Opplysninger om elever på en hemmelig adresse var tilgjengelige for uvedkommende.[19] Hendelsen belyser kommunens selvstendige ansvar for å ivareta ulike hensyn når de utfører oppgaver, og viser hvor alvorlig konsekvensene kan bli ved mangelfull oversikt over informasjonsbehandlingen og svak vurdering og håndtering av risiko.

Alle kommuner har behov for å ha oversikt over hvor store konsekvensene kan bli ved informasjonssikkerhetsbrudd i ulike oppgaver i grunnskolen, for å være i stand til å styre ressursbruken på vurdering og håndtering av risiko.

---

[18] Kommunal- og moderniseringsdepartementet (2020) *Dataforvaltning og -deling i kommunene*. R1021222. S. 36, kapittel 5.5. https://www.regjeringen.no/contentassets/05c9563f28024e1bb82f5e31d1dbfd72/rapport_dataforvaltning-og--deling-i-kommunene_endelig-versjon.pdf

[19] Datatilsynet. *Vedtak om overtredelsesgebyr - Bergen kommune - Melding om avvik i Vigilo*. 03.09.2020.



Figur 5 – Skisse av oppgaven «elevadministrasjon», med informasjonstyper og digitale systemer som benyttes i informasjonsbehandlingen.

2.1.5 P5 Mangelfull forvaltning av sikkerhetstiltak

Virksomheter har utfordringer med forvaltning av sikkerhetstiltak[20].

For eksempel kan det være at de mangler

- systematisk godkjenning og etablering av sikkerhetstiltak
- kostnadseffektiv forvaltning av sikkerhetstiltak
- tydelig ansvar for sikkerhetstiltak
- evaluering og oppfølging av etablerte sikkerhetstiltak

Forvaltning av sikkerhetstiltak på tvers av virksomheten og dens tjenesteleverandører krever et annet perspektiv og annen kompetanse enn å ha ansvaret for noen spesifikke sikkerhetstiltak.

Det er virksomheter som mangler et bevisst forhold til hvilke sikkerhetstiltak som etableres, og hvem som er ansvarlig for dem.

Selv om man har etablert sikkerhetstiltak basert på reelle behov er det behov for å følge dem opp, og evaluere effekten av dem. Slik kan man unngå å ha sikkerhetstiltak som ikke virker etter hensikten, eller som har for store negative sideeffekter.[21]

2.1.6 P6 Arbeidet er kompetansekrevende

Arbeidet i virksomhetene er kompetansekrevende.

[20] Difi-rapport 2018:4 Arbeidet med informasjonssikkerhet i statsforvaltningen, kap. 3.2.2 s. 28
[21] Direktoratet for forvaltning og IKT (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen*. 2018:4. S. 28. https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-statsforvaltningen/2044

Norsk regelverk er i stor grad funksjonsbasert. Det vil si at det stiller krav til hva som skal oppnås, men er fleksibelt med tanke på de spesifikke detaljene i hvordan det skal oppnås. Det er stort rom for tilpasning til en virksomhets størrelse, egenart og risiko. Slik fleksibilitet er nødvendig, ettersom det gjør det mulig å tilpasse styringsaktiviteter og sikkerhetstiltak til lokale behov, og sørge for at sikkerhetsarbeidet både er formålseffektivt og kostnadseffektivt.

Selv om regelverk legger opp til at det finnes flere måter å gjøre vurderinger på, ligger det en forutsetning til grunn om at alle virksomheter må kunne oppnå et «forsvarlig» eller «tilstrekkelig» sikkerhetsnivå for det de har ansvaret for.[22]

Utfordringen er at det kan være kompetansekrevende. Det krever kompetanse i ledelse, organisering, endringsstyring og utvikling av organisasjonskultur. Det krever evne til å ha oversikt over oppgaver og tjenester, gjøre gode vurderinger av, og ta beslutninger om, risiko. Det krever tilstrekkelig faglig kunnskap til å velge, etablere og forvalte sikkerhetstiltak – samt fase ut sikkerhetstiltak som ikke lenger er nyttige.

I internasjonal målestokk har Norge hovedsakelig små virksomheter, og for mange av disse er det en utfordring å dekke alle behovene innen virksomhetsstyring, inkludert informasjonssikkerhet.

Virksomheter som legger lite vekt på styringsaktiviteter, men i stedet hovedsakelig går inn for etablering av anbefalte sikkerhetstiltak fra en tiltaksbank, vil også kunne oppleve utfordringer med kompetanse. Kompetanse- og ressursbehovet kan være stort for å etablere og forvalte sikkerhetstiltak. De vil i tillegg ende opp med utfordringene som følger av utilstrekkelig ledelsesforankring og svak styring. Det kan være for høye kostnader, informasjonssikkerhet som ikke er tilpasset behovet i virksomhetens oppgaver og tjenester, eller en ledelse uten innsikt i eller styring med risiko for virksomhetens oppgaver og tjenester.

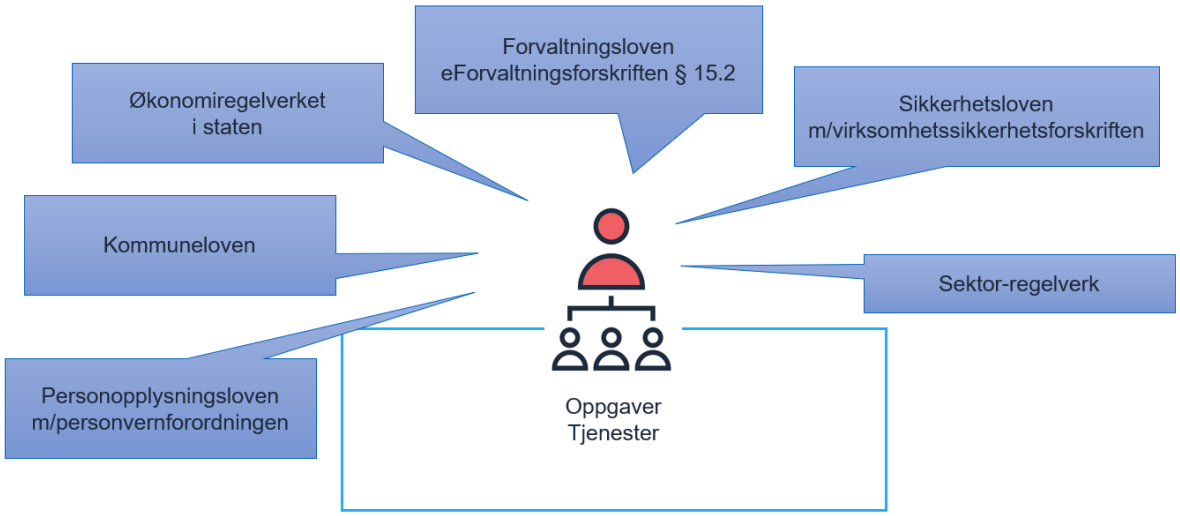
Kompetansebehovet kan til en viss grad avhjelpes med ulike virkemidler, som anbefalinger og veiledning.[23]

Informasjonssikkerhetsområdet er stort, og det er mange ulike roller og mange ulike typer kompetanse som er involvert. Det vil for eksempel være behov for forskjellig kompetanse for å gjennomføre styringsaktiviteter og for etablering og forvaltning av ulike sikkerhetstiltak.

Å ivareta informasjonssikkerhet i styringen av en virksomhet krever et annet perspektiv og annen kompetanse enn å beskytte nettverksteknologi mot menneskestyrte angrep.

Det er noen som skal styre risiko for de oppgavene og tjenestene de har ansvaret for (inkludert informasjonssikkerhet), andre som har ansvaret for å støtte dem i dette arbeidet, og atter andre som skal etablere og forvalte spesifikke sikkerhetstiltak. Den sistnevnte gruppen er i dag i økende grad utenfor virksomhetens egen organisasjon, og har ansvaret for sikkerhetstiltak som en del av tjenesteleveranser til virksomheten.

[22] Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden,* s. 73.
[23] NOU 2018:14 *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.*



Figur 6 – Mange regelverk stiller krav til ledelsens styring, og det er krevende å arbeide helhetlig for å ivareta alle hensyn.

2.1.7 P7 Arbeidet er ressurskrevende

Arbeidet i virksomhetene er ressurskrevende også utover behovet for kompetanse.

Et godt systematisk arbeid med informasjonssikkerhet krever også andre ressurser i tillegg til kompetanse. Virksomhetene må blant annet:

- Etablere styringsaktiviteter
- Utvikle gode føringer for styringsaktivitetene sine
- Ha oversikt over informasjonsbehandlingen
- Prioritere ressursinsats for vurdering og håndtere risiko
- Gjennomføre risikovurdering og håndtering av risiko for oppgaver, tjenester og informasjonssystemer
- Etablere hensiktsmessige sikkerhetstiltak
- Sørge for kostandseffektiv forvaltning av sikkerhetstiltak på tvers av oppgaver og tjenester
- Måle og evaluere hele eller deler av arbeidet med informasjonssikkerhet
- Følge opp evalueringer og forbedre arbeidet med informasjonssikkerhet
- Rapportere til departement, andre styrende organer eller andre interessenter
- Ivareta informasjonssikkerhet ved bruk av tjenesteleverandører

Disse tingene er viktige og nødvendige, og virksomhetene er skal gjøre disse tingene for å få kostnadseffektiv informasjonssikkerhet iht. gjeldende regelverk.

Noen steder kommer ressursbehovet til informasjonssikkerhet i konflikt med andre plikter og behov, og andre viktige oppgaver som må utføres for å levere gode tjenester. Ledelsen i virksomheter med få ressurser har en vanskelig oppgave med prioritering av ressursbruken.

Arbeidet med informasjonssikkerhet kan oppleves som ressurskrevende også for noen av de store virksomhetene i forvaltningen. Store virksomheter som er medlemmer av Skate har gitt

uttrykk for dette: «[..] vi har utfordringer og manglende kompetanse og ressurser i både små og store virksomheter.»[24]

Det at mange virksomheter av ulike størrelse har vesentlige utfordringer på området kan ha stor påvirkning på den samlede informasjonssikkerheten i offentlige tjenester som henger sammen og er avhenge av hverandre.

2.1.8 P8 Krevende å undersøke omfang av sikkerhetstiltak

Det kan være vanskelig å gjøre undersøkelser av om omfang av sikkerhetstiltak i virksomheter er tilstrekkelig. Det kan gjelde ved

- virksomhetsledelsens egne evalueringer
- internrevisjon
- tilsyn fra myndigheter
- et departements overordnede oversikt for egen sektor
- oversikt på tvers av sektorer, for eksempel sentralforvaltningen i staten

Både virksomhetene selv og tilsynsmyndigheter må i stor grad gjøre vurderinger og utarbeide kriterier selv, og tilpasse til ulike tjenestesektorer og typer oppgaver og tjenester, basert på ulike standarder og anbefalinger.

Innen den delen som handler om å beskytte teknologi mot angrep kan det være spesielt krevende for virksomheter å vite om de har tilstrekkelig omfang av sikkerhetstiltak.

NSM fremhever et økt behov for digital sikkerhet. «Det er krevende å opprettholde sikkerhetsnivået når utviklingen går så raskt, med et dynamisk og uoversiktlig sårbarhetsbilde. Trusselaktører tilpasser seg endrede situasjoner raskt og utnytter sårbarheter som oppstår.»[25]

2.1.9 P9 Vanskelig å evaluere på tvers av virksomheter

Det kan være vanskelig å gjøre evaluering av tilstrekkelig informasjonssikkerhet på tvers av virksomheter.

For eksempel om styringsaktivitetene er på plass, fungerer godt, og om tilstrekkelige sikkerhetstiltak er etablert og fungerer etter hensikten.

Det finnes ingen felles målestokk å vurdere mot.

2.1.10 P10 Utfordrende å bruke og følge opp tjenesteleverandører

Det er utfordrende for mange virksomheter å bruke og følge opp tjenesteleverandører.

Offentlige virksomheter har utstrakt bruk av tjenesteleverandører til informasjonsbehandlingen i oppgaver og tjenester. Digdir erfarer at det er et tema som opptar veldig mange, og at det er mange synes det er utfordrende å ivareta tilstrekkelig informasjonssikkerhet i tjenesteleveranser og følge opp tjenesteleverandører.

---

[24] Referat fra møte i Skates arbeidsutvalg (AU) 15.12.2021 i tilknytning til sak om status og utfordringer i offentlig sektor mht. styring og kontroll på informasjonssikkerhetsområdet.
[25] Nasjonal sikkerhetsmyndighet (2021) *RISIKO 2021 – helhetlig sikring mot sammensatte trusler,* s. 14.

Økende bruk av tjenesteleverandører gjør at man i dag har lange verdikjeder på tvers av tjenestesektorer og landegrenser. Det kan være en medvirkende årsak til at virksomheter har problemer med å holde oversikt over egen informasjonsbehandling, og det kan gjøre det vanskelig for virksomhetene å ha kontroll og oversikt over omfanget av etablerte sikkerhetstiltak.[26] Dette gjør virksomhetene desto mer sårbare for trusler, og det gjør også den totale angrepsflaten større.

Det er foreslått endringer i dagens anskaffelsesregelverk, slik at oppdragsgivere blir pliktige til å stille krav om digital sikkerhet.[27] Men denne plikten er allerede implisitt i overordnede krav om tilstrekkelig styring av risiko for virksomhetens oppgaver og tjenester; og er uavhengig av hvilke innsatsfaktorer som benyttes i oppgaveløsningen.

Deler av behovet for informasjonssikkerhet for oppgaver og tjenester må nødvendigvis videreføres som krav til leverandører av tjenester som innebærer informasjonsbehandling, inkludert digitale tjenester.

Staten har noe i standardavtaler[28] som som kan benyttes, men i all hovedsak er virksomhetene overlatt til å komme fram til sine behov for informasjonssikkerhet i tjenesteleveranser og sørge for å stille gode krav som dekker disse. Vi kan ikke si at det er helhetlig, oversiktlig, forutsigbar og ensartet kravstilling fra offentlig forvaltning til leverandørmarkedet.

2.1.11 P11 Manglende tillit mellom offentlige virksomheter kan være hinder for digitalisering

Når virksomheter i forvaltningen skal dele og bruke data og bygge sammenhengende tjenester på tvers av virksomhetsansvaret, er det behov for tillit til at andre virksomheter har tilstrekkelig informasjonssikkerhet.

Et svakt ledd i en tjenestekjede kan få konsekvenser for tjenester hos alle virksomhetene som er involvert. Dersom man skal drive med samstyring, inkludert å gå sammen for å styre risiko for tjenester, så er det behov for å kjenne igjen styringsaktivitetene og måten dette gjøres på.

Vi har ikke sterke indikasjoner på at det er problemer med manglende tillit i dag, men DSBs rapport fra 2020 om risikostyring i verdikjeder [29] vurderer det som viktig at aktører i en verdikjede har tillit til hverandre.

2.1.12 P12 Vanskelig å få til helhetlig tilnærming i virksomhetene

Virksomheter kan oppleve at det er krevende å få til en helhetlig tilnærming til styring av informasjonssikkerhet.

Det kan være en organisatorisk utfordring med silofisering i fagområder, delvis på bakgrunn av oppdeling av ansvar iht. ulike regelverk. Ensidige perspektiver kan også føre til skeivt fokus – for eksempel ved at informasjonssikkerhet ender opp med å kun handle om å sikre

[26] Nasjonal sikkerhetsmyndighet (2021) *Nasjonalt digitalt risikobilde 2021,* s. 26.
[27] Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden*, s. 87.
[28] https://anskaffelser.no/avtaler-og-regelverk/statens-standardavtaler-ssa
[29] Direktoratet for samfunnssikkerhet og beredskap (2020) *Risikostyring i digitale verdikjeder*, s. 31.

konfidensialitet på personopplysninger, eller bare å sikre den digitale teknologien man benytter.

Det hender at IKT-sikkerhet i anskaffelser håndteres adskilt og separat – delvis løsrevet fra vurdering av behovet for informasjonssikkerhet i oppgavene og tjenestene som anskaffelsene er innsatsfaktorer til. Det kan føre til usammenhengende risikostyring, og manglende forståelse for, og håndtering av, risiko hos lederne som har ansvaret for oppgavene og tjenestene.

Nasjonal sikkerhet iht. lov om nasjonal sikkerhet (sikkerhetsloven) handler i svært stor grad om informasjonsbehandling, men spesifikt for grunnleggende nasjonale funksjoner (GNF), og tilfeller der tilsiktede handlinger kan føre til hendelser som går konsekvenser for nasjonale sikkerhetsinteresser. Noen steder håndteres etterlevelse av regelverket likevel adskilt fra det øvrige arbeidet i virksomheten. Det er ikke hensiktsmessig, og ikke i tråd med intensjonen som beskrives i lovproposisjonen. NSMs tilsyn peker også på problemer med manglende forståelse for hvordan pliktene i regelverket bør integreres i virksomhetsstyringen. Det at virksomhetene vurderer risiko med tanke på konsekvenser for egen økonomi o.l. i stedet for konsekvenser for nasjonale sikkerhetsinteresser fører til svake vuderinger, og kan føre til dårlig ivertakelse av nasjonal sikkerhet.

