Digdir

digdir.no

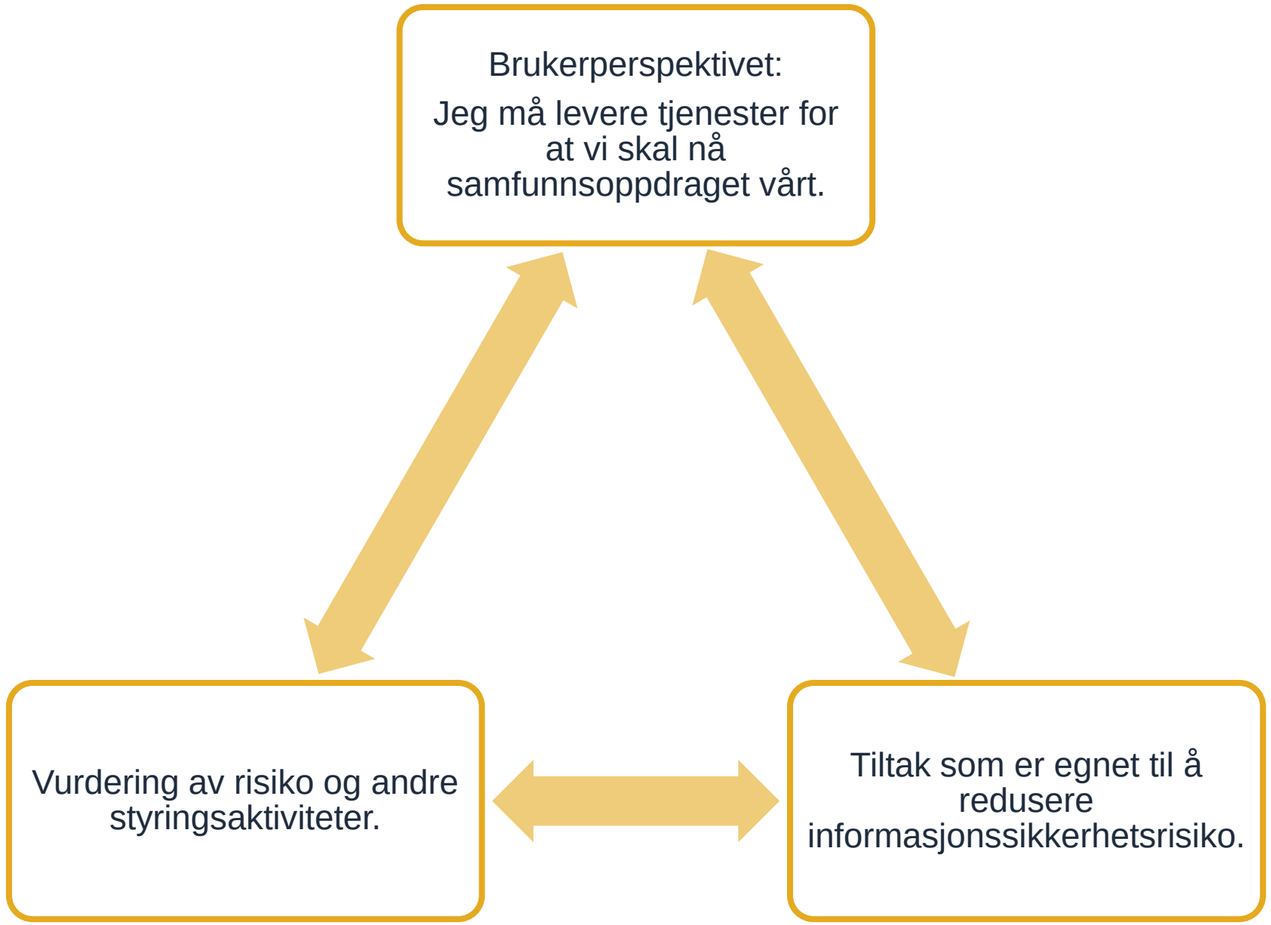
Et nasjonalt løft for informasjonssikkerhet

