Hvordan forbedre informasjonssikkerhetsarbeidet i din virksomhet - 5 viktige områder

NIFS-møtet 18.11.2020

NASJONAL SIKKERHETSMYNDIGHET dsb Direktoratet for samfunnssikkerhet og beredskap dfø NorSIS Norsk senter for informasjonssikring Digdir

Agenda

TID	TEMA
10:00 – 10:10	**Velkommen og innledning** *Kjetil Korslien, Seksjonsleder i Digitaliseringsdirektoratet*
10:10 – 10:30	**Oppfølging av informasjonssikkerhet i styringsdialogen** *Trine Wold Møller, Rådgiver i Direktoratet for forvaltning og økonomistyring (DFØ)*
10:30 – 10:50	**Styring og kontroll av informasjonssikkerhet** *Katrine Aam Svendsen, Seniorrådgiver i Digitaliseringsdirektoratet*
10:50 – 11:00	**PAUSE**
11:00 – 11:20	**Øvelser** *Helen Knutsen, Seniorrådgiver i Direktoratet for samfunnssikkerhet og beredskap (DSB)*
11:20 – 11:40	**Sikkerhetskultur** *Eivind Reiner-Holm, Seniorrådgiver i NorSIS*
11:40 – 11:55	**Sikkerhetskompetanse** *Zoya Shah, Seniorrådgiver i Digitaliseringsdirektoratet*
11:55 – 12:05	**Erfaringsforedrag - bruk av kompetansebeskrivelsene i Ringerike kommune** *Torkjell Dahl, IT-sjef i Ringerike kommune*
12:05 – 12:15	**Avslutning** *Kjetil Korslien, Seksjonsleder i Digitaliseringsdirektoratet*

Digital sikkerhet er en grunnleggende forutsetning for vellykket digitalisering

Digitaliseringsstrategien

Digitaliseringsstrategien for offentlig sektor (2019-2025) skal understøtte digital transformasjon i virksomheter og offentlig sektor som helhet.

Kapittel 9 - Digital sikkerhet omtaler digital sikkerhet som en grunnleggende forutsetning for å opprettholde tillit til offentlig sektors IT-systemer og offentlige digitale tjenester. En vellykket digitalisering handler derfor om å ivareta krav til sikkerhet og den enkeltes personvern på en god måte.

Nasjonal strategi for digital sikkerhet

Nasjonal strategi for digital sikkerhet ble lagt frem i januar 2019. Strategien skal møte utfordringene som følger av en rask og gjennomgående digitalisering av det norske samfunnet.

Tiltak 5 – Sikker digitalisering i offentlig sektor skal underbygge arbeidet med digitalisering av offentlig sektor og er et sentralt tiltak i strategien. Det digitale sikkerhetsarbeidet må sees i et helhetlig perspektiv, på tvers av sektorer og forvaltningsnivåer, og i sammenheng med det øvrige arbeidet for samfunnssikkerhet.

Begge strategiene refererer til kunnskapsgrunnlaget om arbeidet med informasjonssikkerhet i statsforvaltningen, utarbeidet av Difi i 2018

Difi gjennomførte i 2018 en kartlegging og evaluering av arbeidet med informasjonssikkerhet i statsforvaltningen på oppdrag fra KMD

Hovedfunn

Kartleggingens hovedfunn var at en av tre statlige virksomheter ikke har tilstrekkelig styring og kontroll på informasjonssikkerheten, og at departementet i lite grad etterspør status på arbeidet med informasjonssikkerhet hos underliggende virksomheter.

Anbefalinger

Rapporten ga 11 anbefalinger som skulle styrke arbeidet med styring og kontroll av informasjonssikkerhet og sikre at virksomhetene oppnår tilstrekkelig modenhet og blir bedre rustet til å følge endringer i trusselbildet.

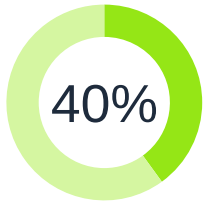
Oppfølging

Anbefalingene følges nå opp i et samarbeidsprosjekt bestående av 5 delprosjekter som utvikler veilednings- og ressursmateriale innen 5 viktige områder for informasjonssikkerhet.

NASJONAL SIKKERHETSMYNDIGHET dsb dfø NorSIS Digdir

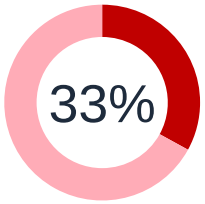
Kunnskapsgrunnlaget avdekket at en av tre virksomheter ikke har tilstrekkelig styring og kontroll på informasjonssikkerheten

Etatsstyrere etterspør i liten grad status på arbeidet med informasjonssikkerhet hos underliggende virksomheter



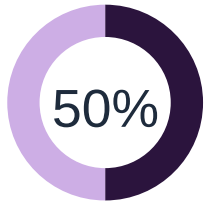
Kun 40% har kartlagt eller målt sikkerhetskulturen i virksomheten

Få departementer har bedt sine underliggende virksomheter analysere status på informasjonssikkerhet



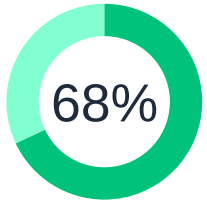
En av tre statlige virksomhet har ikke tilstrekkelig styring og kontroll på informasjonssikkerheten. Det er stor variasjon på innretning og omfang på styring og kontroll i virksomhetene

Virksomhetene har liten kjennskap til regelverkene som stiller krav til informasjonssikkerhet, spesielt økonomiregelverket i staten og § 15 i eForvaltningsforskriften



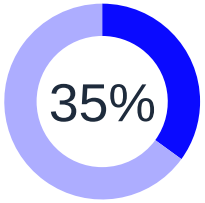
Under halvparten har årlige øvelser. 27% av virksomhetene mangler en IKT-beredskapsplan som er godkjent av virksomhetsleder

Mange virksomheter har utfordringer med å etablere og følge opp sikkerhetstiltak



68% av virksomhetene klarer å dekke opp sitt behov for fagkompetanse på området informasjonssikkerhet

Arbeidet med kompetanseheving på informasjonssikkerhet er i mange tilfeller lite målrettet og ikke tilpasset virksomhetens egenart og behov



35% av virksomhetene har retningslinjer for å akseptere risiko

Flere virksomheter opplever uenighet mellom ledelsen og fagansvarlige på hvor tydelig det foreligger føringer på arbeidet med informasjonssikkerhet

NASJONAL SIKKERHETSMYNDIGHET dsb dfø NorSIS Digdir

På bakgrunn av hovedfunnene ble det satt opp 11 anbefalinger innenfor 6 hovedtemaer

Anbefalinger for helhetlig styrking av informasjonssikkerheten

Styring og kontroll

1. Departementene stiller krav om at virksomhetene rapporterer på sikkerhets-tilstanden for egen virksomhet, og status på arbeidet med styring og kontroll av informasjonssikkerhet i årsrapporten. Rapporteringen bør være lik og sammenlignbar for alle statlige virksomheter.
2. Informasjonssikkerhet inngår som en del av virksomhetsplanen

Risikostyring

3. Den enkelte virksomhet må sikre nødvendig kompetanse på fagfeltet risikostyring
4. Hovedprinsippet om at regelverk for informasjonssikkerhet bør være risikobasert og legge til rette for tilpasning i virksomhetene bør videreføres

Beredskap, øvelser og hendelseshåndtering

5. Virksomhetene gjennomfører minst en årlig øvelse innen informasjonssikkerhet. Både planlegging og rapportering av erfaringer fra øvelsen må knyttes opp mot virksomhetens styringssystem for informasjonssikkerhet
6. DSB bør i samarbeid med NSM og Difi tilpasse sitt kursmateriale for øvelser, slik at det blir enkelt å ta i bruk for mindre virksomheter
7. Vi anbefaler at det i sektorer (for eksempel virksomheter under et departement) eller geografiske regioner (for eksempel i et fylke) gjennomføres felles øvelser
8. Norske virksomheter bør vurdere å delta i internasjonale øvelser for å få erfaring med grenseoverskridende hendelser. ENISA har ansvar for det europeiske øvingsprogrammet Cyber Euro som arrangerer øvelser hvert annet år og hvor NSM NorCERT er etablert som norsk kontaktpunkt

Sikkerhetskultur

9. Virksomheter kartlegger sin sikkerhetskultur. På bakgrunn av kartleggingen utformer virksomheten eventuelle tiltak til forbedring

Kompetanse

10. Virksomhetene bør vurdere å etablere en plan for kompetanseutvikling på området informasjonssikkerhet

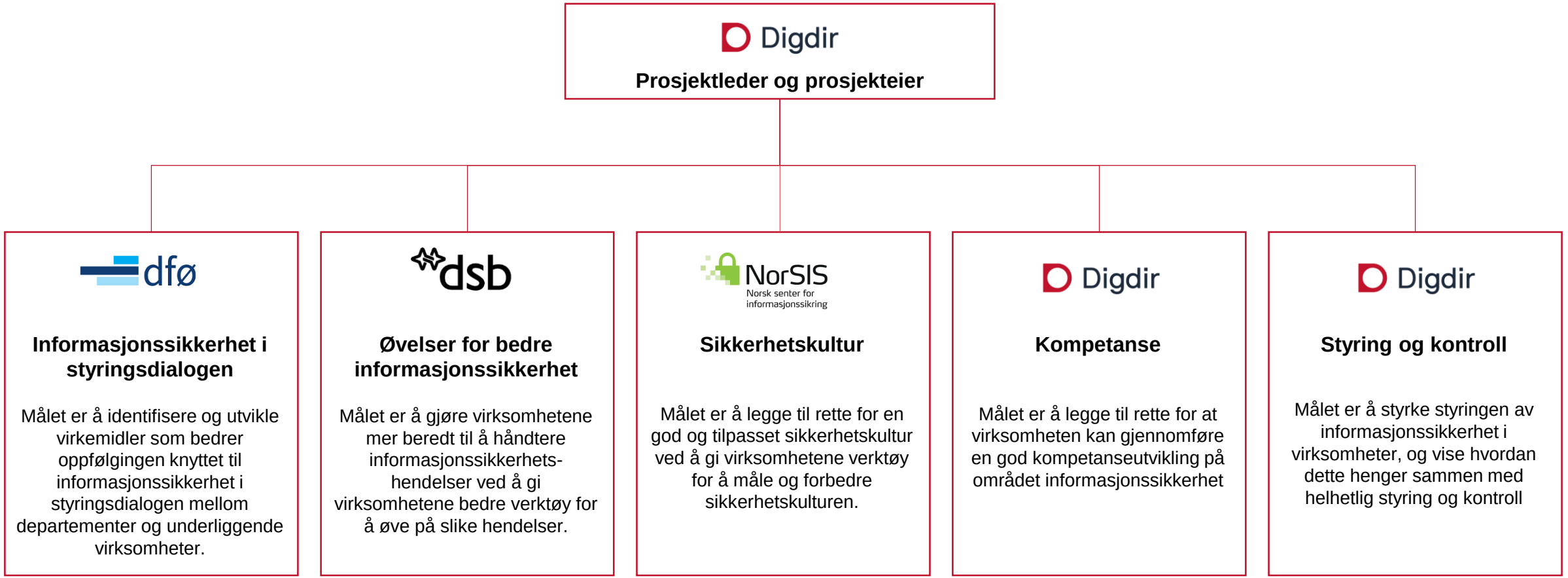
Etatsstyring

11. Informasjonssikkerhet følges opp i styringsdialogen mellom departement og underliggende virksomhet. Etatsstyrere bør ha tilgang på veiledning om hvordan informasjonssikkerhet bør ivaretas i etatsstyringen.

Samarbeidsprosjektet for informasjonssikkerhet har bestått av 5 delprosjekter som har hatt leveranser relatert til anbefalingene

NASJONAL SIKKERHETSMYNDIGHET | dsb Direktoratet for samfunnssikkerhet og beredskap | dfø | NorSIS Norsk senter for informasjonssikring | Digdir

Prosjektet er et samarbeid mellom DFØ, DSB, NorSIS, NSM og Digdir



Delprosjektansvar er basert på etatenes fagkompetanse

For spørsmål, ta kontakt med:

infosikkerhet@digdir.no