Det er utfordrende å oppnå god forståelse om helhetsperspektivet som trengs for å vurdere relevante trusler fra tilsiktede handlinger, uhell og menneskelige feil og de medfølgende konsekvenser et sikkerhetsbrudd kan ha.[30]

Det finnes også tverrsektorielle utfordringer. I en tjenestesektor kan man ha ulik forståelse av risiko, og det faktum at konsekvenser av et sikkerhetsbrudd kan ramme andre tjenestesektorer.[31]

2.1.13 P13 Mangelfull og fragmentert regulering

Det er svært mange regelverk som stiller krav til informasjonssikkerhet i en eller annen form - eksplisitt eller implisitt - og til dels reguleres like hensyn ulikt.

Krav til informasjonssikkerhet kommer i ulike former med svært ulik detaljeringsgrad, og beskrives på forskjellige måter. Regelverkene har ulike formål og ulik innretning, blant annet med tanke på årsaker til og konsekvenser av hendelser. Dette gjør det vanskelig å holde oversikt, og se hva som er ganske likt, og vite hvordan en virksomhet kan arbeide helhetlig med risikostyringen.

En av årsakene til at det har blitt slik er at arbeid med informasjonssikkerhet skal bidra til å ivareta mange ulike hensyn. Informasjonsbehandling, inkludert bruk av digitale systemer, har blitt helt grunnleggende i samfunnet, og har stor betydning for alle oppgaver og tjenester i offentlig forvaltning.

Eksempler på ivaretakelse av ulike hensyn:

- Personopplysningsloven regulerer informasjonssikkerhet når man behandler personopplysninger for å unngå konsekvenser for fysiske personers rettigheter og friheter, uavhengig av årsaker til hendelser.

[30] Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn — Samfunnssikkerhet*, s. 165.
[31] Meld. St. 38 (2016 –2017) *IKT-sikkerhet - Et felles ansvar,* s. 22.

- Sikkerhetsloven er primært opptatt av å unngå hendelser forårsaket av tilsiktede handlinger, for å unngå svikt i grunnleggende nasjonale funksjoner og konsekvenser for nasjonal sikkerhet. I vårt moderne samfunn handler mye av det om informasjonssikkerhet.

Det er behov for god forståelse av regelverkene for å være i stand til å ivareta alle hensyn. For eksempel skal mange virksomheter både unngå konsekvenser for egen økonomi og evne til å utføre oppgaver og tjenester, konsekvenser for nasjonal sikkerhet, og personvernkonsekvenser for de de behandler opplysninger om. Mye av arbeidet en virksomhet da må gjøre vil være det samme eller svært likt uavhengig av regelverk. Styringsaktiviteter vil i hovedsak være de samme, og de fleste sikkerhetstiltakene vil passe for alle oppgaver og tjenester.

Hvis vi konsentrerer oss om den delen av informasjonssikkerhet som handler om IKT-sikkerhet eller digital sikkerhet, så var IKT-sikkerhetsutvalgets vurdering at dagens regulering av IKT-sikkerhet er mangelfull.[32] IKT-sikkerhetsutvalget bemerket også at pliktsubjektene synes det er vanskelig å etterleve summen av regelverk. «Mange aktører har uttrykt at det er vanskelig å vite hvilke krav de skal forholde seg til, fordi dagens regelverk oppfattes som omfattende og fragmentert [..]»[33]

Uoversiktlig regelverk er lite digitaliseringsvennlig. Ulike regler for stat og kommune kan vanskeliggjøre samarbeid og felles tilnærming til tjenesteutvikling i felles i digitalt økosystem. For eksempel ved at noen regler er i rundskriv eller instrukser som bare gjelder statlige virksomheter.

[32] NOU 2018:14 *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*, s. 53.
[33] Ibid, s. 72.

3 Del 3 – Tiltak og anbefalinger

3.1 Et nasjonalt løft for informasjonssikkerhet

Både små og store virksomheter har utfordringer, og det virker som det går sakte fremover.[34] Det er behov for et taktskifte i arbeidet med informasjonssikkerhet i forvaltningen.

Digdir mener det bør komme et nasjonalt løft for informasjonssikkerhet generelt, og digital sikkerhet spesielt. Det er nødvendig for at forvaltningen skal være i stand til løse oppgavene sine og levere tjenester i fremtiden.

3.2 Føringer for nye tiltak i forvaltningen

Virksomhetene har et selvstendig ansvar for å styre risiko for sine oppgaver og tjenester, inkludert informasjonssikkerhet. Arbeidet med informasjonssikkerhet skal være risikobasert, med fleksibilitet og rom for tilpasning til en virksomhets størrelse, egenart og risiko. Det er viktig at det er mulig å gjøre egne vurderinger og tilpasse til den enkelte virksomhets behov, slik flere regelverk stiller krav om.

Det bør legges til rette for effektiv oppgaveløsning i offentlig forvaltning, inkludert effektivt arbeid med informasjonssikkerhet.

Nye tiltak skal ikke være unødvendig kostnadsdrivende, men på lang sikt bidra til mer kostnadseffektivt arbeid med informasjonssikkerhet.

Det bør legges til rette for tillit og samarbeid mellom virksomheter og evne til samstyring av risiko for sammenhengende tjenestekjeder.

Det må være god sammenheng i anbefalinger og veiledning, slik at disse møter behovene hos brukervirksomhetene, og at det er lett å gjøre rett.

Man må ta hensyn til, og se sammenhenger med, europeisk samarbeid drevet fram av EU. Det gjelder spesielt på anskaffelsesområdet, for eksempel med sertifiseringsordning for skytjenester.

3.3 Mulige tiltak

3.3.1 T1 Felles referanseramme

Det kan etableres en felles referanseramme (eller norm) for arbeidet med informasjonssikkerhet i offentlige virksomheter. Ved å bygge på det som allerede finnes, og tilføre noen nye elementer, kan det gis tydelige anbefalinger om:

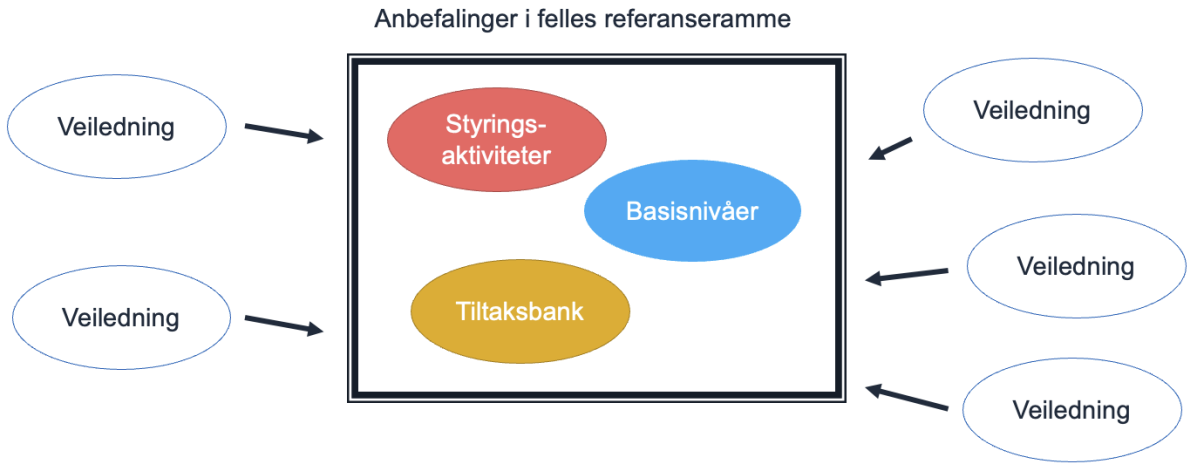
- Struktur og innhold for styringsaktiviteter
- Basisnivåer med sikkerhetstiltak
- Felles tiltaksbank med sikkerhetstiltak

Det kan være andre elementer som også er aktuelle å vurdere å ta med i felles referanseramme.

[34] For eksempel basert på SSBs undersøkelser om sikkerhet i tilknytning til digitalisering og IKT: https://www.ssb.no/statbank/list/iktbruks

Anbefalinger i en felles referanseramme må støttes opp med veiledning fra ulike aktører. Denne veiledningen eksisterer i stor grad allerede, men kan tilpasses slik at den refererer til hvilke elementer i den felles referanserammen det veiledes om i mer detalj. For eksempel vil en tematisk veileder fra NCSC om hvordan en virksomhet kan beskytte seg mot utpressingsskadevare referere til hvilke sikkerhetstiltak fra tiltaksbanken som er spesielt aktuelle med tanke på den trusselen. På denne måten fungerer tiltaksbanken som noe all veiledning om typer eller grupper av sikkerhetstiltak, eller detaljert veiledning om utforming og etablering av spesifikke sikkerhetstiltak, kan referere til. Dette vil gjøre det lettere å se sammenhenger, holde oversikt over sikkerhetstiltak og benytte den veiledningen som er tilgjengelig.

Anbefalinger og tilhørende veiledning skal gjøre det enklere for virksomhetene å ivareta sitt ansvar. Det at ting gjøres mer likt og felles på tvers av forvaltningen kan styrke evnen til samarbeid og samstyring, og bidra til gjensidig tillit mellom tjenesteeiere som er avhengige av hverandre.



Figur 7 – Ulike aktører tar utgangspunkt i felles anbefalinger og tilfører veiledning virksomhetene har behov for

3.3.2 T2 Katalog med oppgaver/tjenester og informasjonstyper

En virksomhet har behov for oversikt over oppgaver og tjenester og informasjonsbehandlingen i disse. En del av arbeidet i styringsaktivitetene er å skaffe seg slik oversikt. For hver oppgave eller tjeneste er det blant annet snakk om hvilke informasjonstyper som behandles, hvilke regelverksbestemmelser som er relevante, hvilke IKT-systemer og digitale løsninger som benyttes, og hvor store konsekvensene kan bli ved informasjonssikkerhetsbrudd. Dette benyttes til å planlegge videre arbeid og prioritere ressursbruken. Det brukes også i arbeidet med vurdering og håndtering av risiko.

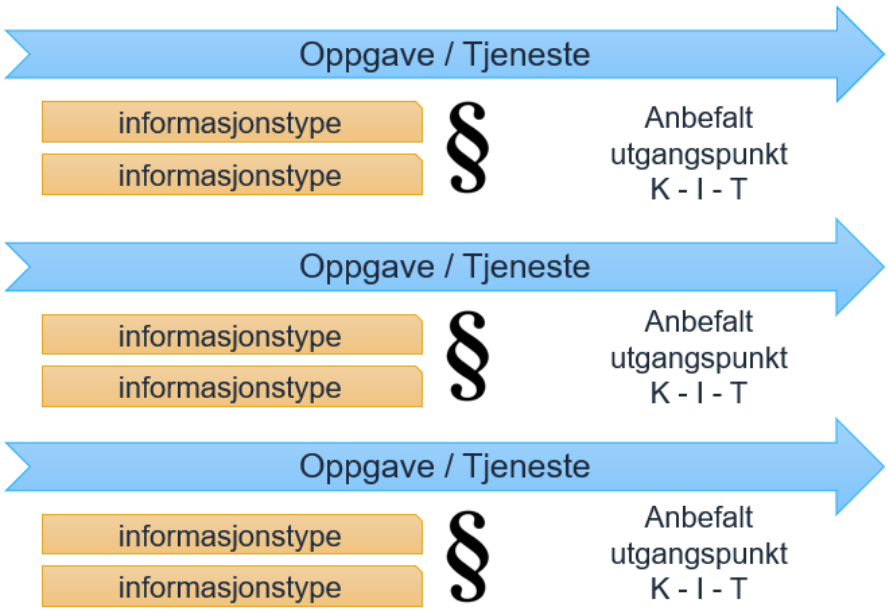
Det kan lages en katalog med oversikt over oppgaver, informasjonstyper som behandles i oppgavene, regelverksbestemmelser som er relevante for de ulike informasjonstypene, og et utgangspunkt for å anslå hvor store konsekvensene ved informasjonssikkerhetsbrudd kan bli. Et slikt halvfabrikat kan redusere omfanget av det som må gjøres i hver enkelt virksomhet, og effektivisere arbeidet med informasjonssikkerhet.

Kommuner og fylkeskommuner har de samme eller svært likeartede oppgaver og tjenester. Virksomheter på alle forvaltningsnivå har en del av de samme støtteoppgavene. For

eksempel personalforvaltning og anskaffelser. Slike oppgaver vil være kandidater for innlemmelse i en slik katalog.

Et arbeid med utvikling og utprøving av en slik katalog må blant annet se på:

- Hvilke elementer som skal inkluderes
- Hvilken grad av «ferdig» oversikt for en oppgave som er godt egnet som utgangspunkt for en virksomhets arbeid med dette
- Sammenheng med aktiviteten det skal benyttes i
- Hvilke oppgaver og tjenester som bør inkluderes



Figur 8 - Oppgaver og informasjonstyper

3.3.3 T3 Basisnivåer med sikkerhetstiltak

Grunnleggende sikkerhetstiltak kan samles i ett eller flere basisnivåer. De kan danne utgangspunktet for virksomhetens valg av sikkerhetstiltak for oppgaver, tjenester eller informasjonssystemer. Det kan både effektivisere arbeidet i virksomhetene og bidra til å gi et mer felles, grunnleggende sikkerhetsnivå på tvers av forvaltningen.

Et basisnivå er et sett med sikkerhetstiltak. Det er satt sammen for å imøtekomme generelle, grunnleggende sikkerhetsbehov, og gjøres tilgjengelig for virksomheters bruk. Sikkerhetstiltak som skal inngå i basisnivåer bør være uttrekk fra en felles tiltaksbank.

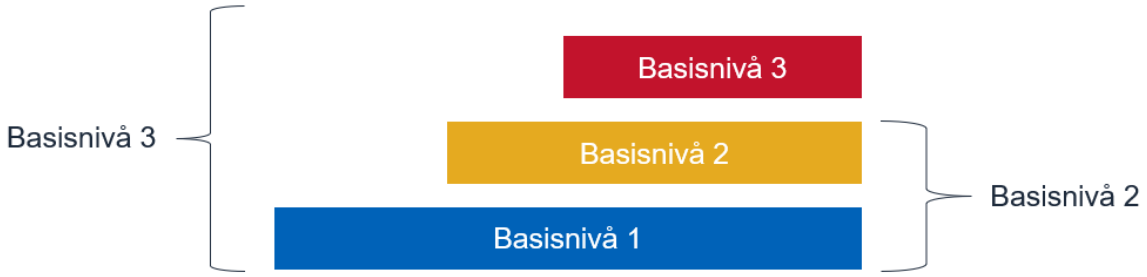
Det kan lages to eller tre basisnivåer som bygger på hverandre. Basisnivå 1 inneholder grunnleggende sikkerhetstiltak som vil være egnet for alle oppgaver og tjenester, eller informasjonssystemer. Basisnivå 2 inneholder alle sikkerhetstiltakene i Basisnivå 1, men er utvidet med flere sikkerhetstiltak. Basisnivå 3 bygger videre fra nivå 2.

Basisnivåene kan korrespondere med kategorier som oppgaver, tjenester eller informasjonssystemer er sortert i, basert på hvor stor konsekvensene kan bli ved informasjonssikkerhetsbrudd. For eksempel kan felleskomponenter og liknende som mange

andre er helt avhengige av, eller som er viktige for kritiske samfunnsfunksjoner, ta utgangspunkt i Basisnivå 3.

Virksomheter benytter styringsaktiviteter for å vurdere og håndtere risiko, og veiledning om tilpasning av basisnivåer, til å tilpasse til egne behov, og sørge for egnede sikkerhetstiltak for sine oppgaver, tjenester og informasjonssystemer.

Det vil være viktig å treffe godt på innhold og omfang i basisnivåene. Det er spesielt viktig at det grunnleggende nivået ikke blir for omfangsrikt. Det bør legges vekt på de grunnleggende tingene, og tilstrekkelig informasjonssikkerhet, uten at det blir kostnadsdrivende; eller at man dreier fokuset fra god styring av risiko til å kun handle om å få på plass sikkerhetstiltak.



3.3.4 T4 Felles tiltaksbank

Det finnes en rekke oversikter over sikkerhetstiltak som man kan vurdere å benytte for å redusere risikoer til et akseptabelt nivå. Ved å hente sikkerhetstiltak fra en tiltaksbank trenger man ikke bruke mye tid og ressurser på å utforme disse selv. Man må passe på at sikkerhetstiltakene er egnet til å møte de risikoene man skal håndtere.

Slike oversikter kommer i form av rammeverk, lister eller kataloger. Sikkerhetstiltakene er gjerne sortert i typer, familier eller etter formål. Vi kaller en slik samling med sikkerhetstiltak for *tiltaksbank*.[35] ISO/IEC 27002 er et kjent eksempel på en tiltaksbank. I føderal forvaltning i USA er det påkrevd å benytte tiltaksbanken NIST SP 800-53 (rev 5).[36] NSMs grunnprinsipper[37] for ikt-sikkerhet, personellsikkerhet og fysisk sikkerhet danner til sammen en tiltaksbank som dekker mange av kategoriene med sikkerhetstiltak som man finner i NIST SP 800-53r5 eller ISO/IEC 27002.