Sikkerhetsfestivalen 2023
Katrine Aam Svendsen
Seksjonssjef (fung.), Statens kompetansemiljø for informasjonssikkerhet

Snakkepunkter

- Hva er «Felles sikkerhet i forvaltningen»?
- Publisering av notat, og tilbakemeldinger
- Videre arbeid og samarbeid
- Felles referanseramme og styringsaktiviteter

Virksomhetsperspektivet



Digdir

digdir.no

«Felles sikkerhet i forvaltningen»

Viktige spørsmål virksomhetene må stille seg selv.

Hvilke oppgaver leverer vi, og hvilken informasjon behandles?

Hvor store konsekvenser kan informasjonssikkerhetshendelser få?

Hvilke sikkerhetstiltak bør vi etablere?

Katalog over oppgaver, og informasjonsbehandling

Vurdering av konsekvensnivå per oppgave

Anbefalte minimumstiltak

Svar fra veiledningsaktørene, på ett sted, felles for alle.

Rapport

Felles sikkerhet i forvaltningen

Digitaliseringsdirektoratet tar initiativ til et tverrsektorielt samarbeid for å sikre en felles retning på arbeidet med informasjonssikkerhet i offentlig forvaltning.

Digdir-notat 12. desember 2022 Informasjonssikkerhet

Et nasjonalt løft for informasjonssikkerhet

Digdir mener det er behov for et taktskifte i arbeidet med informasjonssikkerhet i forvaltningen. Vi 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 sine oppgaver og levere tjenester i fremtiden.

Digdir anbefaler strategisk retning for de neste årene, og peker på mulige tiltak for forvaltningen, og hvilke muligheter og gevinster det kan gi. Vi har beskrevet dette i et notat som kan leses og lastes ned fra denne siden.

Det vil være verdifullt om dette initiativet bidrar til en mer omforent innretning av informasjonssikkerhetsarbeidet i offentlig forvaltning.

Arbeids- og inkluderingsdepartementet

Det er positivt med tverrsektorielt samarbeid og et basisnivå for tiltak som kan tilpasses både små og store virksomheter.

Olje- og energidepartementet

JD stiller seg bak denne beskrivelsen og behovet for å sikre bedre samordning og koordinering av sikkerhetsarbeidet.

Justis- og beredskapsdepartementet

Slik vi vurderer dette så vil det gi flere positive effekter og egner seg derfor godt til å styrke arbeidet med informasjonssikkerhet i forvaltningen.

Utenriksdepartementet

Generelt mener vi det er positivt at Digdir tar initiativ til et tverrsektorielt samarbeid for å sikre en felles retning på arbeidet med informasjonssikkerhet i offentlig forvaltning.

For å lykkes med initiativet om felles og mer helhetlig informasjonssikkerhet i offentlig forvaltning, mener vi det er viktig at alle relevante fagmyndigheter på sikkerhetsområdet legger til grunn den samme strategiske tilnærmingen for sitt arbeid og i relevant veiledningsmateriell.

Nærings- og fiskeridepartementet

Vi forventer at behovet for samarbeid med andre sektorer vil øke i tiden som kommer og imøteser en enda mer helhetlig tilnærming til arbeidet med informasjonssikkerhet i offentlig sektor.

Klima- og miljødepartementet

Tilbakemeldinger – departementer

Det er positivt hvis Digdir kan ta et overordnet ansvar for å koordinere og samle veiledninger og anbefalinger.

KS

KiNS stiller seg bak den beskrevne strategiske retningen og mener det et presserende behov for et nasjonalt løft for informasjonssikkerhet generelt og digital sikkerhet spesielt.

KiNS

NSM synes det er et godt initiativ og det bygger videre på prosjekter og samarbeid knyttet til informasjonssikkerhet i offentlig forvaltning som Digdir har holdt i de siste årene.

Nasjonal sikkerhetsmyndighet (NSM)

Vår vurdering er at tiltakene som beskrives er hensiktsmessige, men ambisjonsnivået for tiltakene er høyt. Tiltakene vil derfor kreve implementering over lang tid.

Direktoratet for høyere utdanning og kompetanse (HK-dir)

Vi støtter at Digdir starter arbeidet med å utforme en tydeligere felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter.

Direktoratet for forvaltning og økonomistyring (DFØ)

Dette arbeidet er meget viktig og det framlagte utkastet er og solid grunnlag for et godt videre arbeid.

Datatilsynet

Det er positivt at Digitaliseringsdirektoratet tar initiativ til å gjøre noe med dette.

Aktørene må instrueres til å samarbeide og samarbeidet må koordineres.

Direktoratet for e-helse

Foreslåtte tiltak

Felles referanseramme

Katalog med oppgaver/tjenester og informasjonstyper

Basisnivåer med sikkerhetstiltak

Felles tiltaksbank

Kategorier og nivåer av konsekvenser

Spesialtilpassede basisnivåer med sikkerhetstiltak

Ny lov om informasjonssikkerhet i offentlig forvaltning

Digdirs anbefalinger

Utvikle felles referanseramme

Utvikling og utprøving av mulige tiltak i forvaltningen

Samarbeid

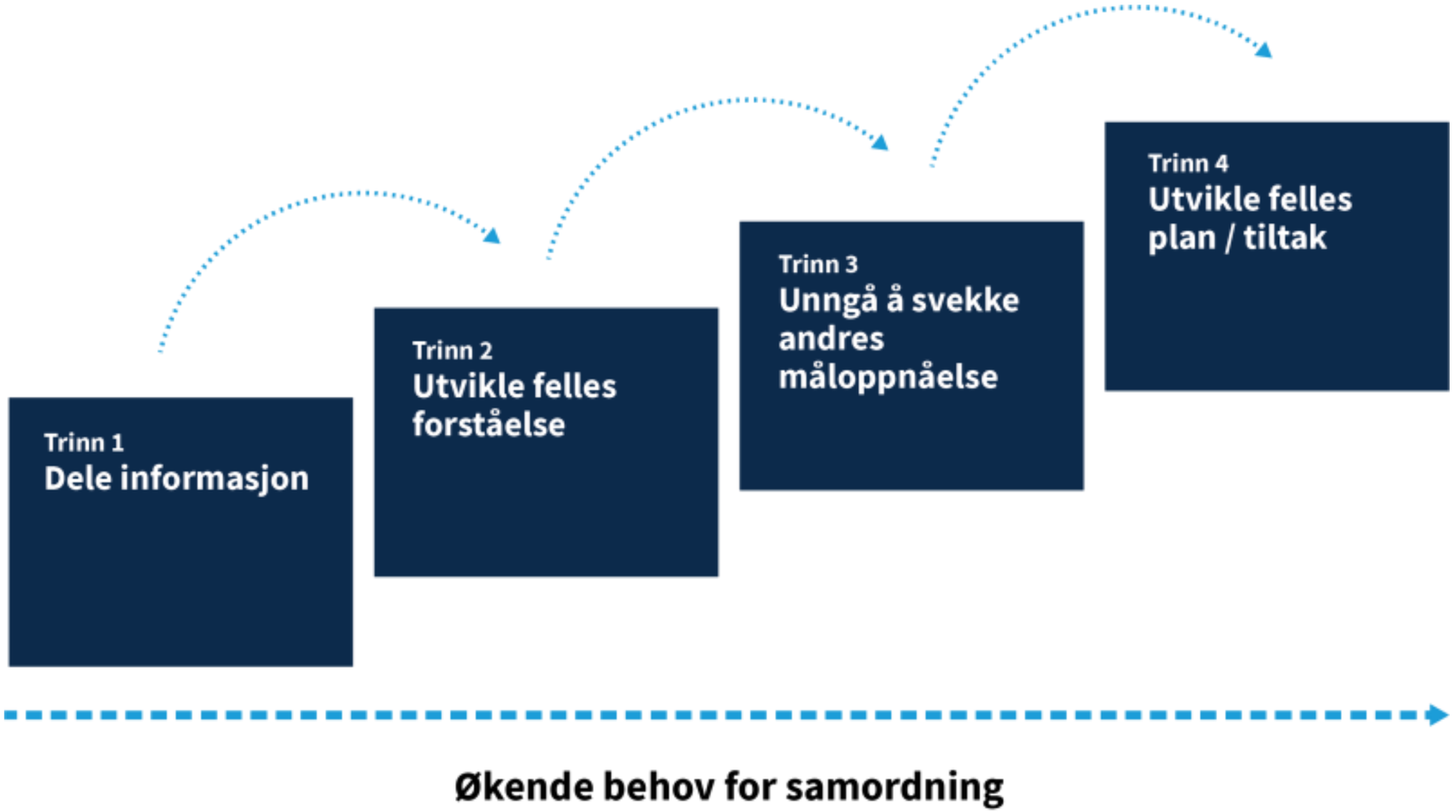
Koordinering på departementsnivå

Veien videre siden notatet - samarbeid

Opprettet styringsgruppe

- Ledet av Digdir
- KS
- DFØ
- Datatilsynet
- NSM
- Direktoratet for e-helse

Samordningsstigen



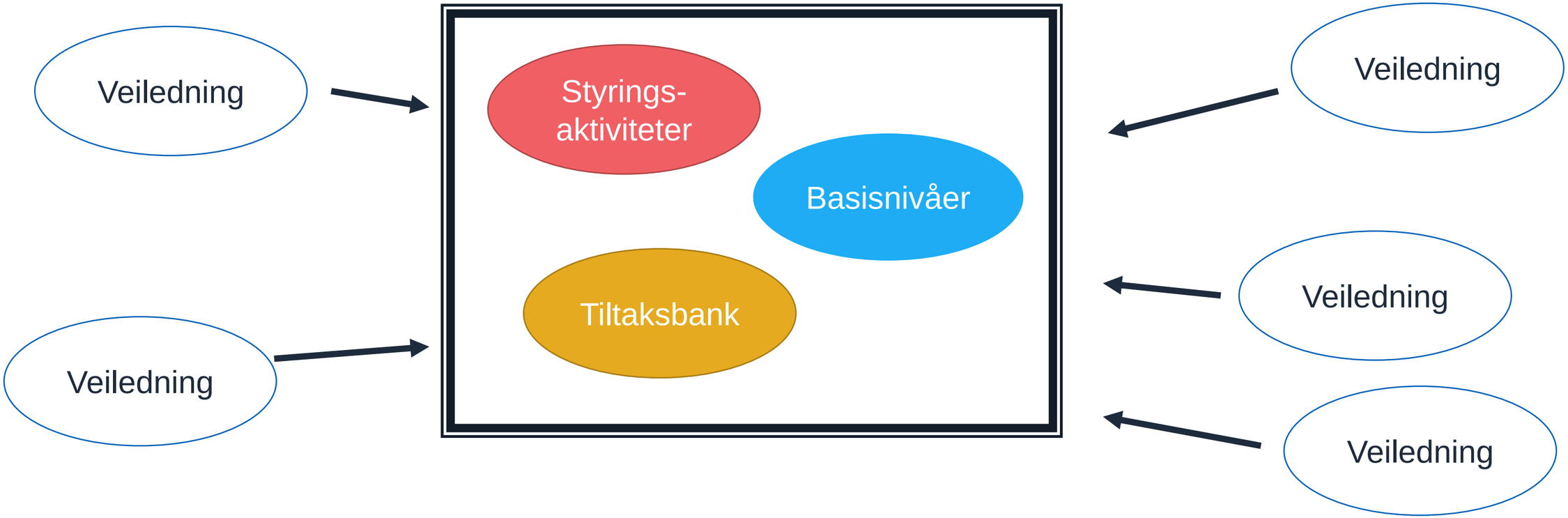
DFØ | Samordning
https://dfo.no/fagomrader/etats-og-virksomhetsstyring/samordning