Det er mange ulike tiltaksbanker i bruk i forvaltningen i Norge. Det er positivt, ettersom det kan tyde på at virksomhetene utnytter fleksibiliteten og tilpasningsmulighetene som er til stede. Ulempen kan være at tiltaksbankene har ulik oppbygning og begrepsbruk, og at det ikke er noe som fungerer som felles referanse for sikkerhetstiltak. Det kan gjøre det

[35] https://www.digdir.no/informasjonssikkerhet/tiltaksbankar/3057
[36] NIST SP 800-53 Rev5 er en tiltaksbank, men vær oppmerksom på at den inneholder noen sikkerhetstiltak som Digdir inkluderer i begrepet styringsaktiviteter. De påkrevde aktivitetene i føderal forvaltning i USA er noe annerledes oppbygd enn Digdirs anbefalinger om styringsaktiviteter i Norge. Sistnevnte er basert på det konseptuelle skillet mellom hovedinnholdet i ISO/IEC 27001 og tiltaksbanken i Annex A (ISO/IEC 27002).
[37] Hovedmålgruppen for NSMs grunnprinsipper for ikt-sikkerhet er virksomheter som forvalter kritiske samfunnsfunksjoner eller kritisk infrastruktur.

vanskeligere å ha en felles forståelse og oppfatning av hvilke sikkerhetstiltak som er tilstrekkelig i ulike situasjoner. Det kan gjøre det vanskelig å samarbeide om sikkerhetstiltak i sammenhengende tjenestekjeder.

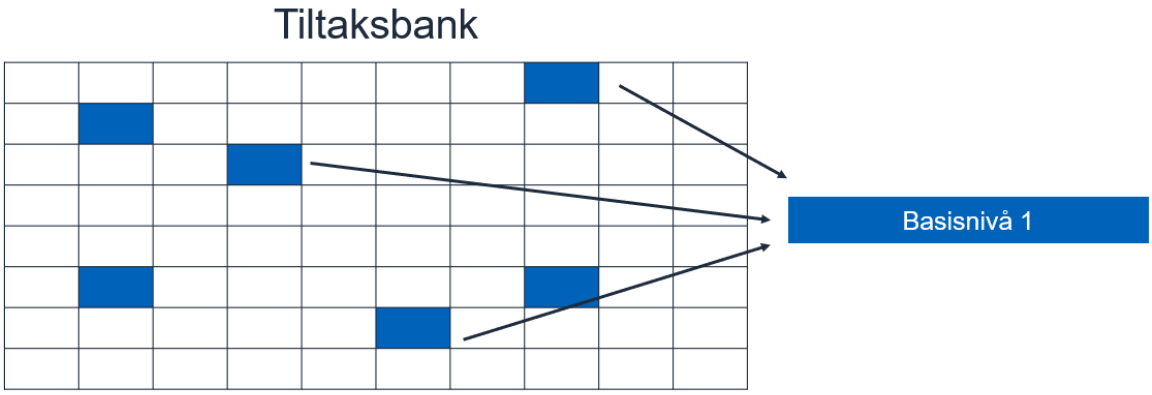
En felles tiltaksbank for offentlig forvaltning vil:

- gjøre det mulig å lage basisnivåer med sikkerhetstiltak fra tiltaksbanken
- fungere som samlingspunkt for veiledning om sikkerhetstiltak, slik at det blir lett for brukere å se ulik veiledning i sammenheng
- fungere som kilde for tilsynsmyndigheter
- bidra til å øke evnen til samarbeid mellom virksomheter

En tiltaksbank kan fylles med en kombinasjon av sikkerhetstiltak og personverntiltak. Det kan gjøre det enklere for virksomhetene å kombinere arbeidet med informasjonssikkerhet og personvern for oppgaver og tjenester som behandler personopplysninger.

Dersom felles tiltaksbank skal utvikles og prøves ut vil det blant annet være behov for å se på:

- Organisering av forvaltningsansvar
- Forutsigbar forvaltningsprosess
- Behov for tilpasning til internasjonale løsninger
- Sammenheng med anskaffelser, spesielt med tanke på at internasjonale tjenesteleverandører allerede har tilpasset seg anerkjente tiltaksbanker
- Kombinasjon av sikkerhetstiltak og personverntiltak i samme tiltaksbank



3.3.5 T5 Kategorier og nivåer av konsekvenser

I arbeidet med informasjonssikkerhet har virksomhetene behov for å estimere mulige konsekvenser ved informasjonssikkerhetsbrudd.

Det brukes til å sortere oppgaver, tjenester eller informasjonssystemer for å prioritere ressursbruken på arbeidet med informasjonssikkerhet der hvor konsekvensene ved informasjonssikkerhetsbrudd kan bli store.

Konsekvenser brukes også for å forstå og vurdere risiko, og inngår i grunnlag for prioritering av ressursbruk i arbeidet med å håndtere risiko.

For i være i stand til å arbeide effektivt med risiko sorterer man vanligvis konsekvenser i kategorier. Det kan for eksempel være konsekvenser for:

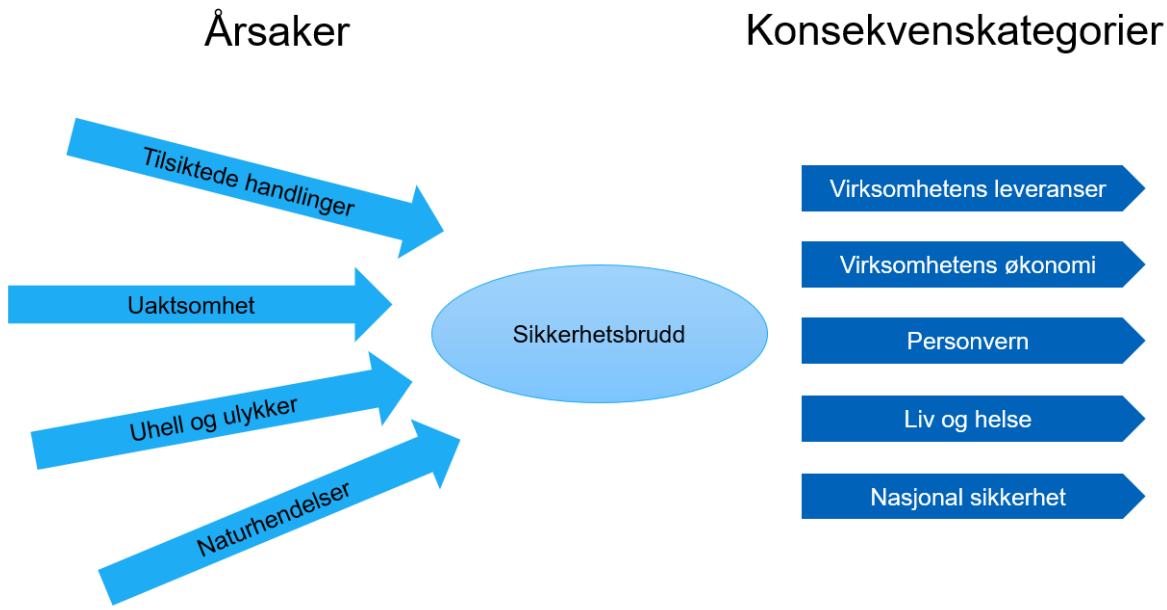
- Virksomhetens evne til å gjennomføre oppgaver og levere tjenester
- Virksomhetens økonomi
- Liv og helse
- Personvern
- Nasjonale sikkerhetsinteresser

En anbefaling om konsekvenskategorier og konsekvensnivåer som kan benyttes av virksomhetene kan redusere arbeidsmengden og effektivisere arbeidet med informasjonssikkerhet.

Det kan bidra til mer felles forståelse av risiko og hvilke hensyn som skal ivaretas, øke kvaliteten på vurderingene, og bidra til at man får mer like resultater fra vurderingene i ulike virksomheter.

Det at disse tingene er gjenkjennbart på tvers av virksomheter vil kunne øke evnen til samarbeid og samstyring av risiko på tvers av virksomheter.

Dersom det skal utvikles basisnivåer med sikkerhetstiltak, så kan sortering basert på konsekvensnivåene benyttes i forbindelse med tilordning av ulike basisnivåer til ulike behov.



Figur 9 - Konsekvenser av informasjonssikkerhetsbrudd

3.3.6 T6 Spesialtilpassede basisnivåer med sikkerhetstiltak

Ved å bygge på de generelle basisnivåene, og hente sikkerhetstiltak fra felles tiltaksbank, kan det lages spesialtilpassede basisnivåer. Ulike interessenter kan utvikle spesialtilpassede basisnivåer for sine behov, eller gå sammen om å utvikle basisnivåer for spesielle bruksområder.

Et spesialtilpasset basisnivå kan være et komplett sett med sikkerhetstiltak, tiltaksforbedringer og annen støtteinformasjon tilpasset for en tjenestesektor, en type informasjonssystem, eller andre spesielle omstendigheter.

Det vil for eksempel være mulig å lage en eller flere spesialtilpassede basisnivåer for skjermingsverdige informasjonssystemer (iht. lov om nasjonal sikkerhet). Et spesialtilpasset basisnivå for helsetjenester kan tas inn i Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), og erstatte dagens opplisting av påkrevde sikkerhetstiltak i kapittel 5.

Innenfor samme felles referanseramme, med felles tiltaksbank og basisnivåer, er det mulig å skalere fra det grunnleggende behovet for de fleste oppgaver og tjenester i forvaltningen til et utvidet og spesialtilpasset sett med sikkerhetstiltak som kan benyttes for skjermingsverdige informasjonssystemer iht. sikkerhetsloven.

3.3.7 T7 Ny lov om informasjonssikkerhet for offentlig forvaltning

Styringsaktiviteter, basisnivåer og tiltaksbank bør i første omgang være anbefalinger og veiledning til virksomhetene. Dette vil gi mulighet til å starte med enkelte deler av forvaltningen og utvikle og tilpasse anbefalingene over tid.

Dersom konseptene viser seg å være nyttige i norsk sammenheng, så vil de ha størst nytteverdi dersom de brukes av de fleste virksomhetene i forvaltningen. På sikt kan det derfor være aktuelt å se på muligheten for å stille krav om bruken av disse. Det kan være starten på en opprydning i dagens fragmenterte regelverk[38], med tanke på at like hensyn skal reguleres likt[39].

Ved å formalisere og regulere sentrale elementer, og sørge for god sammenheng i regelverk, anbefalinger og tilhørende veiledning kan virksomhetene få gode rammebetingelser og hjelpemidler for arbeidet med informasjonssikkerhet.

I melding til Stortinget om samfunnssikkerhet fremgår det at det varierer i hvor stor grad anbefalinger og veiledning blir fulgt opp.

> *Erfaring viser imidlertid at anbefalinger og veiledninger i varierende grad blir fulgt opp av virksomheter. Forståelsen for forebyggende digital sikkerhet er begrenset i mange virksomheter, ikke minst på ledelsesnivå.*[40]

IKT-sikkerhetsutvalget foreslo at det opprettes et lovutvalg for å vurdere en ny IKT-sikkerhetslov,[41] men inntil videre ønsker regjeringen bruke andre virkemidler for å bidra til bedre digital sikkerhet i offentlig sektor.[42]

Vi mener det uansett er behov for bedre utredning før det innføres ny regulering som skal gjelde all offentlig forvaltning. Ny regulering kan gi samfunnsøkonomisk nytte, men det er behov for å se nærmere på innretning på reguleringen; [43] slik at den får tilstrekkelig helhetlig tilnærming, og er egnet til å danne utgangspunkt for en fremtidig harmonisering av regelverk.

---

[38] https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/?ch=4#kap10 Merk at denne referansen omhandler regulering av «IKT-sikkerhet».
[39] https://www.digdir.no/datadeling/veileder-digitaliseringsvennlig-regelverk/2856
[40] Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden*, kapittel 8.2.
[41] https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/?ch=5#kap15-7
[42] Ibid, kapittel 8.4.1.
[43] Samfunnsøkonomisk vurdering av anbefalinger fra IKT-sikkerhetsutvalget, kapittel 5.

En generell lov av denne typen bør være en lov om informasjonssikkerhet som legger opp til helhetlig arbeid for å styre risiko for oppgaver og tjenester i virksomhetene, og inkluderer digital sikkerhet.

Områder som har særlige behov bør skilles ut, slik at man kan gi særlige regler for disse områdene. Så langt det er mulig bør man likevel gjenbruke terminologi og vise til overordnet regelverk. Et eksempel er sikkerhetsloven; den gir en rekke særregler, men tar utgangspunkt i styring og kontroll i en helhetlig tilnærming i virksomhetene.

Det kan også være mulig å utforske regulering kun for statsforvaltningen, via egnet juridisk instrument, for eksempel instruks eller rundskriv. Man kan for eksempel stille tydeligere krav til hva som skal gjøres og til roller som skal ivareta det. De har gjort noe tilsvarende i Storbritannia gjennom innføringen av «Functional Standards».[44]

3.4 Anbefalinger

3.4.1 Utvikle felles referanseramme

Digitaliseringsdirektoratet anbefaler at det startes et arbeid for å utvikle en felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter.

Den kan inneholde sterke anbefalinger om:

- Struktur og innhold for styringsaktiviteter
- Basisnivåer med sikkerhetstiltak
- Felles tiltaksbank med sikkerhetstiltak

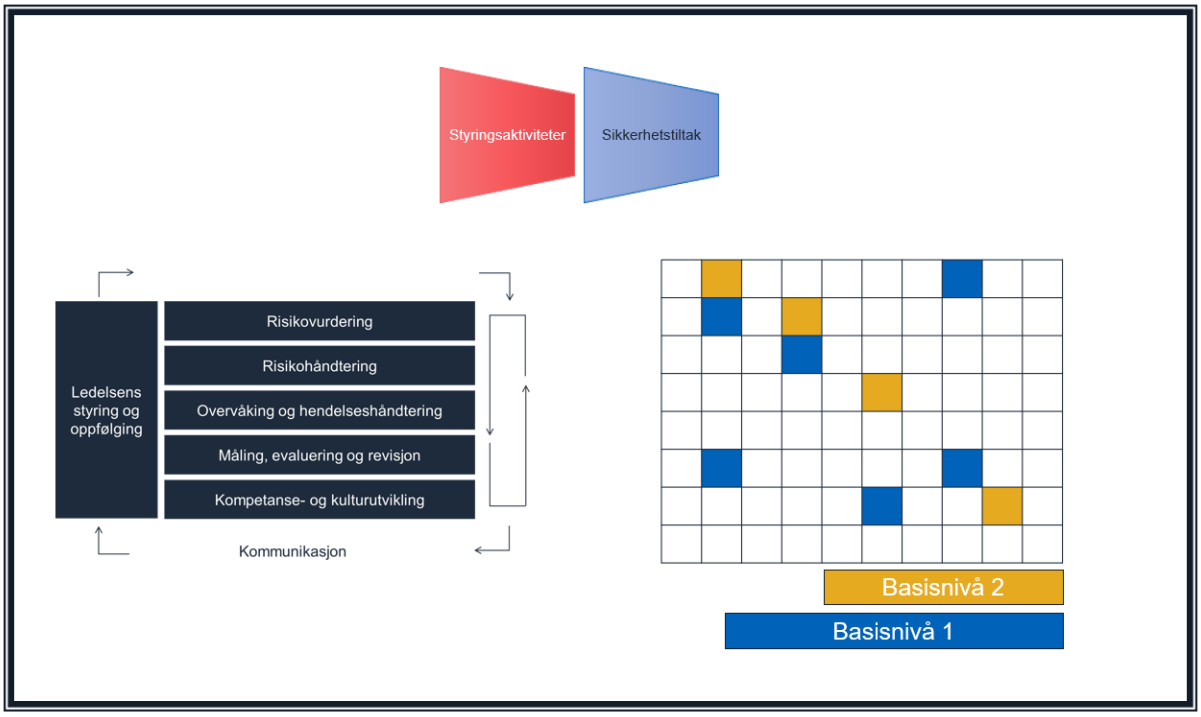
Veiledning om informasjonssikkerhet og digital sikkerhet bør så langt som mulig referere til elementer i felles referanseramme, slik at virksomhetene får et helhetlig og sammenhengende veiledningstilbud. Det samme gjelder for opplæring eller bevisstgjøringskampanjer for ledere og andre målgrupper.

Hvilke elementer som skal inngå i det som er felles, og hvordan anbefalinger og veildning skal tilrettelegges og utformes for brukerne må utvikles i samarbeid mellom flere aktører i forvaltningen, med involvering fra brukervirksomheter. Det kan ta tid å få god, helhetlig sammenheng i anbefalinger og veiledning. Det kan hende det må styres i en langsiktig utvikles i flere etapper.

For å lykkes med dette er vi også helt avhengig av at innholdet i felles referanseramme blir benyttet på tvers av forvaltningen. Det vil også bli viktig å utvikle tiltak for utbredelse og bevisstgjøring både før, under og etter lansering.

[44] UK government, *Government Functional Standard – GovS 007: Security*. Version 2.0, Sep 2021. https://www.gov.uk/government/collections/functional-standards

I et langsiktig perspektiv bør det arbeides med harmonisering av regelverk, og det bør være sterk styring fram mot god sammenheng i regelverk, anbefalinger og tilhørende veiledning. Det er summen av regelverk, anbefalinger og veiledning som kan gi virksomhetene gode rammebetingelser og hjelpemidler for arbeidet med informasjonssikkerhet.



Figur 10 - Felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter

Brukerorientering

I et arbeid med å utvikle god, helhetlig sammenheng i anbefalinger og veiledning blir det viktig å orientere seg rundt brukernes perspektiv.

Som vi ser av utfordringsbildet så opplever svært mange det som krevende å få til god styring og oppnå formålet med regelverkene som stiller krav til virksomhetene og deres ledelse. Virksomhetene bør få hjelp til å få de vesentligste tingene på plass på en måte som de er i stand til å forvalte.

Det er en del elementer alle virksomheter trenger i gjennomføring av styringsaktiviteter, spesielt vurdering og håndtering av risiko. Selv om virksomheter følger anbefalinger om styringsaktivitetene, og benytter eksempler fra veiledning, så må de utforme og tilpasse disse elementene selv. Noen av disse elementene kan utformes sentralt og gjøres tilgjengelig slik at virksomhetene kan bruke dem direkte, eller gjøre mindre tilpasninger til sitt behov.

Det er flere brukerrettede produkter og veiledning som kan utformes for å lette og effektivisere arbeidet med informasjonssikkerhet i virksomhetenes operative arbeid. Dette er et eksempel på dette:

Figur 11 – Virksomhetene finner svar på sentrale spørsmål på ett sted

En slik løype som er enkel å følge kan hjelpe virksomhetene å få grunnleggende sikkerhetstiltak på plass – noenlunde likt på tvers av hele forvaltningen. Det i seg selv er selvfølgelige ikke tilstrekkelig; men for mange virksomheter vil det være noe av det de kan starte med, samtidig som de bygger opp resten av styringsaktivitetene og utvikler kompetanse og modenhet i virksomheten.

Hvordan disse tingene skal utformes, og i hvor stor grad slik sentral veiledning skal integreres med krav eller anbefalinger i felles referanseramme (eller norm), på en måte som gjør det lett å bruke og gir gode resultater for virksomhetene, vil bli sentralt i et videre arbeid i samarbeid mellom ulike aktører.

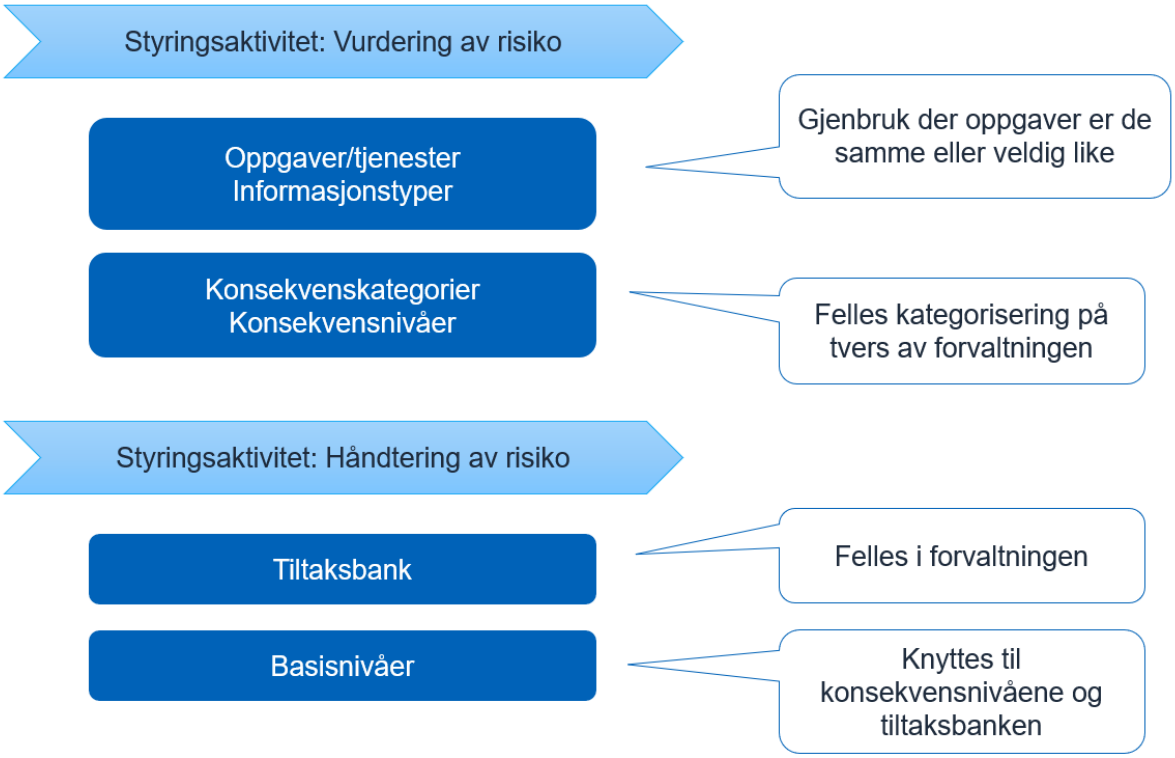
3.4.2 Utvikling og utprøving av mulige tiltak i forvaltningen

Digitaliseringsdirektoratet anbefaler at det startes et arbeid for å utvikle og prøve ut de mulige tiltakene som er beskrevet i dette notatet.

Dersom konseptene som skisseres i dette notatet skal ha full effekt, bør det tas sikte på at de etter hvert skal dekke hele forvaltningen. Under utvikling og utprøving vil det likevel være fornuftig å fokusere spesielt på å møte behovene til virksomheter med lav modenhet eller lite tilgang på nødvendige ressurser til arbeidet med informasjonssikkerhet. Kommunene har de samme eller svært likeartede oppgaver og tjenester, og det være naturlig å starte med noen av tiltakene der.

Det vil være mulig å starte arbeid med tiltak T2 Katalog med oppgaver/tjenester og informasjonstyper. Det er et mindre ressurskrevende tiltak som kan gi gevinst på kort sikt. Det kan utvikles av Digdir i samarbeid med KS og utvalgte kommuner. Det kan fungere som et supplement til eksisterende anbefalinger om styringsaktiviteter, uten å være avhengig av de andre mulige tiltakene.

De andre mulige tiltakene som skisseres i dette notatet er ressurskrevende tiltak som må ses i sammenheng, og det er ulike hensyn som må ivaretas. Vi vil være avhengige av å ha et langsiktig arbeid, hvor noen holder oversikt over helheten og styrer retningen mot et omforent målbilde.



Figur 12 - Felles elementer benyttes i gjennomføringen av styringsaktiviteter

3.4.3 Samarbeid

Digitaliseringsdirektoratet anbefaler at nye tiltak for forvaltningen utvikles i samarbeid mellom de sentrale myndighetsorganene som veileder virksomhetene om informasjonssikkerhet, digital sikkerhet og styring og kontroll.

Det bør være aktiv involvering av, og samarbeid med, et representativt utvalg virksomheter fra ulike forvaltningsnivåer. Det bør legges særlig vekt på å møte behovene hos små, mellomstore eller mindre modne virksomheter. Virksomheter med sentrale roller i felles økosystem for nasjonal digital samhandling, for eksempel forvaltere av felleskomponenter, bør tas med i arbeidet.

På lang sikt kommer det til å være behov for aktører som samarbeider og koordinerer i helheten. Det bør legges vekt på å utvikle gode måter å gjøre dette på.

3.4.4 Koordinering på departementsnivå

Kommunal- og distriktsdepartementet bør sørge for forpliktende samarbeid mellom de myndighetsaktørene som skal involveres og nødvendig koordinering på departementsnivå. Det bør inkludere samarbeid med Justis- og beredskapsdepartementet, som har ansvaret for nasjonal digital sikkerhet, samfunnssikkerhet og beredskap, og lov om nasjonal sikkerhet.

3.5 Mulige gevinster

Videre arbeid i denne retningen, med disse mulige tiltakene, kan blant annet bidra til:

- Mer kostnadseffektivt arbeid med informasjonssikkerhet
- Styrket grunnleggende sikkerhet på tvers av forvaltningen
- Mer effektivt grensesnitt mot tjenesteleverandørmarkedet
- Enklere å utvikle sammenhengende tjenester og dele data
- Tydeligere rammer for informasjonssikkerhet i tjenesteutvikling i felles økosystem

3.6 Vurdering av effekt

Her følger en veldig enkel, foreløpig kobling mellom mulige tiltak (T) og de ulike problemene (P). Denne oversikten er kun en skisse, for å få et innblikk i hvilke effekter mulige tiltak kan få.

Ressursbehov for utvikling, utprøving og implementering av tiltakene er ikke vurdert.

T1 Felles referanseramme

Sterke anbefalinger om:

- Struktur og innhold for styringsaktiviteter
- Basisnivåer med sikkerhetstiltak
- Felles tiltaksbank med sikkerhetstiltak

Kan ha effekt på

- P1 Svake eller manglende styringsaktiviteter
- P2 Mangler grunnleggende sikkerhetstiltak
- P5 Mangelfull forvaltning av sikkerhetstiltak
- P6 Arbeidet er kompetansekrevende
- P7 Arbeidet er ressurskrevende
- P8 Krevende å undersøke omfang av sikkerhetstiltak
- P10 Utfordrende å bruke og følge opp tjenesteleverandører
- P11 Manglende tillit mellom offentlige virksomheter kan være hinder for digitalisering
- P12 Vanskelig å få til helhetlig tilnærming i virksomhetene

T2 Katalog med oppgaver/tjenester og informasjonstyper

Kan bidra til

- Å redusere omfanget av det som må gjøres i hver enkelt virksomhet
- Å effektivisere arbeidet med informasjonssikkerhet
- Å gi mer like vurderinger og prioriteringer

Kan ha effekt på

- P3 Utilstrekkelig oversikt over informasjonsbehandlingen
- P7 Arbeidet er ressurskrevende

T3 Basisnivåer med sikkerhetstiltak

Kan bidra til

- Å gi et godt utgangspunkt for virksomhetenes valg av sikkerhetstiltak for oppgaver, tjenester eller informasjonssystemer
- Å effektivisere arbeidet i virksomhetene

- Å gi et mer felles, grunnleggende sikkerhetsnivå på tvers av forvaltningen

Kan ha effekt på

- P2 Mangler grunnleggende sikkerhetstiltak
- P4 Må til en viss grad gjøre de samme vurderingene
- P5 Mangelfull forvaltning av sikkerhetstiltak
- P6 Arbeidet er kompetansekrevende
- P7 Arbeidet er ressurskrevende

T4 Felles tiltaksbank

Kan bidra til

- Å gjøre det mulig å lage basisnivåer som uttrekk fra tiltaksbanken
- Å få et samlingspunkt for veiledning om sikkerhetstiltak
- Å øke evnen til samarbeid mellom virksomheter
- Å få en felles kilde for tilsynsmyndigheter

Kan ha effekt på

- P2 Mangler grunnleggende sikkerhetstiltak
- P5 Mangelfull forvaltning av sikkerhetstiltak
- 7 Arbeidet er ressurskrevende

T5 Kategorier og nivåer av konsekvenser

Kan bidra til

- Tilordning av basisnivåer til oppgaver/tjenester eller informasjonssystemer
- Å øke kvaliteten på vurderinger
- Å få mer like resultater
- At disse tingene er gjenkjennbart på tvers av virksomheter og øke evnen til samarbeid og samstyring av risiko

Kan ha effekt på

- P1 Svake eller manglende styringsaktiviteter
- P3 Utilstrekkelig oversikt over informasjonsbehandlingen
- P4 Må til en viss grad gjøre de samme vurderingene
- P6 Arbeidet er kompetansekrevend
- P11 Manglende tillit mellom offentlige virksomheter kan være hinder for digitalisering

T6 Spesialtilpassede basisnivåer med sikkerhetstiltak

Kan ha effekt på

- P2 Mangler grunnleggende sikkerhetstiltak
- P4 Må til en viss grad gjøre de samme vurderingene
- P5 Mangelfull forvaltning av sikkerhetstiltak
- P6 Arbeidet er kompetansekrevende
- P7 Arbeidet er ressurskrevende

T7 Ny lov om informasjonssikkerhet for offentlig forvaltning

Kan ha effekt på

- P1 Svake eller manglende styringsaktiviteter
- P11 Manglende tillit mellom offentlige virksomheter kan være hinder for digitalisering
- P12 Vanskelig å få til helhetlig tilnærming i virksomhetene
- P13 Mangelfull og fragmentert regulering

God sammenheng med personvern

Kan bidra til:

- At det blir enklere å kombinere arbeidet med informasjonssikkerhet og personvern for oppgaver og tjenester som behandler personopplysninger
- Å styrke evnen til å ivareta personvern

God sammenheng med offentlige anskaffelser

Kan bidra til:

- Enklere og mer effektive anskaffelser
- Bedre sikkerhet i tjenester som anskaffes

3.7 Økonomiske og administrative konsekvenser

Dette notatet beskriver utfordringer og peker på muligheter for utvikling av informasjonssikkerhetsarbeidet. De mulige tiltakene som beskrives kan bidra til bedre ressursbruk og et mer effektivt arbeid med informasjonssikkerhet i forvaltningen, samt andre positive ringvirkninger.

Økonomiske og administrative konsekvenser vil avhenge av hvilke konsepter og mulige tiltak man velger å utvikle og prøve ut, og hvordan disse utformes. I forbindelse med videre arbeid vil det bli nødvendig å utrede dette nærmere.

Økonomiske og administrative konsekvenser er derfor ikke utredet og beskrevet i dette notatet.

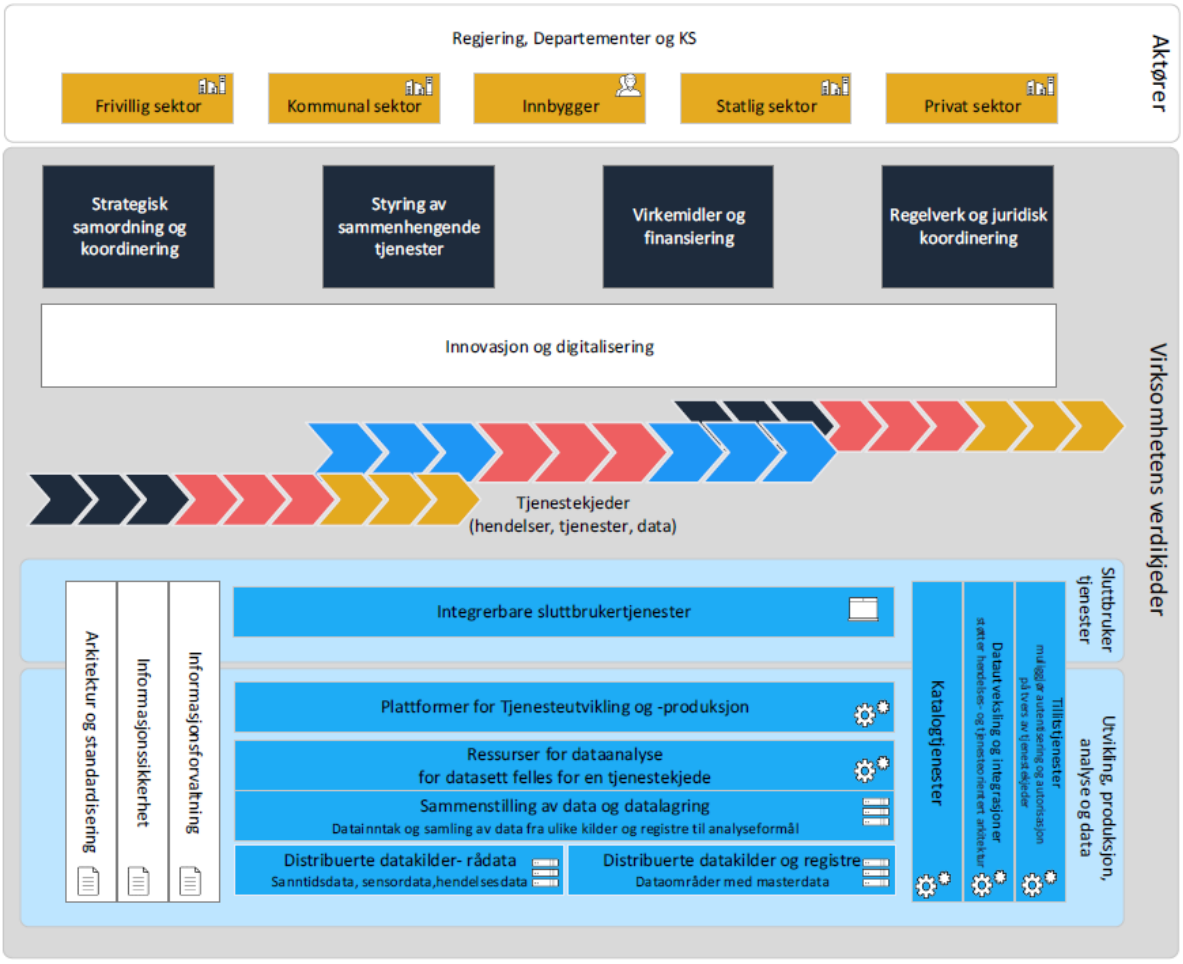
4 Vedlegg

4.1 Vedlegg 1 – Viktige sammenhenger

4.1.1 Digitale tjenester og felles økosystem

Digitale tjenester er en viktig del av oppgavene og tjenestene som leveres av offentlig forvaltning. Det er tjenester hvor informasjonssikkerhet, og spesielt digital sikkerhet, er helt nødvendig for å være i stand til å levere tjenester nå og i framtiden.

Kommuner, fylkeskommuner og statlige virksomheter utvikle brukerrettede, sammenhengende og effektive digitale tjenester. De bygger sine tjenester med utgangspunkt i et felles digitalt økosystem for samhandling[45].



Figur 13 - Modell av felles økosystem for nasjonal digital samhandling og tjenesteutvikling

Dette krever godt samarbeid mellom forvaltningsnivåene om juridiske, organisatoriske, semantiske og tekniske problemstillinger. Felles økosystem skal bidra til at offentlige tjenester oppleves som sammenhengende for brukerne uansett hvilken offentlig virksomhet som tilbyr dem.

Felles utfordringer på informasjonssikkerhetsområdet har betydning for digitale tjenester, og for tjenestekjeder i felles økosystem. Det har allerede vært gjort erfaringer av at en hendelse

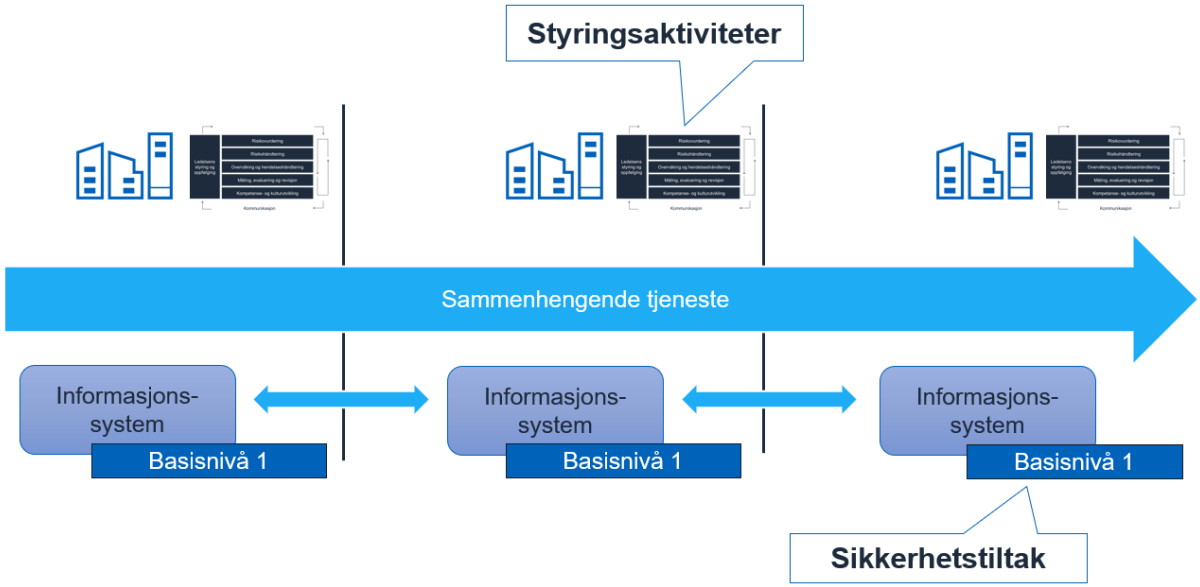
[45] https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/?ch=6

i en virksomhet kan få alvorlige konsekvenser for tjenester hos andre virksomheter. Det svakeste leddet kan bryte hele tjenestekjeden.

Virksomheter som sammen leverer sammenhengende tjenester må håndtere risiko i tjenestekjeden, og det er aktuelt å se på hvordan man kan samarbeide om informasjonssikkerhetsarbeidet.

Digdir gjennomførte i 2021 en kartlegging av krav og anbefalinger rettet mot digitaliseringsarbeid i offentlig forvaltning. Et av funnene var at ansatte i offentlig forvaltning som arbeider med digitalisering er positive til at det blir stilt krav innen digitalisering, men ønsker at det skal bli enklere å gjennomføre kravene i praksis[46].

Rammevilkårene for utvikling av tjenester i felles økosystem bør vektlegge evne til samarbeid og samstyring, og bidra til gjensidig tillit mellom tjenesteeiere som er avhengige av hverandre. Virksomhetene er avhengig av gode rammebetingelser for arbeidet med informasjonssikkerhet, og det bør være lett å gjøre rett.



Figur 14 - Virksomheter har felles tilnærming til informasjonssikkerhet

4.1.2 Anskaffelser og skytjenester

Offentlige virksomheter må styre risiko for sine oppgaver og tjenester, dette gjelder også når de understøttes og gjennomføres ved bruk av anskaffelser, inkludert tjenester som inngår i informasjonsbehandlingen.

Virksomhetene har selv ansvar for å vurdere behov for informasjonssikkerhet i sine oppgaver og tjenester, inkludert spesifikke sikkerhetstiltak som er nødvendige for å bidra til å håndtere risiko. Deler av disse behovene må nødvendigvis videreføres som krav til leverandører av tjenester som innebærer informasjonsbehandling, inkludert digitale tjenester.

[46] Skate AU sak 59/2021

Det er åpenbart at virksomhetene må sørge for at informasjonssikkerhet er ivaretatt hos tjenesteleverandører, og at krav til dette må inngå i avtaler om tjenesteleveranser. Det kan likevel være krevende å vite hva det innebærer og hvordan det kan gjøres.

Det kan for eksempel stilles krav til:

- Styringsaktiviteter hos leverandør
- Samhandling i styringsaktiviteter mellom kunde og leverandør
    - F.eks. knyttet til vurdering av risiko eller håndtering av hendelser
- Innsyn i dokumentasjon som produseres av styringsaktivitetene hos leverandør
    - F.eks. føringene som gjelder hos leverandøren og hvordan disse følges opp, inkludert resultater fra virksomhetsledelsens gjennomgang, eller informasjon om ytelse på sikkerhetstiltak og oppfølging av hendelser
- Overordnede krav til sikkerhetsnivå
    - F.eks. kategorier av sikkerhetstiltak og omfang og styrke på disse
- Krav om spesifikke sikkerhetstiltak
- Krav om tillitsinformasjon
    - Sertifiseringer
    - Rapporter attestert av tredjeparter (f.eks. SOC 2)[47]

EU Cloud Services Scheme

Noen av punktene på listen over inngår i EUs «Cloud Services Scheme» (EUCS).[48]

Det er kandidat til å bli en sertifiseringsordning: “cybersecurity certification scheme for cloud services”. Bruken er begrenset til visse typer IT-tjenester («a specific category of ICT services»).

Leverandører av skytjenester innenfor EU kan i fremtiden komme til å sertifisere tjenestene sine i henhold til «assurance levels». Kravene som skal oppfylles for et «assurance level» inneholder flere ulike ting, både kvalifikasjonskrav for leverandøren og spesifikke sikkerhetstiltak som skal være på plass i tjenesteleveransen.

Sikkerhetstiltakene er hentet fra ulike steder, og er delvis basert på tidligere arbeid i Tyskland og Frankrike. De er ikke hentet fra én tiltaksbank, og de er ikke direkte knyttet til regelverk som stiller de samme kravene til virksomhetenes (kundenes) oppgaver og tjenester.

Kravene og tillitsinformasjon basert på disse kravene, inkludert en form for verifisering av om de er oppfylt, benyttes av de som skal kjøpe disse tjenestene, og vi må regne med at tanken er at «assurance level» sier noe om tilliten man kan ha til at tjenestene oppfyller kravene og kan benyttes til de oppgaver og tjenester de er tiltenkt for.

Samordning av kravstilling fra offentlig sektor til leverandørmarkedet

Det vil være fordeler med større grad av felles kravstilling til leverandørmarkedet.

Det er flere problemstillinger som er aktuelle å se nærmere på i den forbindelse:

- Nytten av større grad av samkjørt kravstilling fra offentlige virksomheter til leverandørmarkedet – inkludert effektiviseringsgevinst for begge parter.

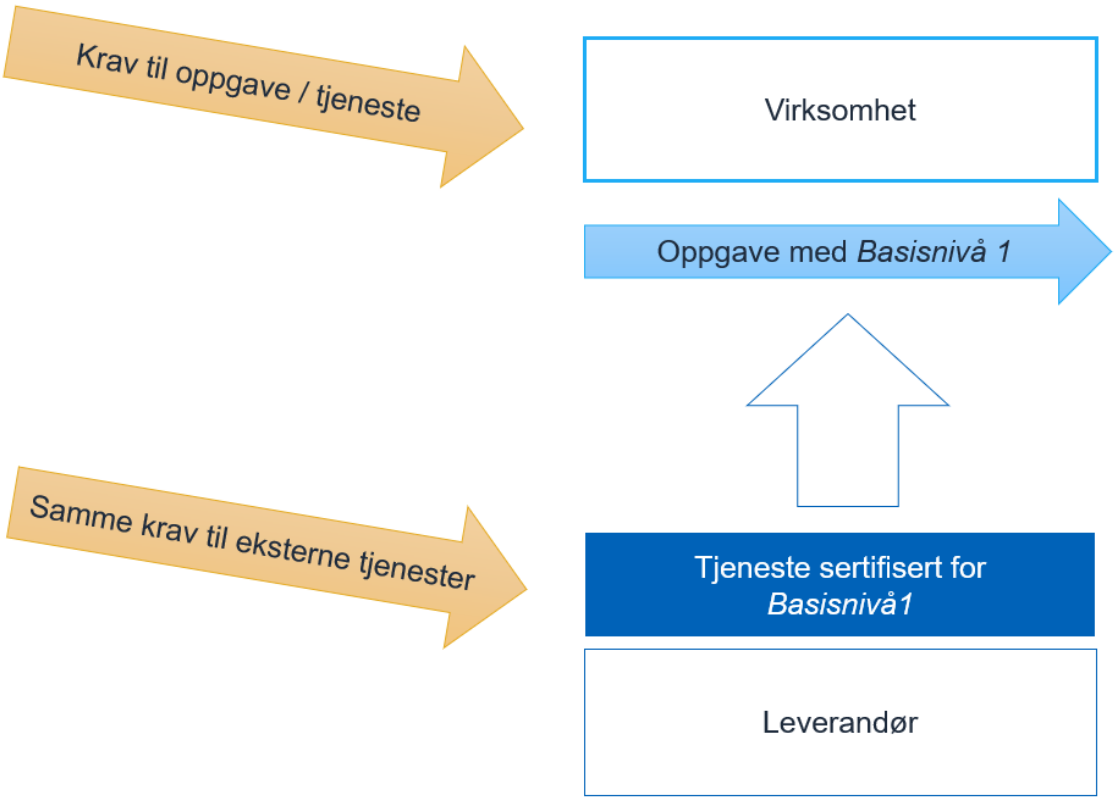
---

[47] https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
[48] EU (ENISA), *EUCS – Cloud Services Scheme*, Dec 2020. https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

- Nytten av leverandører av konsulenttjenester innen styring av informasjonssikkerhet tar utgangspunkt i felles referanseramme og tydelige anbefalinger om hva virksomhetene bør ha på plass
- Nytten av basisnivåer og felles tiltaksbank for offentlig forvaltning i forbindelse med anskaffelser, spesielt kjøp av skytjenester.
- Hvilke muligheter Norge har for nasjonale særkrav i et internasjonalt marked, hvor leverandørene allerede har tilpasset tjenestene til andre kravsett og sertifiseringsordninger.
- Hvilken nytte Norge har av å samordne nasjonale krav mot internasjonale krav og tiltaksbanker.

Samme krav til oppgaver og tjenester uavhengig av tjenestekjøp

Slik EUCS-ordningen er skissert i dag kan den føre til en situasjon hvor visse krav gjelder for visse typer eksterne tjenester. Dersom en offentlig virksomhet organiserer sine oppgaver og tjenester på annen måte, for eksempel ved å ivareta tilsvarende IKT-tjenester selv, så gjelder ikke de samme kravene for disse.



Figur 15 - Krav til offentlige tjenester og eksterne skytjenester

Det kan hende det er fornuftig at anbefalinger og krav rettes til de offentlige virksomhetene og oppgavene og tjenestene de skal levere. De relevante delene av kravene må ivaretas av tjenesteleverandører, alt etter innholdet i tjenesteleveransen. En sertifiseringsordning for skytjenester kan for eksempel bygges på de samme basisnivåene som er anbefalt å benytte

for offentlige oppgaver og tjenester. Det kan organiseres slik at det blir tydelig ansvarsdeling mellom offentlig virksomhet (kunde) og leverandør.

4.1.3 Personvern

Det er mange oppgaver og tjenester i offentlig forvaltning som behandler personopplysninger, og informasjonssikkerhet er viktig for å ivareta fysiske personers rettigheter og friheter når det behandles opplysninger om dem.

Det er mye å hente ved å samkjøre arbeidet med informasjonssikkerhet og personvern for de oppgavene og tjenestene det gjelder.

Styringsaktiviteter kan ha samme struktur uavhengig av hva som skal styres[49]. Det vil likevel være ulike metoder i bruk, og forskjellige måter å gjennomføre deler av aktivitetene på.

En felles tiltaksbank kan inneholde både sikkerhetstiltak og personverntiltak. Det kan gjøre det enklere for virksomhetene å kombinere arbeidet med informasjonssikkerhet og personvern for oppgaver og tjenester som behandler personopplysninger.

Felles fundament for informasjonssikkerhet og personvern

Å legge til rette for helhetlig arbeid og sørge for at anbefalinger og veiledning fra myndigheter henger godt sammen kan bidra til et godt arbeid med informasjonssikkerhet og personvern, og at man unngå unødvendig og kostnadskrevende duplisering av ressursbruk i virksomhetene.

Et felles fundament gir virksomhetene kostnadseffektive, fleksible og konsistente måter å håndtere informasjonssikkerhets- og personvernrisikoer for oppgaver og tjenester.

Personverntiltak

Personverntiltak er tiltak en virksomhet etablerer for å for å sikre etterlevelse av personvernregelverk og håndtere personvernrisikoer.

«Basisnivå Personvern» kan lages som et sett med personverntiltak som virksomhetene kan benytte som utgangspunkt for valg av tiltak for å ivareta personvern i oppgaver og tjenester. Etablering av tiltakene i et slikt basisnivå vil ikke innebære at alle virksomhetens forpliktelser er ivaretatt. Virksomhetene må fortsatt gjøre egne vurderinger.

Eksempler på personverntiltak kan være:

- Informasjon om behandlingen til de man behandler personopplysninger om
- Rutine for samtykke til behandling av personopplysninger
- Rutine for håndtering av klager på behandling av personopplysninger
- De-identifisering (anonymisering) av personopplysninger
- Databehandleravtale

Forskjell på basisnivå med sikkerhetstiltak og basisnivå personvern

Sikkerhetstiltak som inngår i basisnivå med sikkerhetstiltak brukes for å håndtere risiko knyttet til tap av konfidensialitet, integritet og tilgjengelighet generelt – alle informasjonssystemer, inkludert alle typer informasjon og hensyn som skal ivaretas.

[49] https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

Personvernrisiko oppstår både ved tiltenkt behandling av personopplysninger og ved tap av konfidensialitet, integritet og tilgjengelighet for personopplysninger. Virksomheter som behandler personopplysninger, må derfor samordne arbeidet med informasjonssikkerhet og personvern og koordinere aktiviteter relatert til valg og etablering av sikkerhets- og personverntiltak.

Tiltak som inngår i basisnivå med personverntiltak er viktige for å ivareta personvern. De er ikke nødvendigvis rettet inn mot å forebygge, oppdage og håndtere hendelser knyttet til tap av konfidensialitet, integritet og tilgjengelighet.

Kombinasjonen av et basisnivå med sikkerhetstiltak og basisnivå personvern skal gi et godt utgangspunkt for håndtering av risiko på disse områdene for oppgaver og tjenester som behandler personopplysninger.

4.2 Vedlegg 2 – Begreper og konsepter

Dettee vedlegget gir en beskrivelse av hvordan en del sentrale begreper benyttes i dette notatet. Den inneholder også en mer utdypende beskrivelse av noen av konseptene som benyttes i forbindelse med mulige tiltak.

For en oversikt over hva arbeidet med informasjonssikkerhet i offentlige virksomheter handler om, se også:

Helhetlig styring og kontroll av informasjonssikkerhet, [50] som er utarbeidet av Digdir, NSM og DFØ, med bidrag fra KS og Datatilsynet.

Miniveileder om oppfølging av informasjonssikkerhet i styringsdialogen, [51] som er utarbeidet av DFØ, Digdir og NSM.

4.2.1 Oppgaver og tjenester, informasjonsbehandling og informasjonssystemer

Oppgaver og tjenester

Når dette notatet nevner oppgaver og tjenester så menes de oppgavene og tjenestene som offentlige virksomheter har ansvaret for.

Det er de primære oppgavene de er satt til å utføre eller tjenester de leverer. For eksempel

- Administrere dagpengeordning
- Saksbehandling i barnevernet
- Føre tilsyn
- Utføre operasjoner på et sykehus

Offentlige virksomheter har også en rekke støtteoppgaver, som økonomistyring, personalforvaltning, anskaffelser mv. hvor informasjonsbehandling er viktig.

Informasjonsbehandling

[50] https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284
[51] https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/

Informasjonsbehandling er viktig i stort sett alle oppgaver og tjenester i offentlig forvaltning – fra saksbehandling i et departement til vanntilførsel fra kommunale vannverk. Det er enten selve kjernen i arbeidet eller viktig støtte til oppgavene som utføres.

> *Forvaltninga kan samanliknast med ein informasjonsfabrikk der råvara er informasjon, og resultatet av arbeidet er meir informasjon. Eit særdrag ved ved denne «fabrikken» er at han er styrt av regelverk i form av lover og forskrifter.*[52]

Informasjon behandles av både mennesker og digitale systemer. Det inkluderer halv- eller helautomatisk behandling av digitale data, og data som kun brukes maskinelt, og som ikke nødvendigvis skal leses og forstås av mennesker.

Dersom informasjonsbehandlingen ikke fungerer slik den bør, vil det få konsekvenser for oppgaver og tjenester, måloppnåelse, effektivitet og etterlevelse av lover og regler. Styring av informasjonssikkerhet er derfor en viktig del av den risikobaserte styringen av en offentlig virksomhet. Informasjonssikkerhet for de digitale tjenestene er en viktig del av dette.

Informasjonssystem

I dette notatet benyttes «informasjonssystem» i omtrent samme betydningen som ligger til grunn for lov om nasjonal sikkerhet (sikkerhetsloven):[53]

Med begrepet informasjonssystem menes systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker.

Informasjonssystem skal i sikkerhetsloven forstand forstås vidt. Begrepet omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer.

Det fremgår ikke tydelig av denne beskrivelsen at systemet benyttes til informasjonsbehandling. Det kan derfor være nyttig å se på hva NIST benytter[54] for føderal forvaltning i USA:

Information system: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information resources: Information and related resources, such as personnel, equipment, funds, and information technology.

En beskrivelse basert på de nevnte kildene kan derfor være:

Et informasjonssystem er et avgrenset sett med ressurser som benyttes til informasjonsbehandling. Det består av elementer som mennesker, teknologi, informasjon og prosesser. Den digitale teknologien som inngår i systemet kan være IKT-systemer og komponenter som disse er bygget opp av.

---

[52] Informasjonsforvaltning i offentleg sektor, Rapport 2013:10, Difi
[53] NOU 2016:19 *Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. S. 262. https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/?ch=1
[54] https://csrc.nist.gov/glossary/term/information_system

Informasjonsbehandling er et vidt begrep som inkluderer bruk av automatiserte digitale systemer, også de som styrer fysiske prosesser.

Dette til forskjell fra en bruk av begrepet hvor det i stor grad begrenser seg til teknologiske elementer, slik som i NIS-direktivet[55] eller den gamle sikkerhetsloven.

4.2.2 Informasjonssikkerhet og digital sikkerhet

Dette er en kort beskrivelse av hvordan disse sentrale begrepene benyttes i dette notatet.

Arbeidet med informasjonssikkerhet i en virksomhet handler om å styre risiko ved bruk av informasjonssystemer til å utføre oppgaver og levere tjenester. Det handler om å sikre all informasjonsbehandling som inngår i oppgaver og tjenester, eller understøtter dem.

Det betyr å sikre at informasjon i alle former

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Det handler om å sikre informasjonssystemene som brukes – inkludert alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i informasjonssystemene.

Informasjonssikkerhetsbrudd kan forekomme uten at digitale elementer er involvert. For eksempel konfidensialitetsbrudd som følge av at en ansatt bryter taushetsplikten muntlig.

Disse definisjonene kan bidra til å forklare hva informasjonssikkerhet handler om:

- NIST IR 7298: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- ISO/IEC 27000:2018: preservation of confidentiality, integrity and availability of information

Digital sikkerhet, cybersikkerhet og IKT-sikkerhet

I mange sammenhenger benyttes digital sikkerhet, cybersikkerhet og IKT-sikkerhet synonymt med informasjonssikkerhet. I andre sammenhenger menes en del av arbeidet med informasjonssikkerhet – for eksempel sikring av den digitale teknologien som benyttes.

Det handler ofte bare om forskjellige perspektiver på det som er nesten det samme.

Det kan likevel være viktig å være bevisst på tilfeller

- hvor bruken av disse begrepene begrenser seg til å sikre teknologien som benyttes
- hvor bruken av disse begrepene begrenser seg til beskyttelse mot menneskestyrte angrep

Dette notatet benyttes «digital sikkerhet» i tilfeller hvor det i hovedsak handler om sikring av de digitale elementene, altså IKT-systemer og nettverk. I stortingsmelding om samfunnssikkerhet[56] beskrives det slik:

[55] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Article 4

[56] Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden*, kapittel 8.

Digital sikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. Brukes synonymt med begrepene IKT-sikkerhet og cybersikkerhet.

Digital sikkerhet er uansett en stor og svært viktig del av arbeidet med informasjonssikkerhet.

4.2.3 Styringsaktiviteter og sikkerhetstiltak

Styringsaktiviteter er et sett med aktiviteter som utføres jevnlig og systematisk rundt omkring i virksomheten. Den ordinære ledelsen har hånden på rattet og eier disse aktivitetene. Styringsaktivitetene er kjernen i styringssystemet, og sammen med sikkerhetstiltakene sørger de for god informasjonssikkerhet for virksomhetens oppgaver og tjenester.

Eksempler på styringsaktiviteter:

- Vurdering av risiko
- Måling, evaluering og revisjon

Du kan lese mer om styringsaktiviteter på Digdirs nettsider.

Sikkerhetstiltak er en viktig måte å håndtere risiko på.

Risiko kan som kjent håndteres på ulike måter. Risiko kan unngås ved å ikke utføre oppgaver som er opphavet til risiko, eller ved å utføre oppgaver og levere tjenester på andre måter. Risiko kan deles med andre, for eksempel gjennom en forsikringsavtale. Risiko må også ofte aksepteres for å få utført nødvendige oppgaver.

Innen informasjonssikkerhet er det svært viktig å etablere og forvalte varige tiltak som reduserer risiko, slik at virksomheten kan utføre sine oppgaver og levere tjenester på en god måte. Slike varige tiltak reduserer risiko ved å redusere konsekvenser av uønskede hendelser eller sannsynligheten for at de inntreffer. Det er disse varige tiltakene vi som regel omtaler som sikkerhetstiltak.

Eksempler på sikkerhetstiltak:

- Administrasjon av brukerkontoer
- Identifisering og autentisering av bruker for tilgang til system
- Kontroll med adgang til lokaler
- Egnethetsvurdering av ansatte til spesielle stillinger
- Avtale med tjenesteleverandør

Du kan lese mer om sikkerhetstiltak på Digdirs nettsider.

Figur 16 - Styringsaktiviteter og sikkerhetstiltak

4.2.4 Basisnivåer

Det er kan være utfordrende for virksomheter å velge sikkerhetstiltak som kan sikre oppgaver og tjenester og gjøre dem i stand til å håndtere risiko for informasjonsbehandlingen.

Vi kan se for oss to ulike tilnærminger i utvelgelsen av sikkerhetstiltak:

- Virksomhetsgenerert utvalg
- Basisnivåer

Førstnevnte er den som er beskrevet i Digdirs veiledning om styring av informasjonssikkerhet. Virksomheten henter sikkerhetstiltak fra ulike kilder eller utformer dem helt selv, og lager seg et sett med grunnleggende sikkerhetstiltak på tvers av sine oppgaver og tjenester som kalles «fellessikring». Oppgaver, tjenester eller informasjonssystemer med særskilte behov får også «tilleggssikring». Hensikten med denne måten å organisere det på er å få et effektivt arbeid med vurdering og håndtering av risiko, og kostnadseffektiv forvaltning av sikkerhetstiltak.

Den andre tilnærmingen tar utgangspunkt i basisnivåer. Det er sett med sikkerhetstiltak, satt sammen for å imøtekomme generelle, grunnleggende sikkerhetsbehov, og som gjøres tilgjengelig for virksomheters bruk. Disse to tilnærmingene kan kombineres, ved at basisnivåer benyttes som utgangspunkt for fremgangsmåten som er beskrevet i Digdirs veiledning. Resten av denne beskrivelsen handler om mulig bruk av basisnivå-konseptet i Norge, og vi går ikke nærmere inn på tilnærmingen med virksomhetsgenerert utvalg.

Grunnleggende sikkerhetstiltak

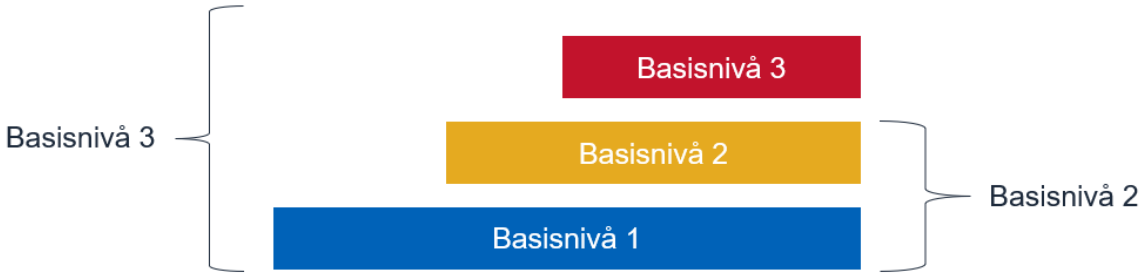
Grunnleggende sikkerhetstiltak kan samles i et eller flere basisnivåer. Et basisnivå er et sett med sikkerhetstiltak hentet fra en felles tiltaksbank. Hensikten med et slikt basisnivå er å gi

et godt utgangspunkt i prosessen med å velge sikkerhetstiltak. Bruken av basisnivåer kan også bidra til å gi et styrket og mer felles grunnleggende sikkerhetsnivå på tvers av forvaltningen.

Bruk av begrepet basisnivå er bevisst. Sikkerhetstiltakene i basisnivåer er utgangspunkt for virksomhetens valg og tilpasning av sikkerhetstiltak. Omfanget av sikkerhetstiltak skal korrespondere med de mulige konsekvensene informasjonssikkerhetsbrudd kan få for virksomhetens leveranser, økonomi, ansatte, innbyggere, andre virksomheter, samfunnsfunksjoner eller nasjonal sikkerhet.

Nivåer

Det kan lages to eller tre basisnivåer som bygger på hverandre.



Figur 17 - Basisnivåer med sikkerhetstiltak

- Basisnivå 1
  - Grunnleggende sikkerhetstiltak som vil være egnet for alle oppgaver og tjenester
- Basisnivå 2
  - Inneholder alle sikkerhetstiltakene i Basisnivå 1, men er utvidet med flere sikkerhetstiltak
- Basisnivå 3
  - Inneholder alle sikkerhetstiltakene i Basisnivå 2, men er utvidet med flere sikkerhetstiltak

Sammenheng med konsekvensnivåer

Basisnivåene kan korrespondere med kategorier som oppgaver, tjenester eller informasjonssystemer er sortert i, basert på hvor stor konsekvensene kan bli ved informasjonssikkerhetsbrudd.

Ordinær kategori benytter Basisnivå 1. Kategori for «medium» benytter Basisnivå 2. Kategori for «høy» benytter Basisnivå 3. Sistnevnte kan for eksempel være felleskomponenter og liknende som mange andre er helt avhengige av, eller som er viktige for kritiske samfunnsfunksjoner.

Tilordning

I forbindelse med utvikling av bruk av basisnivå-konseptet i Norge må man se på hva basisnivåer skal tilordnes til. De kan for eksempel tilordnes til:

- Oppgaver og tjenester
- Informasjonssystemer
- Virksomheter (som utgangspunkt for oppbygging av «fellessikring»)

Omfang

Det vil være viktig å treffe godt på innhold og omfang i basisnivåene. Det er spesielt viktig at det grunnleggende nivået ikke blir for omfangsrikt. Det bør legges vekt på de grunnleggende tingene, og tilstrekkelig informasjonssikkerhet, uten å bli kostnadsdrivende; eller at man dreier fokuset i virksomhetene fra god styring av risiko til å kun handle om å få på plass sikkerhetstiltak.

Tilpasning

Virksomheter benytter styringsaktiviteter for å vurdere og håndtere risiko, og veiledning om tilpasning av basisnivåer, til å sørge for egnede sikkerhetstiltak for sine oppgaver, tjenester og informasjonssystemer.

Det finnes ikke ett enkelt sett med sikkerhetstiltak som dekker alle behov i alle oppgaver og tjenester i enhver mulig situasjon. Å velge de mest passende sikkerhetstiltakene for å bidra til tilstrekkelig håndtering av risiko, krever god forståelse av virksomhetens oppdrag, prioriteringer, oppgaver og tjenester, hvilken betydning disse har, og miljøene hvor informasjonsbehandlingen foregår. Med denne forståelsen kan virksomheter oppnå tilstrekkelig informasjonssikkerhet på en kostnads- og ressurseffektiv måte.

Virksomheter tilpasser basisnivået ut fra flere faktorer, blant annet:

- Behov i oppgaver og tjenester
- Regelverk, inkludert sektorspesifikke krav
- Kunnskap om trusler
- Teknologi som benyttes
- Virksomhetens forutsetninger og begrensninger
- Ny kunnskap om god praksis

Tilpasning vil også kunne påvirkes av andre faktorer. Beslutninger må ta hensyn til andre risiko-relaterte problemer som virksomheten håndterer, kostnader, og tilgang på ressurser. Det vil være tilfeller hvor et sikkerhetstiltak rett og slett ikke er relevant, for eksempel fordi det angår teknologi som ikke er i bruk. Sikkerhetstiltak fjernes likevel ikke uvilkårlig fra basisnivået. Det må forventes at tilpasningsbeslutninger er forsvarlige, basert på virksomhetens oppdrag og behov, og velbegrunnede og risikobaserte beslutninger. Fjerning av sikkerhetstiltak, og begrunnelsen for dette, bør dokumenteres og godkjennes av ansvarlig risikoeier.

Forvaltning av basisnivåer

Sikkerhetstiltak som inngår i basisnivåer må evalueres jevnlig og oppdateres basert på erfaring med bruken av dem, nytt eller oppdatert regelverk, retningslinjer og standarder, tilgjengelighet og bruk av ny teknologi, og nye trusler og angrep. Vi må forvente at sikkerhetstiltak som inngår i basisnivåer vil endres over tid, etter hvert som sikkerhetstiltak tas ut, oppdateres og legges til. I tillegg til behovet for å gjøre endringer, er det også et behov

for stabilitet. Endringer i et basisnivå bør gjøres gjennom en åpen og offentlig prosess for å få tilbakemelding fra offentlig og privat sektor, og for å bygge konsensus omkring endringene i basisnivåene.

4.2.5 Spesialtilpassede basisnivåer

Spesialtilpassede basisnivåer kan utvikles med utgangspunkt i et generelt basisnivå.

Ved å bygge på de generelle basisnivåene, og hente sikkerhetstiltak fra felles tiltaksbank, kan det lages spesialtilpassede basisnivåer. Ulike interessenter kan utvikle dem for sine behov, eller gå sammen om å utvikle dem for spesielle bruksområder.

I visse situasjoner kan det være fordelaktig for virksomheter å tilpasse et generelt basisnivå for å utvikle et sett med sikkerhetstiltak for virksomheter med liknende oppgaver og behov, eller for å håndtere spesialiserte krav, teknologi som benyttes, særskilte oppgaver eller operative miljøer. Det er mange tilfeller hvor det finnes spesielle, men likeartede, behov. Det kan for eksempel være for en tjenestesektor eller et bruksområde i en tjenestesektor.

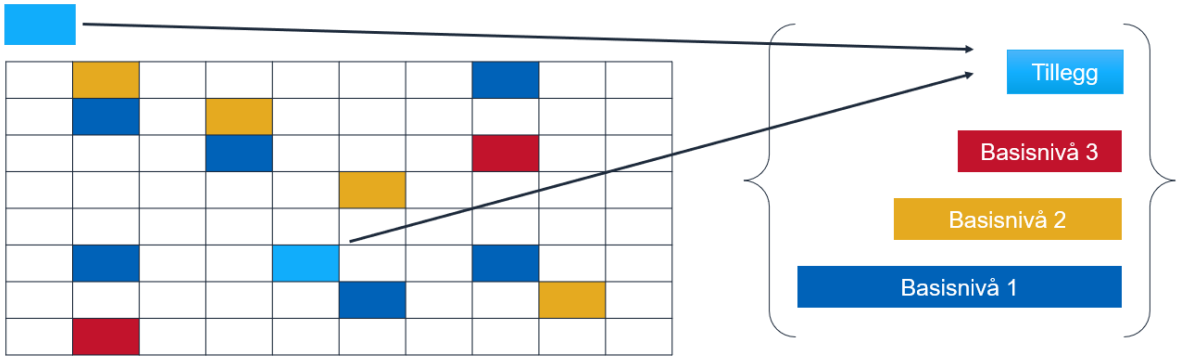
I slike tilfeller, kan et spesialtilpasset basisnivå utvikles for en tjenestesektor, teknologiområder, spesielle omstendigheter eller miljø. Dette kan publiseres og gjøres tilgjengelig for virksomheter med tilsvarende behov. Slik kan man oppnå mer felles og standardisert informasjonssikkerhet, konsistent etablering av sikkerhetstiltak og kostnadseffektive løsninger.

Et spesialtilpasset basisnivå kan være et komplett sett med sikkerhetstiltak, tiltaksforbedringer og annen støtteinformasjon (for eksempel tilpasninger av enkelt-tiltak) som er utledet fra og bygd på et generelt basisnivå. Det er en fordel om sikkerhetstiltak og tilpasninger er hentet fra en felles tiltaksbank, slik at den fungerer som samlingspunkt for alle involverte.

Spesialtilpassede basisnivåer utvikles for å kunne brukes for oppgaver, tjenester eller informasjonssystemer blant virksomheter med felles interesser og behov, og komplementerer og utvider konseptet med generelle basisnivåer ved å:

- gi mulighet for å legge til, endre eller fjerne sikkerhetstiltak
- gi mulighet for å tilpasse sikkerhetstiltak til spesifikk teknologi, ulike typer informasjonsbehandling, operative miljøer, ulike typer systemer
- gi mulighet for å tilpasse sikkerhetstiltak til ulike oppgaver og tjenester, tjenestesektorer og regelverkskrav

Det vil for eksempel være mulig å lage en eller flere spesialtilpassede basisnivåer for skjermingsverdige informasjonssystemer (iht. lov om nasjonal sikkerhet). Det kan utvikles et spesialtilpasset basisnivå for helsetjenester. Det kan tas inn i Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), og erstatte dagens opplisting av påkrevde sikkerhetstiltak i normens kapittel 5[57].



Figur 18 - Spesialtilpasset basisnivå for skjermingsverdig informasjonssystem (sikkerhetsloven)

Det er mulig å skalere fra det grunnleggende behovet for de fleste oppgaver og tjenester til sikkerhetslov-området, innenfor samme felles referanseramme med felles tiltaksbank og basisnivåer. Man kan bygge fra et sett med sikkerhetstiltak som dekker de grunnleggende behovene i stort sett alle oppgaver og tjenester, til et utvidet og spesialtilpasset sett med sikkerhetstiltak som kan benyttes for skjermingsverdige informasjonssystemer iht. sikkerhetsloven. Og alt foregår innenfor samme konseptuelle ramme, med omforent forståelse av innholdet i sikkerhetstiltakene.

Eksempler på spesialtilpassede basisnivåer for føderal forvaltning i USA (de kaller dem «overlays»):

- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security, appendix G
- CNSSI No. 1253 Security Categorization and Control Selection for National Security Systems, appendix F

4.2.6 Kategorier og nivåer av konsekvenser

I arbeidet med informasjonssikkerhet har virksomhetene behov for å estimere mulige konsekvenser ved informasjonssikkerhetsbrudd.

Det brukes til å sortere oppgaver, tjenester eller informasjonssystemer for å prioritere ressursbruken på arbeidet med informasjonssikkerhet der hvor konsekvensene ved informasjonssikkerhetsbrudd kan bli store. Det er det samme konseptet som benyttes til kategorisering av objekter og infrastruktur i sikkerhetsloven.

Konsekvenser brukes også som et av flere elementer i en risikomodell for å forstå og vurdere risiko. Som en del av det å anslå størrelse på risiko, så danner det grunnlag for prioritering av ressursbruk i arbeidet med å håndtere risiko.

[57] Spesifikke sikkerhetstiltak, slik begrepet benyttes i dette notatet, stilles det hovedsakelig krav til i normens kapittel 5.

For i være i stand til å arbeide effektivt med risiko sorterer man vanligvis konsekvenser i kategorier. Det kan for eksempel være konsekvenser for:

- Virksomhetens leveranser
- Virksomhetens økonomi
- Liv og helse
- Personvern
- Nasjonale sikkerhetsinteresser

En anbefaling om konsekvenskategorier og konsekvensnivåer som kan benyttes i styringsaktivitetene vil være nyttig hjelp til arbeidet i hver virksomhet. Det kan redusere arbeidsmengden og effektivisere arbeidet med informasjonssikkerhet.

Det kan bidra til mer felles forståelse av risiko og hvilke hensyn som skal ivaretas, øke kvaliteten på vurderingene, og bidra til at man får mer like resultater fra vurderingene i ulike virksomheter.

Det at elementene som inngår i slike vurderinger gjenkjennbart på tvers av virksomheter vil kunne øke evnen til samarbeid og samstyring av risiko på tvers av virksomheter.

Dersom det skal utvikles basisnivåer med sikkerhetstiltak, så kan sortering basert på konsekvensnivåene benyttes i forbindelse med tilordning av ulike basisnivåer til ulike behov.

Dersom en felles normering eller anbefaling om konsekvenskategorier og -nivåer skal utvikles og prøves ut, så vil det blant være behov for å se på:

- Hvordan dette er lagt opp i eksisterende veiledning, inkludert eksemplene i Digdirs veiledning om styring av informasjonssikkerhet, og brukeres erfaringer med disse
- Bruken av terskelverdier ifbm. NIS-direktivet
- Konsepter og fremgangsmåter som er i bruk i føderal forvaltning i USA

4.3 Vedlegg 3 – Krav, anbefalinger og veiledning

Om bruken av begrepene anbefalinger og veileding

Når dette notatet omtaler anbefalinger, så mener vi de anbefalingene som virksomhetene skal ha gode grunner til å ikke følge. En anbefaling er med andre ord noe en offentlig virksomhet *bør* gjøre.

Når dette notatet omtaler veiledning, så mener vi de tingene som er til hjelp til å følge krav og anbefalinger. For eksempel veiledning om metoder og praktiske fremgangsmåter for å gjennomføre påkrevde og anbefalte aktiviteter.

Sammenliknet med veiledning, så er anbefalinger noe som lettere kan gjøres obligatorisk ved at det gjøres om til krav i forskrift, eller at det på annen måte stilles krav om det i et juridisk instrument.

Dette tilsvarer skillet mellom anbefalinger og veiledning[58] i Referansekatalogen eller Digitaliseringsrundskrivet.

Oversikt over krav i regelverk

Beskrivelse av dagens regelverk er tilgjengelig fra flere kilder:

[58] https://www.digdir.no/digitalisering-og-samordning/introduksjon-til-krav-og-anbefalingar/2767

- Digdir: Internkontroll i praksis – Informasjonssikkerhet – Regelverkskrav og anbefalinger[59]
- DFØ/Digdir/NSM: Miniveileder om oppfølging av informasjonssikkerhet i styringsdialogen - Krav i regelverk[60]
- KS: Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet – Relevant lovgivning[61]
- Digdir/NSM/DFØ: Helhetlig styring og kontroll av informasjonssikkerhet - Ulike perspektiver gir ulikt fokus[62]
- NOU 2018: 14 IKT-sikkerhet i alle ledd - Regulering av IKT-sikkerhet[63]

Anbefalinger og veiledning

Digitaliseringsrundskrivet inneholder noen anbefalinger for statlige virksomheter[64].

Regjeringens digitaliseringsbrev til kommunene peker på en del av den samme veiledningen som Digitaliseringsrundskrivet.[65]

En oversikt over aktører som veileder og tilgjengelig veiledning er tilgjengelig som en del av veiledning om helhetlig styring og kontroll av informasjonssikkerhet, utarbeidet av Digdir, NSM og DFØ:

https://www.digdir.no/informasjonssikkerhet/veiledningsaktorer-innen-styring-og-kontroll/2280

4.4 Vedlegg 4 – Trusler og farer

Trusler og farer innen informasjonssikkerhet handler om årsaker til hva som kan skje i gjennomføring av oppgaver og leveranse av tjenester, inkludert bruk av digitale systemer og tjenester.

Det er forskjellige utløsende årsaker som kan føre til sikkerhetsbrudd i informasjonsbehandlingen, for eksempel:

- tilsiktede handlinger
- uaktsomhet
- uhell og ulykker
- naturhendelser

De konseptene og mulige tiltakene som beskrives i dette notatet er i liten grad avhengig av hvilke trusler og farer som er mest aktuelle til enher tid. Vi har derfor ikke inkludert en gjennomgang av trusler og farer i dette notatet.

---

[59] https://www.digdir.no/informasjonssikkerhet/regelverkskrav-og-anbefalinger-internkontroll-informasjonssikkerhet/3229
[60] https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/utdyping-av-krav-i-regelverk
[61] https://www.ks.no/fagomrader/forskning-og-utvikling-fou/forskning-og-utvikling/slik-sikrer-du-oppfolging-av-personvern-og-informasjonssikkerhet/
[62] https://www.digdir.no/informasjonssikkerhet/ulike-perspektiver-gir-ulikt-fokus/2279
[63] https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/?ch=3#kap6
[64] https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2895185/
[65] https://www.regjeringen.no/no/dokument/dep/kdd/andre-dokumenter/brev/utvalgte_brev/2022/digitalisering-i-offentlig-sektor-orientering-til-kommunesektoren/id2898570/

Vi oppfatter det slik at trusler og farer på informasjonssikkerhetsområdet er godt kjent. Innenfor digital sikkerhet er utviklingen med økt sårbarhet som følge av økende avhengighet av digitale systemer mye omtalt. Utviklingen i trusselbildet, hvor det som regel er tilsiktede handlinger som omtales, er også godt dekket og beskrevet andre steder. Se for eksempel NSMs rapporter Risiko 2022 og Nasjonalt digitalt risikobilde 2022[66].

Trusler og farer påvirker utforming av sikkerhetstiltak og daglig operativt arbeid

Trusler og farer er relevant for utforming av sikkerhetstiltak i felles tiltaksbank, eller i forbindelse med valg av sikkerhetstiltak som skal inngå i basisnivåer. Disse kommer likevel ikke til å behøve spesielt hurtig oppdatering.

Mesteparten av det som handler om hurtige endringer skjer i detaljer i etablerte sikkerhetstiltak, i det daglige operative arbeidet. Det er ikke nødvendigvis snakk om etablering av helt nye sikkerhetstiltak – på detaljeringsnivået av sikkerhetstiltak som benyttes i ISO/IEC 27002 og NIST 800-53.

I forbindelse med Russlands angrep på Ukraina publiserte NSM en sjekkliste over prioriterte tiltak virksomheter bør iverksette i en skjerpet sikkerhetssituasjon[67]. Den fungerer blant annet som en påminnelse om noen av de grunnleggende sikkerhetstiltakene virksomheter har behov for. Inneholdet er stort sett tiltak som vil kunne inngå i det basisnivået alle virksomheter bør ha etablert, til enhver tid, for alle sine oppgaver og tjenester.

Slik rådgivning om særskilte situasjoner eller trusler kan referere til sikkerhetstiltak i basisnivåer og felles tiltaksbank. Det vil gjøre det lettere for virksomhetene å ha oversikt og se sammenhenger.

4.5 Vedlegg 5 – Nasjonale strategier

Dette er en enkel og overordnet oversikt over hvilke målsetninger i nasjonale strategier som initiativet som beskrives i dette notatet kan bidra til.

Initaitivet kan også bidra til å nå målsetninger i sektorstrategier, slik om innenfor e-helse, men vi har ikke utarbeidet en oversikt over disse.

Legg merke til noen av nyansene i beskrivelsene i de nasjonale strategiene, og hvordan de henger sammen med det som beskrives i dette notatet. Blant annet så fokuserer noen av målsetningene i Nasjonal strategi for digital sikkerhet på digitale hendelser og digitale angrep. Digital sikkerhet utgjør en stor og vesentlig del av virksomhetenes arbeid med informasjonssikkerhet for sine oppgaver og tjenester. Men alle uønskede hendelser er ikke digitale, og de fleste hendelser har andre årsaker enn angrep[68].

Nasjonal strategi for digital sikkerhet

1 Norske virksomheter digitaliserer på en sikker og tillitvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.

---

[66] https://nsm.no/regelverk-og-hjelp/rapporter/
[67] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/digital-beredskap-i-en-skjerpet-situasjon/
[68] Se for eksempel Mørketallsundersøkelsen 2022, kapittel 3.1 https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

- Virksomheter har en risikobasert tilnærming mot uønskede digitale hendelser, og bruker anerkjente rammeverk, standarder og styringssystemer for digital sikkerhet.
- Offentlig sektor har god styring og kontroll på sin digitale sikkerhet. Virksomhetenes styringssystem for digital sikkerhet understøtter virksomhetenes hovedfunksjon, og bidrar til at sikkerhetshendelser i en offentlig virksomhet ikke medfører alvorlig skade hos andre.
- Privatpersoner, næringslivet og forvaltningen har tillit til at offentlige digitale tjenester er sikre og pålitelige.
- Myndighetene gir råd, anbefalinger og veiledninger om digital sikkerhet for å gi virksomhetene et kunnskapsgrunnlag for sitt sikkerhetsarbeid.
- Myndighetene legger til rette for samarbeid i offentlig sektor og mellom offentlig og privat sektor.

2 Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.

- Myndighetene stiller krav til sikkerhet i kritisk digital infrastruktur, veileder og fører tilsyn med at sikkerheten er forsvarlig. Offentlige og private virksomheter som eier kritisk digital infrastruktur gjennomfører tiltak som sørger for forsvarlig sikkerhet i disse.

4 Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.

- Norske virksomheter tar ansvar for å håndtere digitale angrep i egen virksomhet, og for å dele informasjon om disse til myndighetene og andre relevante aktører.

Én digital offentlig sektor – Digitaliseringsstrategi for offentlig sektor 2019–2025

- 3 Økt deling av data og verdiskaping
- 4 Klart digitaliseringsvennlig regelverk
- 5 Felles økosystem for nasjonal digital samhandling og tjenesteutvikling
- 6 Styring og samordning for en mer sammenhengende offentlig sektor
- 9 Digital sikkerhet

4.6 Vedlegg 6 – Sammendrag

4.6.1 Bakgrunn og formål

De langsiktige målsetningene som ligger til grunn for initiativet er en styrket og mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning, herunder:

- Alle virksomheter i forvaltningen har velfungerende styring og kontroll av informasjonssikkerhet.
- Virksomhetene i offentlig forvaltning har gode rammebetingelser for arbeidet med informasjonssikkerhet, inkludert digital sikkerhet. Dette inkluderer et helhetlig og brukerorientert veiledningstilbud.

Digdir ønsker å skape forståelse for utfordringene og interesse for et tverrsektorielt samarbeid for å få en helhetlig, felles retning på arbeidet med informasjonssikkerhet i offentlig forvaltning.

I dette notatet beskriver vi utfordringene virksomhetene har med å få god styring på området, og peker på konsepter og løsninger som kan utvikles for å gi virksomhetene bedre forutsetninger for å lykkes, og legge til rette for

- effektivt arbeid med informasjonssikkerhet
- samstyring i sammenhengende tjenestekjeder
- god sikkerhet på tvers av hele forvaltningen

Dersom en felles retning på arbeidet med informasjonssikkerhet skal realiseres vil det kreve at relevante fagmyndigheter legger til grunn den samme tilnærmingen, og benytter den som utgangspunkt for sine ulike veiledningsansvar.

Resultatet vil være at virksomhetene på alle forvaltningsnivå får mer spesifikke og resultatorienterte anbefalinger. Det vil i tillegg være behov for samordning og konsolidering av eksisterende veiledning om hvordan de kan gå fram for å finne og dekke egne behov.

4.6.2 Betydning for evne til å utføre oppgaver og levere tjenester

I vår moderne verden har informasjonsbehandling svært stor betydning for offentlige virksomheters oppgaveløsing. Informasjonssikkerhet handler om å sikre informasjonsbehandlingen i de oppgavene og tjenestene som offentlige virksomheter har ansvaret for. Digital sikkerhet og sikkerhet i digitale tjenester er en viktig del av dette.

Informasjonssikkerhetsbrudd kan få konsekvenser for virksomhetens leveranser, økonomi og evnen til å utføre oppgaver og yte tjenester. Slike brudd kan også få følger for innbyggere og ansatte, andre virksomheter, samfunnsfunksjoner eller nasjonale sikkerhetsinteresser. Informasjonssikkerhet på tvers av forvaltningen har stor betydning for samfunnssikkerheten.

Virksomhetenes ledelse har et selvstendige ansvar

Lederne for offentlige virksomheter har et selvstendig ansvar for å styre risiko for de oppgavene og tjenestene som de har ansvaret for. De må ta ansvaret for å styre arbeidet med informasjonssikkerhet som en del av det å styre risiko for virksomhetens oppgaver og tjenester.

Arbeidet med informasjonssikkerhet skal være risikobasert, med fleksibilitet og rom for tilpasning til en virksomhets størrelse, egenart og risiko. Dette skal gi tilstrekkelig og

kostnadseffektiv informasjonssikkerhet for alle oppgaver og tjenester, inkludert digitale tjenester.

For å ivareta dette ansvaret må ledelsen styre informasjonssikkerhet som en del av det å styre virksomheten. De delene av styringen som har spesiell oppmerksomhet på informasjonssikkerhet kalles gjerne «styringssystem for informasjonssikkerhet», og kan deles inn i to hoveddeler:

- Styringsaktiviteter
- Sikkerhetstiltak

4.6.3 Avgrensning

Det er vanskelig å dekke alt som kan inngå i informasjonssikkerhet og digital sikkerhet under én paraply. Dette notatet tar utgangspunkt i, og tar i hovedsak for seg, det selvstendige ansvaret hver virksomhet i forvaltningen har for å styre risiko for sine oppgaver og tjenester; hvordan anbefalinger og veiledning kan hjelpe dem med å lykkes med å ivareta det ansvaret, og hvordan det kan bli mer effektivt og gjøres mer likt på tvers av virksomhetene.

Det er likevel snakk om å se arbeidet med informasjonssikkerhet på tvers av forvaltningsnivåene og virksomhetene i forvaltningen, og hvordan de kan få en mest mulig felles referanseramme for arbeidet, og få gode rammebetingelser for samarbeid og samstyring.

4.6.4 Utfordringsbildet

Anbefalinger og veiledning om hvordan arbeidet med informasjonssikkerhet kan gjennomføres har vært tilgjengelig fra flere aktører i flere år. Det er likevel krevende for den enkelte virksomhet å ha tilstrekkelig informasjonssikkerhet, og ivareta forpliktelser i alle regelverk.

Utfordringsbildet er sammensatt, og inkluderer blant annet:

- Virksomheter har svake eller manglende styringsaktiviteter
- Virksomheter mangler grunnleggende sikkerhetstiltak
- Virksomheter må til en viss grad gjøre de samme vurderingene
- Virksomheter har utilstrekkelig oversikt over informasjonsbehandlingen
- Virksomheter har mangelfull forvaltning av sikkerhetstiltak
- Arbeidet i virksomhetene er kompetansekrevende
- Arbeidet er ressurskrevende også utover behovet for kompetanse
- Det er krevende å undersøke om omfang av sikkerhetstiltak er tilstrekkelig
- Det er vanskelig å evaluere informasjonssikkerhet på tvers av virksomheter
- Det er utfordrende å bruke og følge opp tjenesteleverandører
- Manglende tillit mellom offentlige virksomheter kan være hinder for digitalisering
- Vanskelig å få til helhetlig tilnærming i styringen av virksomhetene
- Mangelfull og fragmentert regulering

4.6.5 Tiltak og anbefalinger

Et nasjonalt løft for informasjonssikkerhet

Både små og store virksomheter har utfordringer, og det virker som det går sakte fremover. Det er behov for et taktskifte i arbeidet med informasjonssikkerhet i forvaltningen.

Digdir mener det bør komme et nasjonalt løft for informasjonssikkerhet generelt, og digital sikkerhet spesielt. Det er nødvendig for at forvaltningen skal være i stand til løse oppgavene sine og levere tjenester i fremtiden.

4.6.6 Mulige tiltak i forvaltningen

Digdir har identifisert syv mulige tiltak:

- T1 Felles referanseramme
- T2 Katalog med oppgaver/tjenester og informasjonstyper
- T3 Basisnivåer med sikkerhetstiltak
- T4 Felles tiltaksbank
- T5 Kategorier og nivåer av konsekvenser
- T6 Spesialtilpassede basisnivåer med sikkerhetstiltak
- T7 Ny lov om informasjonssikkerhet for offentlig forvaltning

Felles referanseramme

Ved å bygge på det som allerede finnes, og tilføre noen nye elementer, kan vi etablere en tydeligere felles referanseramme (eller «norm») for arbeidet med informasjonssikkerhet i offentlige virksomheter. Det kan inkludere tydelige anbefalinger om:

- Styringsaktiviteter
- Basisnivåer med sikkerhetstiltak
- Felles tiltaksbank med sikkerhetstiltak

Anbefalinger i en felles referanseramme må støttes opp med veiledning fra ulike aktører. Denne veiledningen eksisterer i stor grad allerede, men bør referere til hvilke elementer i den felles referanserammen det veiledes om i mer detalj.

Anbefalinger og tilhørende veiledning skal gjøre det enklere for virksomhetene å ivareta sitt ansvar. Det at ting gjøres mer likt og felles på tvers av forvaltningen kan styrke evnen til samarbeid og samstyring, og bidra til gjensidig tillit mellom tjenesteeiere som er avhengige av hverandre.

Som vi ser av utfordringsbildet så opplever svært mange det som krevende å få til god styring og oppnå formålet med ulike regelverk. Virksomhetene bør få hjelp til å få de vesentligste tingene på plass på en måte som de er i stand til å forvalte. Det er flere brukerrettede produkter og veiledning som kan utformes for å lette og effektivisere arbeidet med informasjonssikkerhet i virksomhetenes operative arbeid.

Oversikt over informasjonsbehandlingen og dens betydning

For å få til effektiv styring har man behov for oversikt over oppgaver, tjenester og informasjonsbehandlingen i disse. En katalog med oversikt over oppgaver og informasjonstyper som behandles i dem kan gjøres tilgjengelig og redusere omfanget av det som må gjøres i hver enkelt virksomhet. Det vil bidra til å effektivisere arbeidet med informasjonssikkerhet.

Basisnivåer med sikkerhetstiltak

Grunnleggende sikkerhetstiltak kan samles i et eller flere basisnivåer. De kan danne utgangspunktet for virksomhetens valg av sikkerhetstiltak for oppgaver, tjenester eller informasjonssystemer. Det kan både effektivisere arbeidet i virksomhetene og bidra til å gi et mer felles, grunnleggende sikkerhetsnivå på tvers av forvaltningen.

Sikkerhetstiltak som skal inngå i basisnivåer bør være uttrekk fra en felles tiltaksbank.

Felles tiltaksbank med sikkerhetstiltak

Ved å hente sikkerhetstiltak fra en felles tiltaksbank[69] trenger man ikke bruke mye tid og ressurser på å utforme disse selv. En felles tiltaksbank for offentlige forvaltning vil:

- gjøre det mulig å lage basisnivåer med sikkerhetstiltak fra tiltaksbanken
- fungere som en felles referanse for veiledning om sikkerhetstiltak, slik at det blir lett for brukere å se ulik veiledning i sammenheng
- fungere som kilde for tilsynsmyndigheter
- bidra til å øke evnen til samarbeid mellom virksomheter

Kategorier og nivåer av konsekvenser

En anbefaling om konsekvenskategorier og konsekvensnivåer som alle kan benytte kan effektivisere arbeidet med informasjonssikkerhet. Det kan øke kvaliteten på vurderinger, og bidra til at resultatene blir mer like på tvers av virksomheter. Det at konsekvenskategorier og -nivåer er gjenkjennbare på tvers av virksomheter vil kunne øke evnen til samarbeid og samstyring av risiko.

Anbefalinger eller regulering

Konseptene bør utvikles som anbefalinger til virksomhetene. Dersom de viser seg å være nyttige, så vil de ha størst nytteverdi dersom de brukes av de fleste virksomhetene i forvaltningen. På sikt kan det derfor være aktuelt å se på muligheten for å regulere bruken av disse. Det kan være starten på en opprydning i dagens fragmenterte regelverk, med tanke på at like hensyn skal reguleres likt.

4.6.7 Viktige sammenhenger

Felles økosystem for nasjonal digital samhandling og tjenesteutvikling

Virksomheter skal samarbeide og dele data i et felles økosystem for digital samhandling og tjenesteutvikling i større grad i fremtiden. Når tjenester fra ulike virksomheter henger tettere sammen blir virksomhetene i større grad avhengig av andre virksomheter, og at de har tilstrekkelig informasjonssikkerhet.

Felles utfordringer på informasjonssikkerhetsområdet har betydning for digitale tjenester, og for tjenestekjeder i felles økosystem. Når tjenester henger sammen, kan en hendelse i én virksomhet kan få direkte konsekvenser for tjenester hos andre virksomheter.

Når virksomheter skal utvikle og levere tjenester sammen, er det behov for samarbeid og samstyring for å håndtere risiko i tjenestekjeden. Slikt samarbeid vil inkludere samstyring av informasjonssikkerhet.

[69] https://www.digdir.no/informasjonssikkerhet/tiltaksbankar/3057

Det er derfor viktig å se på hvordan rammebetingelsene for informasjonssikkerhet kan legge til rette for dette på en god måte.

Personvern

Det er mange oppgaver og tjenester i offentlig forvaltning som behandler personopplysninger, og informasjonssikkerhet er viktig for å ivareta fysiske personers rettigheter og friheter når det behandles opplysninger om dem.

Det kan være mye å hente i å samkjøre arbeidet med informasjonssikkerhet og personvern for de oppgavene og tjenestene det gjelder.

Styringsaktiviteter kan ha samme struktur uavhengig av hva som skal styres[70]. Mye er likt selv om det vil være ulike metoder i bruk, og forskjellige måter å gjennomføre deler av aktivitetene på.

En felles tiltaksbank kan inneholde både sikkerhetstiltak og personverntiltak. Det kan gjøre det enklere for virksomhetene å kombinere arbeidet med informasjonssikkerhet og personvern for oppgaver og tjenester som behandler personopplysninger.

Det kan også lages et basisnivå med personverntiltak som kan tilordnes oppgaver og tjenester som behandler personopplysninger.

Offentlige anskaffelser og skytjenester

Offentlige virksomheter må styre risiko for sine oppgaver og tjenester også når de understøttes og gjennomføres ved bruk av anskaffelser, inkludert kjøp av tjenester som inngår i informasjonsbehandlingen. Det kan være fordeler med større grad av felles kravstilling til leverandørmarkedet.

Det kan være fornuftig at anbefalinger og krav rettes til de offentlige virksomhetene og oppgavene og tjenestene de skal levere. De relevante delene av kravene må ivaretas av tjenesteleverandører, alt etter innholdet i tjenesteleveransen. Dersom krav til sikkerhetstiltak for skytjenester bygges på de samme basisnivåene som er anbefalt å benytte for offentlige oppgaver og tjenester, så kan det gi tydelig ansvarsdeling mellom kunde og leverandør. Det kan også benyttes til å utforme sertifiseringsordning for skytjenester.

4.6.8 Anbefalinger

Digdir anbefaler at det startes et arbeid for å utvikle en felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter.

Det bør startes et arbeid for å utvikle og prøve ut de mulige tiltakene som er beskrevet i dette notatet. Dersom det skal ha full effekt, bør det tas sikte på at det etter hvert skal dekke hele forvaltningen. Under utvikling og utprøving vil det likevel være fornuftig å fokusere spesielt på å møte behovene til virksomheter med lav modenhet eller lite tilgang på nødvendige ressurser til arbeidet med informasjonssikkerhet. Kommunene har de samme eller svært likeartede oppgaver og tjenester, og det vil være naturlig å starte med noen av tiltakene der.

[70] https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

Digitaliseringsdirektoratet anbefaler at nye tiltak for forvaltningen utvikles i samarbeid mellom de sentrale myndighetsorganene som veileder virksomhetene om informasjonssikkerhet og styring og kontroll og virksomheter fra ulike forvaltningsnivåer.

Mulige gevinster

Felles sikkerhet i forvaltningen kan blant annet bidra til:

- Mer kostnadseffektivt arbeid med informasjonssikkerhet
- Styrket grunnleggende sikkerhet på tvers av forvaltningen
- Mer effektivt grensesnitt mot tjenesteleverandørmarkedet
- At det blir enklere å utvikle sammenhengende tjenester og dele data

Tydeligere rammer for informasjonssikkerhet i tjenesteutvikling i felles økosystem

4.7 Vedlegg 7 – Figurer

Figur 1 – Felles retning på arbeidet med informasjonssikkerhet i forvaltningen 3

Figur 2 – Virksomheter har behov for styringsaktiviteter og sikkerhetstiltak for å få god informasjonssikkerhet 4

Figur 3 - Oppgaver og tjenester i offentlig forvaltning 5

Figur 4 - Informasjonssikkerhet inngår i styringen av en virksomhet 7

Figur 5 – Skisse av oppgaven «elevadministrasjon», med informasjonstyper og digitale systemer som benyttes i informasjonsbehandlingen. 10

Figur 6 – Mange regelverk stiller krav til ledelsens styring, og det er krevende å arbeide helhetlig for å ivareta alle hensyn. 12

Figur 7 – Ulike aktører tar utgangspunkt i felles anbefalinger og tilfører veiledning virksomhetene har behov for 18

Figur 8 - Oppgaver og informasjonstyper 19

Figur 9 - Konsekvenser av informasjonssikkerhetsbrudd 22

Figur 10 - Felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter 25

Figur 11 – Virksomhetene finner svar på sentrale spørsmål på ett sted 26

Figur 12 - Felles elementer benyttes i gjennomføringen av styringsaktiviteter 27

Figur 13 - Modell av felles økosystem for nasjonal digital samhandling og tjenesteutvikling 31

Figur 14 - Virksomheter har felles tilnærming til informasjonssikkerhet 32

Figur 15 - Krav til offentlige tjenester og eksterne skytjenester 34

Figur 16 - Styringsaktiviteter og sikkerhetstiltak 40

Figur 17 - Basisnivåer med sikkerhetstiltak 41

Figur 18 - Spesialtilpasset basisnivå for skjermingsverdig informasjonssystem (sikkerhetsloven) 44

4.8 Vedlegg 8 – Kilder

Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden.* [https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf]

Meld. St. 28 (2020 – 2021) *Vår felles digitale grunnmur - Mobil-, bredbånds- og internettjenester.* [https://www.regjeringen.no/no/dokumenter/meld.-st.-28-20202021/id2842784/]

Meld. St. 38 (2016 –2017) *IKT-sikkerhet - Et felles ansvar.* [https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/]

Meld. St. 29 (2016–2017) *Perspektivmeldingen 2017*. [https://www.regjeringen.no/no/dokumenter/meld.-st.-29-20162017/id2546674/]

Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn — Samfunnssikkerhet.* [https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/]

NOU 2018: 14 *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.* [https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/]

NOU 2016: 19 *Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* [https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/]

NOU 2022: 11 *Ditt personvern – vårt felles ansvar*.[https://www.regjeringen.no/no/dokumenter/nou-2022-11/id2928543/]

FIPS 199. *Standards for Security Categorization of Federal Information and Information Systems.* [https://doi.org/10.6028/NIST.FIPS.199]

FIPS 200. *Minimum Security Requirements for Federal Information and Information Systems NIST Cybersecurity Framework.* [https://doi.org/10.6028/NIST.FIPS.200]

SP 800-37 Rev. 2. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. [https://doi.org/10.6028/NIST.SP.800-37r2]

SP 800-53 Rev. 5. *Security and Privacy Controls for Information Systems and Organizations.* [https://doi.org/10.6028/NIST.SP.800-53r5]

SP 800-53B. *Control Baselines for Information Systems and Organizations.* [https://doi.org/10.6028/NIST.SP.800-53B]

NIST Special Publication 800-39 (2011): Managing Information Security Risk [https://doi.org/10.6028/NIST.SP.800-39]

SP 800-60 Vol. 1 Rev. 1. *Guide for Mapping Types of Information and Information Systems to Security Categories.*[https://doi.org/10.6028/NIST.SP.800-60v1r1]

SP 800-60 Vol. 2 Rev. 1. *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices.* [https://doi.org/10.6028/NIST.SP.800-60v2r1]

Committee on National Security Systems (CNSSI), No. 1253, *Security Categorization And Control Selection For National Security Systems,* 2014. [https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf]

NISTIR 8170. *Approaches for Federal Agencies to Use the Cybersecurity Framework*. [https://doi.org/10.6028/NIST.IR.8170-upd]

Riksrevisjonen (2018) *Riksrevisjonens årlige revisjon og kontroll – budsjettåret 2017. Dokument 1 (2018–2019).* [https://www.riksrevisjonen.no/globalassets/rapporter/no-2018-2019/riksrevisjonensarligerevisjonogkontroll2017.pdf]

Kommunal- og moderniseringsdepartementet (2020) *Dataforvaltning og -deling i kommunene*. R1021222. [https://www.regjeringen.no/contentassets/05c9563f28024e1bb82f5e31d1dbfd72/rapport_dataforvaltning-og--deling-i-kommunene_endelig-versjon.pdf]

Nasjonal sikkerhetsmyndighet (2020) NSMs g*runnprinsipper for IKT-sikkerhet*, versjon 2.0. [https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/]

Nasjonal sikkerhetsmyndighet (2020) *NSMs grunnprinsipper for personellsikkerhet.* [https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/]

Nasjonal sikkerhetsmyndighet (2020) *NSMs grunnprinsipper for fysisk sikkerhet*. [https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-fysisk-sikkerhet/introduksjon/]

Nasjonal sikkerhetsmyndighet (2021) *Nasjonalt digitalt risikobilde 2021.* [https://nsm.no/getfile.php/137495-1635323653/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf]

Nasjonal sikkerhetsmyndighet (2022) *Nasjonalt digitalt risikobilde 2022*. [https://nsm.no/getfile.php/1312007-1667980738/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf]

Nasjonal sikkerhetsmyndighet (2021) *Risiko 2021 – helhetlig sikring mot sammensatte trusler*. [https://nsm.no/getfile.php/136419-1616673370/Filer/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf]

Nasjonal sikkerhetsmyndighet (2022) *Risiko 2022 – Økt risiko krever økt årvåkenhet*. [https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf]

Datatilsynet. *Virksomhetenes plikter* [https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/]

Datatilsynet. *Informasjonssikkerhet og internkontroll* [https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/]

European Data Protection Board. *Guidelines, Recommendations, Best Practices* [https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en]

Digitaliseringsdirektoratet (2020) *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner.* 2020:3. [https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102]

Direktoratet for forvaltning og IKT (2018) *Arbeidet med informasjonssikkerhet i statsforvaltningen.* 2018:4. [https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-statsforvaltningen/2044]

Difi-rapport 2013:10 *Informasjonsforvaltning i offentleg sektor* [https://www.digdir.no/informasjonsforvaltning/informasjonsforvaltning-i-offentleg-sektor/1375]

Direktoratet for samfunnssikkerhet og beredskap (2020), *Risikostyring i digitale verdikjeder*. [https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf]

KPMG, *IKT-sikkerhet I Østre Toten kommune forut for dataangrepet 9. januar 2021,* august 2021. [https://www.ototen.no/_f/p1/i5689ceb7-72b4-44d0-970c-a5c4828047e5/endelig-rapport-26082021-kpmg_sladdet.pdf]

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [https://eur-lex.europa.eu/eli/dir/2016/1148/oj]

EU (ENISA), *EUCS – Cloud Services Scheme*, Dec 2020. [https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme]

European Commission, Directorate-General for Communications Networks, Content and Technology, Álvarez, M., Cortés, C., Orue-Echevarria, L., et al., *Certification schemes for cloud computing* : executive summary, Publications Office, 2019. [https://data.europa.eu/doi/10.2759/508460]

UK government, *Government Functional Standard – GovS 007: Security*. Version 2.0, Sep 2021. [https://www.gov.uk/government/collections/functional-standards]

NISTIR 8062. *An Introduction to Privacy Engineering and Risk Management in Federal Systems.* [https://doi.org/10.6028/NIST.IR.8062]

Datatilsynet. *Vedtak om overtredelsesgebyr - Bergen kommune - Melding om avvik i Vigilo*. [https://www.datatilsynet.no/contentassets/fd5c454b4eae4924af94943ba68002bf/20_02181-3-vedtak-om-overtredelsesgebyr---bergen-kommune.pdf]

Næringslivets sikkerhetsråd. *Mørketallsundersøkelsen 2022* [https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2022-web-sider.pdf]