Arbeid med felles referanseramme

→ → → et felles og samordnet målbilde

Felles referanseramme

Felles referanseramme
Et ***helhetlig konsept*** for forvaltningen



Digdirs anbefaling

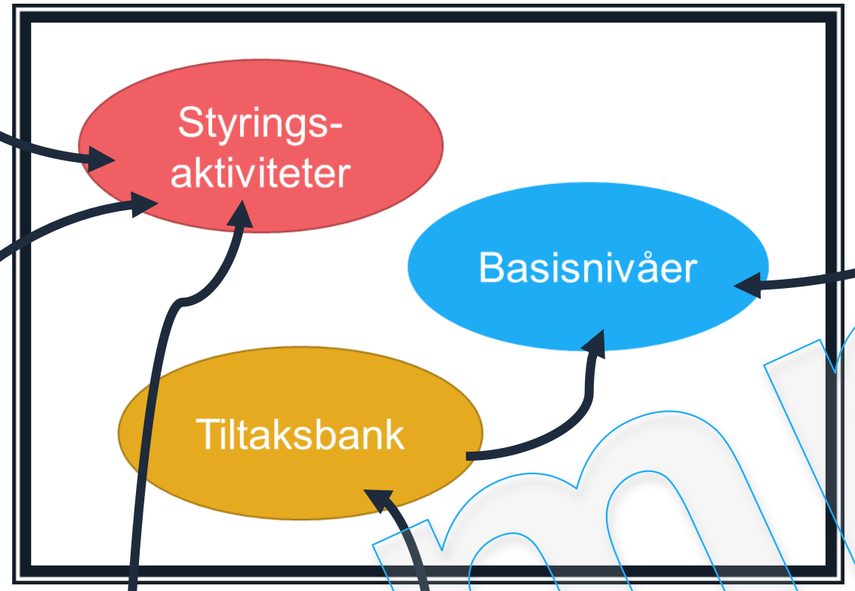
Digdir

Internkontroll i praksis - informasjonssikkerhet

Metode for kartlegging av sikkerhetskultur

KS

Spesifikt om styringsaktiviteter i kommuner



digdir.no

Veiledning til innføring av ulike nivåer

Veiledning på innføring av konkrete tiltak

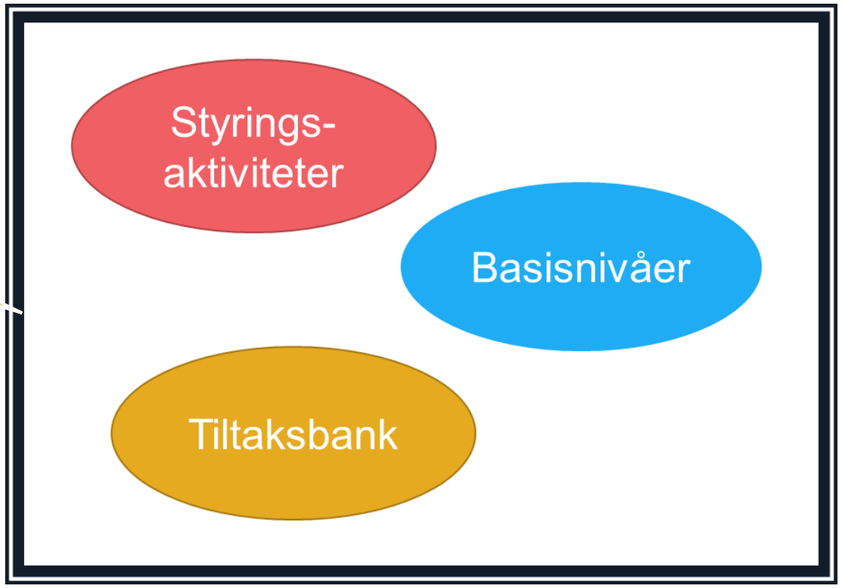
Direktoratet for e-helse

Spesifikt om styringsaktiviteter i helsesektoren

NSM

Direktoratet for e-helse

Tydeligere
gjeldende anbefalinger



Mer operativ og
resultatorientert hjelp


Styrings-
aktiviteter

Eksempler – Styringsaktiviteter

Fellestrekk for styring og kontroll

Det er noen grunnleggende aspekter ved styring og kontroll som er felles for flere fagområder. Ved å se sammenhengen mellom ulike fagområder, kan virksomheten jobbe målrettet, effektivt og koordinert med styring og kontroll.

På denne siden

Eksempler – Styringsaktiviteter (2)

- Styringsaktiviteter i Digdirs veiledning

- Anbefalinger for hovedaktiviteter

1 Ledelsens styring og oppfølging

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten som inkluderer tilstrekkelig informasjonssikkerhet. Dette skal gjøres ved å ha styringsaktiviteter som gjennomføres systematisk hele virksomheten, og å etablere tilstrekkelige sikkerhetstiltak for virksomhetens oppgaver og tjenester.

Virksomhetens ledelse sørger for å

- få etablert og følge opp styringsaktivitetene
- gi føringer for styringsaktivitetene og det øvrige arbeidet med informasjonssikkerhet
- sørge for tilstrekkelig ressurser til arbeidet med informasjonssikkerhet
- følge opp at styringsaktivitetene fungerer godt og gjøre nødvendige endringer ved behov
- følge opp at virksomhetens oppgaver og tjenester har tilstrekkelig informasjonssikkerhet

- Anbefalinger for delaktiviteter

1.1 Virksomhetsledelses gjennomgang

Virksomhetsledelsen skal minimum årlig gå gjennom status for styring og kontroll på informasjonssikkerhetsområdet. Omfang og innretning skal være tilpasset risiko og vesentlighet.

Gjennomgangen skal bidra til å

- avklare status på virksomhetens arbeid med informasjonssikkerhet
- vurdere om styringsaktivitetene fungerer effektivt og gir ønskede resultater
- avklare status på områder og tjenester der virksomhetsledelsen er spesielt opptatt av informasjonssikkerheten
- avklare status på risikoer eller risikoområder virksomhetsledelsen er spesielt opptatt av
- avklare status på endringer og andre beslutninger fra tidligere gjennomganger
- å oppsummere vesentlige avvik i informasjonssikkerheten og arbeidet med styring og kontroll
- vurdere tilbakemeldinger på informasjonssikkerhetsarbeidet, slik som avvik, resultater fra måling eller evaluering, resultater fra revisjoner, status på regelverksetterlevelse
- avklare om kulturen i virksomheten understøtter informasjonssikkerhetsmålene og et systematisk arbeid med styring og kontroll
- avklare om det har vært endringer i rammebetingelser
- gi ledelsen kunnskap om lokale, nasjonale og internasjonale trender rundt trusler, uønskede hendelser og risikoer
- ta beslutninger om forbedring og andre endringer, og finansiering av disse

Ved behov for mer informasjon om status, bør virksomhetsleder beslutte at virksomheten skal måle tilstanden på indikatorer over tid, eller få gjennomført evalueringer eller internrevisjon.

Virksomhetsleder skal på bakgrunn av gjennomgangen gi eventuelle nye eller oppdaterte føringer for styringsaktivitetene og øvrig arbeid med informasjonssikkerhet, og sørge for at disse finansieres og iverksettes.

Den informasjonen som utarbeides for, og gjennomgås i, denne aktiviteten bør benyttes til å utarbeide og kommunisere styringsinformasjon til overordnet, styrende organ – for eksempel til en statlig virksomhets styringsdialog med sitt departement.

Spørsmål?

Digdir.no/infosikkerhet

Infosikkerhet@digdir.no

digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarevegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo