Dialogverktøy – støtte til styringsdialogen om informasjonssikkerhet

Om dialogverktøyet

Dette dialogverktøyet er et hjelpemiddel til styringsdialogen om informasjonssikkerhet mellom departement og virksomhet. Målgruppen består primært av dere som er etatsstyrere i departementene, men verktøyet kan også være nyttig for virksomheter. Dialogverktøyet kan dere benytte både som forberedelse til og i selve styringsdialogen.

Dialogverktøyet må brukes sammen med *Miniveileder om oppfølging av informasjonssikkerhet i styringsdialogen*.

Dialogverktøyet beskriver hvilke temaer som det kan være relevant å ta opp i styringsdialogen. Om temaene skal tas opp, hvordan de skal tas opp og behandles, eller hvilke spørsmål som skal stilles, må – i likhet med all annen etatsstyring – tilpasses egenart samt risiko og vesentlighet. Verktøyet passer ikke alle tenkelige behov eller for oppfølgingen av alle statlige virksomheter.

Innholdet er basert på krav og anbefalinger i lov, forskrift og veiledninger. Verktøyet er likevel ikke ment å fungere som en fasit, men som et hjelpemiddel dere kan bruke i dialogen mellom departement og underliggende virksomhet.

Alt i dialogverktøyet handler om arbeidet med informasjonssikkerhet i en virksomhet. For eksempel, står det «styring og kontroll», så menes «styring og kontroll på informasjonssikkerhetsområdet».

Struktur

Dialogverktøyet er delt i to – en hoveddel og en fordypningsdel:

Hoveddelen tar for seg overordnede vurderinger av risiko, status og utfordringer i tillegg til virksomhetenes styringssystem. Oppfølging på dette overordnede nivået vil normalt være tilstrekkelig for å vurdere om arbeidet med informasjonssikkerhet er tilfredsstillende: Arbeidet på dette nivået er noe alle etatsstyrere bør være i stand til å ivareta. Nærmere bestemt vil det si at departementet påser at det er etablertgod nok internkontroll i virksomheten, framfor at det undersøker konkrete tiltak og aktiviteter.

Fordypningsdelen kan dere bruke når det er nødvendig å gå mer grundig inn i enkelte temaer for styring og kontroll på informasjonssikkerhetsområdet. Fordypningsdelen – som benyttes når behovet for det er vurdert og fastlagt – har fire deler:

- Systematiske aktiviteter for styring og kontroll
- Sikkerhetstiltak
- Etterlevelse av regelverk
- Spesielle temaer

Behovet for å gå nærmere inn i innholdet i og i hvilken struktur den underliggende virksomheten har på internkontrollsystemet, etablerte sikkerhetstiltak og etterlevelse av regelverk, baseres på vurdering av egenart samt risiko og vesentlighet. Et eksempel er der etatsstyrer vurderer at informasjonssikkerhetsarbeidet i virksomheten ikke er tilfredsstillende, og at det er nødvendig å gå gjennom arbeidet mer detaljert for å dekke departementets behov for styringsinformasjon og ivareta det overordnede ansvaret. I fordypningsdelen vil det være behov for hjelp fra personer med fagkompetanse innen risikostyring generelt og informasjonssikkerhet spesielt.

Vedlegg A beskriver hvordan innholdet i de enkelte delene er bygget opp.

Forarbeid

Godt utbytte av bruken av dialogverktøyet avhenger av at det foreligger en overordnet forståelse av risiko, vesentlighet og vurdering av egenart. Disse spørsmålene kan benyttes i forbindelse med slike vurderinger:

- Hvilken betydning har oppgavene og tjenestene virksomheten har ansvaret for?
- Hvilken betydning har informasjonsbehandling for disse oppgavene og tjenestene?
- Hva kan konsekvensene bli ved informasjonssikkerhetsbrudd i oppgaver og tjenester?
- I hvilken grad kan informasjonssikkerhetsbrudd få konsekvenser for virksomheten selv, eksempelvis for virksomhetens økonomi og tjenestenivå og for ansatte, og for andre utenfor, slik som innbyggere, andre virksomheter, samfunnsfunksjoner eller nasjonale sikkerhetsinteresser?
- Hvilken betydning har digitale tjenester og bruk av informasjonsteknologi for oppgaveløsningen?
- Har rammevilkårene endret seg? (som strategiske valg, oppgaveportefølje, regelverk og teknologisk utvikling)
- Hva er virksomhetens behov for utvikling og innovasjon, og hvilken betydning har informasjonssikkerhet i tilknytning til dette?

Hvordan verktøyet kan benyttes

Dialogverktøyet kan benyttes i forskjellige etatsstyringsaktiviteter. Det kan for eksempel benyttes i forbindelse med

- planlegging og oppfølging av etatsstyringsmøter
- overordnet dialog om, eller vurdering av, virksomhetens arbeid med styring og kontroll generelt og informasjonssikkerhet spesielt
- arbeid med styringsdokumenter som instruks, tildelingsbrev og årsrapport

Du finner mer informasjon om når det er aktuelt å tenke informasjonssikkerhet i etatsstyringsdialogen, i veileder til oppfølging av informasjonssikkerhet.

Det kan for eksempel være at du som er etatsstyrer, allerede har god oversikt over virksomhetens risiko, vesentlighet og egenart, inkludert hvilken betydning virksomhetens oppgaver og tjenester har – men ønsker bedre innsikt i hvilken betydning informasjonsbehandling generelt, og bruk av digital teknologi spesielt, har for virksomhetens oppgaver og tjenester. Eller kanskje er det slik at du ønsker mer informasjon om hvordan ledelsen i virksomheten arbeider med informasjonssikkerhet.

Dette er bare et eksempel på når verktøyet kan brukes – innholdet i dialogverktøyet, og støttematerialet det er lenket til, kan gi støtte i mange forskjellige situasjoner.

HOVEDDEL – STYRINGSDIALOG OM INFORMASJONSSIKKERHET

Overordnet om risiko, status og utfordringer

Denne delen av dialogverktøyet tar for seg hvordan risiko knyttet til informasjonsbehandling påvirker virksomhetens mål og resultater. Det handler om å ha overordnet oversikt over risiko, vite hvilken betydning informasjonsbehandling har for virksomhetens oppgaver og tjenester, og få greie på om virksomheten lykkes i arbeidet med informasjonssikkerhet. I hovedsak handler det om styringsinformasjonen ledelsen presenterer som et resultat av at de har god styring og kontroll, og i mindre grad om hvordan de går fram for å få det til.

Hensikt: En gjennomgang av denne delen vil gi deg som er etatsstyrer, innsikt i om ledelsen har tilstrekkelig oversikt over risiko, er i stand til å styre risiko, og gi overordnet oversikt over status på arbeidet med informasjonssikkerhet. Det vil bidra til å gi kunnskap om resultatene fra internkontrollarbeidet: ledelsens oversikt over risiko, ressursbruk og informasjonssikkerhetsarbeidets betydning for virksomhetens mål og resultater. En gjennomgang av dette gir deg evnen til å gjøre en overordnet vurdering av om ledelsen lykkes med styring og kontroll på informasjonssikkerhetsområdet.

Overordnede spørsmål:

- Har ledelsen oversikt over hvilken betydning informasjonssikkerhet har for virksomhetens oppgaver og tjenester og for å ivareta andre lovpålagte forpliktelser?
- Er arbeidet med informasjonssikkerhet en integrert del av virksomhetens risikostyring og internkontroll?
- Kan ledelsen redegjøre overordnet om hvordan de lykkes i arbeidet med informasjonssikkerhet?

Indikerer god styring og kontroll
Ledelsen beskriver informasjonssikkerhetsområdet på en tilfredsstillende måte og knytter det til styring av risiko for virksomhetens oppgaver og tjenester.
Ledelsen beskriver områder med høy(ere) risiko. Eksempler kan være enkelte oppgaver eller tjenester, prosjekter eller etterlevelse av regelverk. (Det er snakk om risiko knyttet til primær måloppnåelse, ikke risiko «for informasjonssikkerheten».)
Ledelsen gir en overordnet oversikt over svært høye risikoer de har akseptert, eller redegjør for svært høye risikoer som har vært akseptert siden sist. Redegjørelsen beskriver grunnlaget for beslutningene i den grad det er nødvendig.

Ledelsen redegjør overordnet for endringer i rammebetingelser som påvirker arbeidet med informasjonssikkerhet eller risiko på området. Eksempler er • endringer i oppgaver og tjenester • endringer i regelverk som de må ta hensyn til • trusselutvikling nasjonalt, internasjonalt eller knyttet til det virksomheten driver med • bruk av ny teknologi i oppgaveløsningen
Ledelsen redegjør for tilstand og modenhet i arbeidet med informasjonssikkerhet.
Ledelsen beskriver prioriteringer og ressursbruk for arbeidet med informasjonssikkerhet på et overordnet nivå.
Ledelsen tar opp spesielle problemer og utfordringer i arbeidet med informasjonssikkerhet og beskriver hvordan de løser disse.
Ledelsen redegjør for vesentlige behov for investeringer til, eller omstilling av, arbeidet med informasjonssikkerhet – og hvordan de går fram for å håndtere dette. Eksempler er • styrking av de ledelsesstyrte systematiske aktivitetene for styring og kontroll • investering for å etablere sikkerhetstiltak det er behov for • behov for ressurser til å vurdere og håndtere risiko i forbindelse med omstilling av oppgaveløsningen, for eksempel bruk av ny teknologi eller tjenesteutsetting

Kan indikere manglende styring og kontroll
Ledelsen beskriver detaljer i internkontrollen i stedet for • å redegjøre overordnet om måloppnåelse og risiko • å formidle den oversikten og styringsinformasjonen som god styring og kontroll gir dem
Ledelsen gir inntrykk av at dette er noe som styres av andre roller i virksomheten, uten at ledelsen har oversikt selv.
Ledelsen gir inntrykk av at det er teknisk IT-fag som omtales, i stedet for virksomhetens måloppnåelse og risiko.

Ledelsen beskriver hva som kan skje i teknologi og IT-komponenter, uten å relatere dette til konsekvenser for virksomhetens oppgaver og tjenester.
Ledelsen beskriver detaljer i teknologi som benyttes, i stedet for å redegjøre for styring av risiko for oppgaver og tjenester som teknologien understøtter.
Ledelsen trekker bare fram deler av det de skal ivareta, uten å redegjøre for helheten. For eksempel kan beskrivelsen deres være begrenset til • bare behov for konfidensialitet (f.eks. knyttet til taushetsplikt) • bare konsekvenser for personer når de behandler opplysninger om dem (personvern) • bare konsekvenser for nasjonale sikkerhetsinteresser
Informasjonssikkerhet er ikke en sentral del av virksomhetens arbeid med tjenesteutvikling, innovasjon og bruk av digital teknologi.

Støttemateriale

Les mer om sammenhengen mellom risikostyring og internkontroll her:

https://dfo.no/fagomrader/risikostyring/sammenhengen-mellom-risikostyring-og-internkontroll

Styringssystem

Denne delen handler om systematisk arbeid på informasjonssikkerhetsområdet og tar for seg hvordan ledelsen oppnår god informasjonssikkerhet ved å bruke styringssystemet som sitt redskap for å ha styring og kontroll. Denne delen av verktøyet ser på styringssystematikken som helhet. Dersom styringssystemet fungerer godt, vil ledelsen kunne redegjøre for alt i hoveddelen av dialogverktøyet på en god måte.

Systematisk gjennomføring av aktiviteter for styring og kontroll på informasjonssikkerhetsområdet

Hensikt: En gjennomgang av denne delen vil gi deg som er etatsstyrer, innsikt i hvordan ledelsen styrer arbeidet med informasjonssikkerhet. Å undersøke om virksomheten har tilstrekkelig styring og kontroll på dette området, er en del av oppfølgingen av styring og kontroll og risikostyringen i virksomheten som helhet. Ettersom flere forskjellige regelverk stiller krav til at virksomheten skal ha dette, så vil det også gi innsikt i etterlevelse av regelverk.

Overordnede spørsmål:

- Hvordan har ledelsen innrettet styringssystemet som sitt redskap for å ha styring og kontroll på informasjonssikkerhetsområdet?

Indikerer god styring og kontroll
Ledelsen har oversikt over de systematiske aktivitetene for styring og kontroll med informasjonssikkerhet og kan redegjøre for disse.
Styring og kontroll av informasjonssikkerhet er en integrert del av styring og kontroll i virksomheten.
Internkontrollens struktur og innhold er lagt opp i tråd med gjeldende krav og anbefalinger. Eksempler er • eForvaltningsforskriften § 15 andre ledd, med krav om helhetlig styring som ivaretar krav i ulike regelverk • Digitaliseringsdirektoratets veiledning • sikkerhetsloven, med krav om sikkerhetsstyring som en del av virksomhetsstyringen
Virksomheten har systematiske aktiviteter som dekker det som er anbefalt: • ledelsens styring og oppfølging • risikovurdering • risikohåndtering • overvåking og hendelseshåndtering • måling, evaluering og revisjon • kompetanse- og kulturutvikling • kommunikasjon

Kan indikere manglende styring og kontroll
Ledelsen ser ikke på styringssystemet som sitt redskap for å ha styring og kontroll på området.
Informasjonssikkerhet styres for seg selv – uten knytning til virksomhets- og risikostyringen ellers.
Virksomheten har en rekke dokumenter, policy og retningslinjer, men kan ikke redegjøre for hvordan arbeidet blir gjennomført i praksis.

Ledelsen beskriver ikke styringsaktiviteter, inkludert aktiviteter for å foreta gode beslutninger om ressursbruk, prioritering og risiko tilknyttet de oppgavene og tjenestene de har ansvaret for.
Ledelsen beskriver hovedsakelig forskjellige sikkerhetstiltak uten å vektlegge de ledelsesstyrte systematiske aktivitetene for å styre informasjonssikkerhetsområdet. (Styringsaktivitetene inkluderer aktiviteter for å vurdere risiko og håndtere risiko – bl.a. for å velge sikkerhetstiltak.)

Organisering av informasjonssikkerhetsarbeidet

Hensikt: En gjennomgang av denne delen vil gi deg som er etatsstyrer, innsikt i hvordan ledelsen har organisert arbeidet i virksomheten. Dette inkluderer roller, ansvar og myndighet for å gjennomføre og følge opp de systematiske aktivitetene (styringsaktivitetene).

Overordnede spørsmål:

- Er organiseringen oversiktlig, og er det tydelig hvem som har ansvaret for hva i arbeidet med informasjonssikkerhet i virksomheten?
- Er ansvaret for å styre risiko på dette området en del av ledelsesansvaret for virksomhetens oppgaver og tjenester?

Indikerer god styring og kontroll
Virksomhetens leder har en «fagansvarlig informasjonssikkerhet» (eller liknende rolle eller stabsfunksjon) som støtter ledelsen i arbeidet, og samarbeidet fungerer godt.
Ansvaret for å vurdere og håndtere risiko innen informasjonssikkerhet er delegert ordinær linjevei, slik at det ivaretas av dem som har ansvaret for virksomhetens primære mål og resultater. (Risiko styres, og beslutninger tas, av dem som har ansvaret for virksomhetens oppgaver og tjenester, men de får støtte fra «fagansvarlig informasjonssikkerhet» eller liknende rolle.)
«IT-avdelingen» og liknende funksjoner fungerer som tiltaksleverandører og har ansvar for å forvalte sikkerhetstiltak. De bistår også risikoeiere i å vurdere og håndtere risiko.
Arbeidet med informasjonssikkerhet og finansieringen av dette er inkludert i virksomhetsplanleggingen og virksomhetens budsjett.

Kan indikere manglende styring og kontroll
Virksomheten har en «fagansvarlig informasjonssikkerhet» (eller liknende) som utfører det meste av oppgavene uten at ledelsen er involvert.
Styring av risiko på området er delegert til IT-avdelingen, eller det forventes håndtert av andre roller, for eksempel personvernombud eller sikkerhetsleder.

Arbeidet med informasjonssikkerhet er formåls- og kostnadseffektivt

Hensikt: En gjennomgang av denne delen vil gi deg som er etatsstyrer, innsikt i om styringssystemet fungerer formåls- og kostnadseffektivt.

Overordnede spørsmål:

- Hvordan vurderer og påser ledelsen at arbeidet med informasjonssikkerhet er formålseffektivt?
- Er ledelsen i stand til å prioritere ressursinnsatsen på arbeidet med informasjonssikkerhet – for eksempel til oppgaver og tjenester hvor behovet er størst?
- Er arbeidet med informasjonssikkerhet kostnadseffektivt?

Indikerer god styring og kontroll
Ledelsens vurdering er at styringssystemet fungerer, og at det er et godt redskap som gir evne til å styre.
Arbeidet understøtter måloppnåelsen og bidrar til at virksomheten får utført sine oppgaver og levert tjenester.
Det er tilstrekkelig med ressurser til arbeidet med informasjonssikkerhet.
Virksomhetens leder har overordnet oversikt over informasjonsbehandlingen og kan redegjøre for hvilken betydning informasjonsbehandlingen har for oppgaver og tjenester.
Virksomhetens leder vet hvilke konsekvenser informasjonssikkerhetsbrudd kan få – både for virksomhetens oppgaver og tjenester og for individer, andre virksomheter og samfunnet.
Ledere i virksomheten er i stand til å prioritere arbeidet med risiko til de områdene hvor de potensielle konsekvensene ved informasjonssikkerhetshendelser er størst.

Ledere i virksomheten evaluerer eget arbeid med informasjonssikkerhet og benytter det til å kontinuerlig forbedre formåls- og kostnadseffektivitet.

Kan indikere manglende styring og kontroll
Virksomhetens leder kjenner ikke til i hvilke av virksomhetens oppgaver og tjenester informasjonssikkerhetsbrudd kan få størst konsekvenser.
Virksomhetens leder kan ikke redegjøre for ressursbruk og prioriteringer.
Å gjennomføre styringsaktivitetene er svært ressurskrevende, og de er ikke i stand til å få gjort alt som skal gjøres.
Ledere i virksomheten vurderer ikke jevnlig behovet for å gjennomføre nærmere vurdering av risiko innen sitt ansvarsområde, slik at ressursbruken på risikovurderinger framstår som tilfeldig, lite prioritert, mangelfull eller for omfattende.

Støttemateriale

Les mer i veiledningen som gir anbefalinger til virksomhetenes arbeid med styring og kontroll på informasjonssikkerhetsområdet:

http://internkontroll-infosikkerhet.difi.no/

Disse delene kan være av spesiell interesse for etatsstyrere:

- Virksomhetskontekst
- Overordnet om de systematiske aktivitetene
- Regelverkskrav

Finn anbefalte standarder og veiledning til forvaltningen her:

https://www.difi.no/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet

Vurder behov for å gå dypere inn i enkelte tema

Du som er etatsstyrer bør alltid vurdere om det er spesielle temaer det er behov for å gå nærmere inn på.Ulike strategiske valg: Virksomheten gjør strategiske valg, for eksempel større endringer i oppgaveløsningen. Det kan være behov for å ta opp informasjonssikkerhet i forbindelse med anskaffelsesstrategi og tjenesteutsetting eller i forbindelse med å utnytte mulighetene som ny teknologi gir for å løse oppgaver og levere tjenester på nye måter.

- Regelverksendringer: Endringer i regelverk som stiller krav til arbeidet med informasjonssikkerhet, eller hvor informasjonssikkerhet har vesentlig betydning, gjør at virksomheten må tilpasse arbeidet sitt med informasjonssikkerhet, og departementet ønsker å vite hvordan dette er ivaretatt.

Dette er spesielt relevante eksempler, men andre behov er også aktuelle.

Dersom det er slike behov – bruk fordypningsdelen.

FORDYPNING I TEMAER KNYTTET TIL INFORMASJONSSIKKERHET

Noen ganger kan det være behov for en mer inngående dialog om og oppfølging av informasjonssikkerhetsområdet. Vurderinger av egenart, risiko og vesentlighet legger et grunnlag slik at departementet og virksomheten kan vurdere om styringsdialogen om temaet informasjonssikkerhet krever fordypning. Fordypningsdelen benyttes ved behov for å gå nærmere inn i spesifikke deler av informasjonssikkerhetsarbeidet, som innhold og struktur på underliggende virksomhets internkontrollsystem, etablerte sikkerhetstiltak og etterlevelse av regelverk.

Det vil vanligvis være behov for hjelp fra personer med spesialkompetanse innen informasjonssikkerhet, risikostyring og internkontroll for å gå inn i disse delene. Det vil også være behov for at fagpersoner i underliggende virksomhet bidrar aktivt.

Systematiske aktiviteter for styring og kontroll

Dialogen om denne delen går mer i detalj på innholdet i og strukturen på noen av de sentrale aktivitetene innen styring og kontroll på informasjonssikkerhetsområdet – styringsaktiviteter som gjennomføres rundt omkring i virksomheten. Det er snakk om ledelsesstyrte aktiviteter for å gi føringer for hvordan arbeidet skal foregå i virksomheten, hvordan de skal prioritere arbeidet, utrede behov, beslutte bruk av ressurser, undersøke om arbeidet er effektivt, holde oversikt og ha tilstrekkelig styringsinformasjon mv.

Det er anbefalt at virksomhetene har (varianter av) disse hovedaktivitetene:

- Ledelsens styring og oppfølging
- Risikovurdering
- Risikohåndtering
- Overvåkning og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling
- Kommunikasjon

Hensikt: En gjennomgang av dette området vil gi deg som er etatsstyrer, innsikt i innholdet i forskjellige styringsaktiviteter i virksomheten.

Overordnede spørsmål:

- Er strukturen og innholdet i styringsaktivitetene hensiktsmessig og i henhold til gjeldende krav og anbefalinger?

Indikerer god styring og kontroll
Virksomhetens leder har gitt tydelige føringer for aktivitetene: hva som skal gjøres, hvordan det skal gjøres, og hvem som har ansvaret for at det blir gjort.
Ledere rundt omkring i virksomheten holder oversikt over informasjonsbehandlingen i sine oppgaver og tjenester. De har oversikt over informasjonstyper som behandles, aktuelle regelverk, IKT-systemer og digitale tjenester som benyttes, og hvor store konsekvensene kan bli ved sikkerhetsbrudd («verdivurdering»).
Virksomheten benytter sin oversikt over informasjonsbehandlingen til å prioritere arbeidet med informasjonssikkerhet. For eksempel kan det gjelde hvor og når det er behov for å gjøre nærmere vurdering av risiko, eller hvor det skal prioriteres å bruke ressurser til sikkerhetstiltak.
Risikoeiere vurderer regelmessig risiko i tilknytning til oppgavene og tjenestene virksomheten har ansvar for.
Virksomheten har ledelsesstyrt aktivitet for håndtering av risiko, som blant annet kan inkludere • valg av alternativer for å håndtere risiko • kriterier for å akseptere risiko • godkjenning av forslag til hvordan risiko skal håndteres
Kriteriene for å akseptere risiko fungerer godt og gir ledere i virksomheten god støtte til å ta slike beslutninger.
Ved beslutning om å etablere sikkerhetstiltak vurderes kostnader, antatt effekt og mulige negative sideeffekter.
Virksomheten gjennomfører systematisk godkjenning og etablering av sikkerhetstiltak. Dette kan inkludere • beslutning om, og finansiering av, etablering av sikkerhetstiltak • avtaler med tiltaksleverandører om ansvar for utforming, etablering og forvaltning av sikkerhetstiltak
Risikoeiere vurderer status på sine ansvarsområder minst en gang i året.
Tiltaksleverandører vurderer status på sine ansvarsområder minst en gang i året.
Virksomheten vurderer behov for å evaluere av hele eller deler av internkontrollen på området eller å bruke indikatorer som gjør dem i stand til å følge utviklingen over tid.

Virksomheten har oversikt over sitt behov for kompetanse på informasjonssikkerhetsområdet.
Virksomheten klarer å dekke sitt behov for kompetanse på informasjonssikkerhetsområdet.
Ledere får nødvendig grunnopplæring for å kunne utføre sine oppgaver på en god måte. Grunnopplæringen dekker alle vesentlige roller i de systematiske aktivitetene.
Virksomheten har kartlagt eller målt sikkerhetskulturen og benytter kunnskapen til å styrke organisasjonen.
Virksomheten har vurdert om informasjonssikkerhetshendelser vil kunne føre til utfordringer med virksomhetskontinuitet.
Virksomheten har beredskap og er forberedt på å håndtere hendelser som utfordrer virksomhetens evne til å fungere, eller som fører til alvorlig svikt i oppgaver og tjenester.
Virksomheten har tydelige roller, ansvar og prosedyrer for hvordan de håndterer hendelser. Dette inkluderer hvordan ledelsen involveres strategisk og taktisk ved behov.
Virksomheten har god oversikt over hendelser og avvik. De benytter denne kunnskapen til å forbedre arbeidet.

Kan indikere manglende styring og kontroll
Virksomhetens leder har gitt føringer for arbeidet med informasjonssikkerhet, men aktivitetene gjennomføres ikke systematisk av ledere rundt omkring i virksomheten.
Virksomhetens arbeid med informasjonssikkerhet dekker ikke alle typer informasjon, IKT-systemer, digitale tjenester og uønskede hendelser. Omfanget er for eksempel begrenset til • personopplysninger • tilsiktede hendelser (menneskestyrte angrep)
Virksomheten har ikke tilstrekkelig oversikt over verdikjeder. Ledere i virksomheten har ikke oversikt over hvor avhengige de er av eksterne løsninger og tjenester, for eksempel hvor avhengige de er av nasjonale felleskomponenter og -løsninger.

Virksomheten vurderer ikke (informasjonssikkerhets)risiko ved oppstart og gjennomføring av utviklingsprosjekter og anskaffelsesprosesser.
Virksomheten vurderer risiko, men arbeider ikke systematisk for å håndtere risiko.
Virksomheten evaluerer ikke eget arbeid og har derfor liten mulighet til å drive kontinuerlig forbedring.
Ledelsen tar ikke ansvar for å utvikle god sikkerhetskultur.
Virksomheten bruker ikke hendelser til læring og forbedring.
Virksomheten har ikke oversikt over kostnadene som følge av informasjonssikkerhetshendelser.
Virksomheten arbeider ikke systematisk og målrettet med øvelser.
Virksomhetens kompetansetiltak er ikke tilpasset ulike målgrupper og behov.

Støttemateriale

Veiledningen som gir anbefalinger til virksomhetenes arbeid med styring og kontroll på informasjonssikkerhetsområdet, gir en beskrivelse av de systematiske aktivitetene: https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter

Et sammendrag, inkludert en grunnleggende innføring, er tilgjengelig i PDF-format:

https://internkontroll-infosikkerhet.difi.no/sammendrag

Sikkerhetstiltak

En av måtene virksomhetene håndterer risiko på, er ved å etablere og forvalte (informasjons)sikkerhetstiltak. Når disse er etablert og virker etter hensikten, er virksomheten i stand til å forebygge, oppdage og reagere på informasjonssikkerhetshendelser. Det handler om at virksomheten har sikkerhetstiltak tilpasset sine behov, at de følger opp om disse er effektive og ikke har unødige negative sideeffekter, og at forvaltningen av sikkerhetstiltakene er kostnadseffektiv. Det handler også om i hvilken grad virksomheten følger opp anbefalinger fra myndigheter, og om det er tilstrekkelig omfang på forskjellige typer av sikkerhetstiltak.

Effektiv etablering og forvaltning av sikkerhetstiltak

Hensikt: En gjennomgang av denne delen vil gi deg som er etatsstyrer, en oversikt over om virksomheten er i stand til å etablere og forvalte de sikkerhetstiltakene den har behov for, samt følge opp at disse fungerer etter hensikten, og at forvaltningen av dem er kostnadseffektiv.

Overordnede spørsmål:

- Er virksomheten i stand til å etablere og forvalte sikkerhetstiltak i et omfang som er hensiktsmessig?
- Har virksomheten tilstrekkelig oversikt over etablerte sikkerhetstiltak?

Indikerer god styring og kontroll
Virksomheten har hensiktsmessig oversikt over etablerte sikkerhetstiltak.
Virksomheten er i stand til å etablere og forvalte de sikkerhetstiltak som de har behov for.
Det er tydelig hvem som er ansvarlig for at sikkerhetstiltak er etablert og virker etter hensikten.
Risikoeiere, eller de som skal bistå dem med å vurdere risiko, har god oversikt over eksisterende, etablerte sikkerhetstiltak.
Virksomheten har etablert et grunnleggende sett med sikkerhetstiltak for all sin informasjonsbehandling (kalt «fellessikring» i Digitaliseringsdirektoratets veiledning).
Virksomheten har brukt anerkjente tiltaksbanker (rammeverk med sikkerhetstiltak) i valg av sikkerhetstiltak.
Virksomheten har benyttet veiledning fra myndighetsorganer i arbeidet med grunnleggende sikkerhetstiltak. De har for eksempel plukket grunnleggende sikkerhetstiltak fra Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet.
Virksomheten har et balansert sett med sikkerhetstiltak, med sikte på å forebygge, oppdage og håndtere hendelser.
Virksomheten evaluerer etablerte sikkerhetstiltak regelmessig for å finne ut om tiltakene virker etter hensikten og ikke har utilsiktede negative sideeffekter.

Kan indikere manglende styring og kontroll
Virksomheten er ikke i stand til å etablere og forvalte sikkerhetstiltakene de har behov for. Dette kan for eksempel skyldes

• budsjett • kompetanse
Virksomheten redegjør hovedsakelig for tekniske sikkerhetstiltak knyttet til IKT og snakker ikke om sikkerhetstiltak knyttet til fysisk og miljømessig sikring, tiltak rettet mot mennesker, tilrettelegging av arbeidsoppgaver eller andre relevante områder.
Virksomheten redegjør hovedsakelig for tiltak for å forebygge informasjonssikkerhetsbrudd og snakker ikke om evne til å oppdage og reagere på informasjonssikkerhetsbrudd.
Virksomheten jobber med å etablere alle sikkerhetstiltak fra en tiltaksbank (rammeverk med sikkerhetstiltak, f.eks. ISO/IEC 27002), uten å ha oversikt over risiko og egne behov.

Støttemateriale

Veiledningen som gir anbefalinger til virksomhetenes arbeid med styring og kontroll på informasjonssikkerhetsområdet, inneholder artikler med bakgrunnsinformasjon som kan gi dypere innsikt i hva sikkerhetstiltak er, og hvordan virksomheten kan organisere arbeidet med disse, se:

Hva er risikohåndtering?

Sikkerhetstiltak

Fellessikring og tilleggssikring

Tiltaksbanker

Etablering av anbefalte sikkerhetstiltak

Hensikt: En gjennomgang av denne delen vil gi deg som er etatsstyrer, en oversikt over om virksomheten har vurdert anbefalte sikkerhetstiltak fra anerkjente rammeverk som NSMs grunnprinsipper for IKT-sikkerhet i sitt arbeid med håndtering av risiko.

Regelverk spesifiserer i liten eller ingen grad detaljer i hvilke sikkerhetstiltak en virksomhet skal etablere. Å etablere alle disse sikkerhetstiltakene er derfor ikke påkrevet, og å etablere alle er heller ikke nødvendigvis tilstrekkelig for alle behov. De fleste virksomheter vil derimot ha behov for sikkerhetstiltak av alle typer, eller innen alle områder, som er nevnt her i denne delen.

Henvisningene av typen «[GP 1.1]» er referanser til NSMs grunnprinsipper for IKT-sikkerhet. Disse er tatt inn for å gjøre det enkelt å referere til utfyllende informasjon i veiledning fra Nasjonal sikkerhetsmyndighet.

Overordnede spørsmål:

- Benytter de anerkjente anbefalinger og veiledning, som NSMs grunnprinsipper for IKT-sikkerhet, når de velger og utformer sikkerhetstiltak?
- Har virksomheten alle relevante typer sikkerhetstiltak?

Indikerer god styring og kontroll
Virksomheten har identifisert og kartlagt leveranser, verdikjeder og IKT-ressurser som kan virke inn på risiko og valg av sikringstiltak. Dette inkluderer prinsipper for å • [GP 1.1] Kartlegge leveranser og verdikjeder • [GP 1.2] Kartlegge enheter og programvare • [GP 1.3] Kartlegge brukere og behov for tilgang
Virksomheten har etablert hensiktsmessige sikkerhetstiltak for å beskytte sine informasjonssystemer basert på ønsket risikonivå og i henhold til beste praksis. Dette inkluderer disse prinsippene: • [GP 2.1] Ivareta sikkerhet i anskaffelsesprosesser • [GP 2.2] Ivareta sikker design av IKT-miljø • [GP 2.3] Ivareta en sikker konfigurasjon • [GP 2.4] Ha kontroll på IKT-infrastruktur • [GP 2.5] Ha kontroll på kontoer • [GP 2.6] Ha kontroll på bruk av administrative privilegier • [GP 2.7] Kontrollerer dataflyt • [GP 2.8] Beskytte data i ro og i transitt • [GP 2.9] Beskytte e-post og nettleser • [GP 2.10] Etablere hensiktsmessig logging
Virksomheten har etablert mekanismer for å opprettholde etablert sikkerhetstilstand i informasjonssystemene og oppdage avvik fra ønsket tilstand. Dette inkluderer disse prinsippene: • [GP 3.1] Sørge for god endringshåndtering • [GP 3.2] Beskytte mot skadevare • [GP 3.3] Verifiserer konfigurasjon • [GP 3.4] Gjennomfører inntrengingstester og «red-team»-øvelser

Virksomheten er forberedt på å håndtere eventuelle hendelser som oppstår. Dette inkluderer disse prinsippene: • [GP 4.1] Forberede virksomheten på håndtering av hendelser • [GP 4.2] Vurdere og kategorisere hendelser • [GP 4.3] Kontrollere og håndtere hendelser • [GP 4.4] Evaluere og lære av hendelser
Virksomheten følger god praksis for systemutvikling. Informasjonssikkerhet er utformet og iverksatt i hele utviklingsprosessen til informasjonssystemer. Virksomheten har etablert regler for utvikling av programvare og systemer og benytter dette i forbindelse med utvikling i hele organisasjonen.

Virksomheten følger god praksis for fysisk og miljømessig sikkerhet og har etablert gode rutiner for dette.

Virksomheten har tatt hensyn til fysisk sikkerhet i forbindelse med sikre områder, inkludert

- fysiske sikkerhetssoner
- fysisk adgangskontroll
- sikring av kontorer, rom og fasiliteter
- beskyttelse mot eksterne og miljømessige trusler
- arbeid i sikre områder
- områder for varelevering

Virksomheten har tatt hensyn til fysisk sikkerhet i forbindelse med bruk av IKT-utstyr, inkludert

- plassering og beskyttelse av utstyr
- understøttende utstyr
- kablingssikkerhet
- vedlikehold av utstyr
- fjerning av aktiva
- sikring av utstyr og aktiva utenfor organisasjonen
- sikker avhending eller gjenbruk av utstyr
- uovervåket brukerutstyr
- policy for ryddig arbeidsplass og låst skjerm

Virksomheten følger god praksis for personellsikkerhet og har etablert gode rutiner for dette.

Virksomheten jobber for å skape en god virksomhetskultur og har gode rutiner for informasjonssikkerhet ved ansettelse, oppfølging og opphør av ansettelsesforhold.

Virksomheten har innført gode rutiner for kompetanseheving, opplæring og bevisstgjøring av ansatte.

Kan indikere manglende styring og kontroll

Virksomheten har bare delvis oversikt over kritiske IKT-systemer og informasjonsflyt til og fra disse systemene. Virksomheten har ikke oversikt over autorisert og uautorisert maskin- og programvare som benyttes i virksomheten. Virksomheten har manglende oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i virksomheten, og har ikke formaliserte retningslinjer for tilgangskontroll.
Informasjonssikkerhet er ikke en del av virksomhetens anskaffelsesprosess. Virksomheten har ikke etablert en helhetlig sikkerhetsarkitektur og mangler eller har mangelfull implementering av viktige sikkerhetsfunksjoner (for eksempel katalogtjenester, kryptografiske moduler, brannmurer, antivirus og verktøy for systemovervåkning). Alle brukere får lov til å laste ned, åpne og kjøre alle programmer fra e-post, fra nettleser eller fra USB-minnepinner. Informasjonssystemene er ikke inndelt i logiske soner. Alle brukere har i praksis tilgang til alle nettverksressurser. Maskin- og programvare er ikke tilstrekkelig konfigurert og tilpasses i liten grad for å tilfredsstille virksomhetens behov. Virksomheten har ikke tilfredsstillende kontroll på livssyklusen til kontoer: fra de opprettes, til de brukes og endres, og til de deaktiveres eller slettes. Virksomheten har manglende kontroll på tildeling og bruk av administrative privilegier. Sensitive virksomhetsdata beskyttes ikke tilfredsstillende på bærbare enheter og når det sendes over usikre medier, som internett. Virksomheten har gjort lite for å sikre e-post og nettlesere. Gamle programversjoner benyttes, og det er ikke aktivert tiltak for å verifisere avsender av e-post og sjekke vedlegg for skadevare. Virksomheten mangler systematisk innsamling av logger og andre sikkerhetsrelevante data fra aktuelle systemer. Dataene gjennomgås og analyseres i liten grad.

Endringsprosessen i virksomheten er uformell og dokumenteres ikke. Det er vanskelig å få oversikt over hvilke endringer som er planlagt, hvilke endringer som er gjennomført, og hvordan endringene har blitt godtatt og testet. Virksomheten har ikke oversikt over hvilke tiltak som er innført for å beskytte informasjonssystemene mot skadevare. Virksomheten har en adhoc rutine for installering av sikkerhetsoppdateringer. Datamaskiner, servere og nettverksutstyr mangler mange viktige sikkerhetsoppdateringer. Virksomheten mangler, eller har manglende implementering av, verktøy som beskytter mot kjent skadevare. Eksempler på slike verktøy er antivirus, brannmurer og antiskadevare. Inntrengingstesting benyttes sjelden eller aldri for å undersøke motstandskraften til informasjonssystemene. Virksomheten har mangelfulle rutiner for sikkerhetskopiering og gjenoppretting av data. Sikkerhetskopier og gjenoppretting testes sjelden eller aldri.
Virksomheten har et mangelfullt planverk for hendelseshåndtering for å ivareta behovet for virksomhetskontinuitet ved beredskap og krise. Planverket blir ikke testet tilstrekkelig i organisasjonen. Virksomheten har mangelfulle rutiner for å vurdere og kategorisere hendelser. Virksomheten har mangelfulle rutiner for kontrollere og håndtere hendelser. Virksomheten har få eller ingen rutiner for å evaluere og lære av hendelser.
Informasjonssikkerhet er bare delvis integrert i virksomhetens utviklingsprosesser. Virksomheten har ikke etablert klare regler for utvikling av programvare og systemer. Nye systemer som innføres, testes ikke systematisk før produksjonssetting.
Virksomheten stiller få eller ingen krav til fysisk sikkerhet ved sikring av bygg, kontorer og øvrige rom og fasiliteter, inkludert fysisk adgangskontroll.

Virksomheten har liten mulighet til å oppdage fysiske sikkerhetsbrudd, og sikkerhetsbrudd som oppstår, rapporteres i liten grad til ledelsen.
Virksomheten har få eller ingen etablerte rutiner for bakgrunnssjekk og verifisering av kvalifikasjoner for kandidater før ansettelse. Virksomheten er lite opptatt av kompetanseheving, opplæring og bevisstgjøring av ansatte.

Støttemateriale

Her finner du Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet:

https://www.nsm.stat.no/grunnprinsipper-ikt

Finn ut hva Datatilsynet sier om programvareutvikling med innebygget personvern:

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

Les mer om krav til sikkerhetstiltak i regelverk:

https://internkontroll-infosikkerhet.difi.no/godt-vite/risikohandtering/krav-i-regelverk

Etterlevelse av regelverk

Denne delen drar fram særlig relevant regelverk, spesielt tverrsektorielt regelverk som er relevant for alle statlige virksomheter. Ved behov for å ha dialog om etterlevelse av regelverk er det viktig at etatsstyrere også har oversikt over sektorregelverk og særlover som er relevante for den aktuelle virksomheten.

Innholdet i tabellen er prefikset med navn på regelverk som omtales, og kan benyttes der dette regelverket er relevant.

Hensikt: Ved gjennomgang av dette temaet vil du som er etatsstyrer, få innsikt i virksomhetens etterlevelse av regelverk.

Overordnede spørsmål:

- Har virksomheten oversikt over sine forpliktelser knyttet til informasjonssikkerhet i henhold til gjeldende regelverk?

- Kan virksomheten redegjøre for om de etterlever regelverk?
- Kan virksomheten redegjøre for hvordan de etterlever regelverk?

Indikerer god styring og kontroll
Forvaltningsloven: Virksomheten har styring og kontroll i tråd med eForvaltningsforskriften § 15 andre ledd, som er basert på anerkjent internasjonal standard og gjeldende anbefalinger for etterlevelse av bestemmelsen. Arbeidet med styring og kontroll med informasjonssikkerhet er en integrert del av virksomhetens helhetlige styringssystem og inkluderer relevante krav som er fastsatt i annen lov, forskrift eller instruks.
Sikkerhetsloven: Ledelsen viser god forståelse for innholdet i sikkerhetsloven med forskrifter og har oversikt over hvor sikkerhetsbrudd kan få konsekvenser for grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser.
Sikkerhetsloven: Sikkerhetsstyring etter denne loven er en del av virksomhetens styringssystem. Innholdet i de systematiske aktivitetene er tilpasset for å ivareta alle særkrav i dette regelverket i de tilfellene der det er behov for det.
Sikkerhetsloven: Virksomheten har etablert sikkerhetstiltak i tråd med minimumskravene, inkludert kravene i virksomhetsikkerhetsforskriften.
Sikkerhetsloven: Virksomheten kan redegjøre for hvordan de oppnår forsvarlig sikkerhetsnivå for det som skal sikres etter loven.
Personopplysningsloven m/personvernforordningen: Virksomheten behandler personopplysninger med tilstrekkelig sikkerhet og kan dokumentere etterlevelse av regelverket.
Virksomheten har god oversikt over hvilke særlover og sektorregelverk som gjelder informasjonsbehandlingen deres, og god forståelse for hvilke krav det stiller til deres arbeid med informasjonssikkerhet.

Kan indikere manglende styring og kontroll
Virksomheten har ikke oversikt over regelverk de er omfattet av.
Virksomheten håndterer forskjellige regelverk for seg, er ikke i stand til å se sammenhengene og har ikke en helhetlig oppfølging av dem.

Forvaltningsloven: Virksomheten har ikke styring og kontroll i tråd med eForvaltningsforskriften § 15 andre ledd og tilhørende anbefalinger.
Sikkerhetsloven: Virksomheten kan ikke redegjøre for pliktene de har etter sikkerhetsloven med forskrifter.
Personopplysningsloven m/personvernforordningen: Virksomheten har ikke oversikt over hvordan de bahndlerpersonopplysninger og hvilket behov det er for å sikre personopplysningene med tanke på konfidensialitet, integritet og tilgjengelighet for å ivareta fysiske personers rettigheter og friheter.

Spesielle temaer

De spesielle temaene som er tatt med, vil normalt kunne ha en naturlig plass i de generelle områdene over, men hensikten med dette området i verktøyet er å gi støtte til å gå dypere inn i særlig aktuelle temaer ved behov.

Det kan for eksempel være behov for særskilt dialog om anskaffelsesstrategi og tjenesteutsetting eller om hvilken betydning informasjonssikkerhet har i forbindelse med at virksomheten skal utnytte mulighetene som ny teknologi gir. Det kan også være behov for dialog om hvilken innvirkning eksisterende og kommende trender kan få for virksomheten og innretningen av arbeidet med informasjonssikkerhet.

Hensikt: En gjennomgang av spesielle temaer, etter behov, kan gi deg som er etatsstyrer, dypere innsikt i relevante aspekter ved virksomhetens arbeid med informasjonssikkerhet når det er behov for det.

Overordnede spørsmål:

- Er virksomheten i stand til å holde seg oppdatert om trusselbildet og benytte det i sine vurderinger?
- Er virksomheten i stand til å holde seg oppdatert om teknologiutviklingen?
- I hvilken grad er virksomheten i stand til å utnytte ny, relevant teknologi og tilgjengelige digitale tjenester?

Indikerer god styring og kontroll

Virksomheten er kjent med oppdaterte vurderinger av trender og trusselbildet fra relevante myndigheter. Det kan for eksempel være snakk om informasjon fra • Nasjonal sikkerhetsmyndighet (NSM) / Nasjonalt cybersikkerhetssenter • Datatilsynet • Politiets sikkerhetstjeneste (PST) • Etterretningstjenesten • Direktoratet for samfunnssikkerhet og beredskap (DSB) • Digitaliseringsdirektoratet
Virksomheten er kjent med oppdaterte vurderinger av trender og trusselbildet fra relevante kilder nasjonalt og internasjonalt.
Virksomheten har innsikt i relevant ny teknologi og innovative måter å utvikle og levere digitale tjenester på.
Virksomheten er i stand til å realisere gevinstene av å ha god informasjonssikkerhet i sine innbyggerrettede tjenester.

Kan indikere manglende styring og kontroll
Virksomheten har få eller ingen rutiner for å holde seg oppdatert på det aktuelle trusselbildet og kommende, teknologiske trender. Virksomheten har få eller ingen rutiner for å vurdere hvilken innvirkning aktuelle trusler og kommende teknologiske trender kan ha for virksomheten.
Virksomheten utvikler nye tjenester med ny teknologi uten at informasjonssikkerhet er inkludert i arbeidet.
Virksomheten er ikke kjent med sikkerhetsutfordringene de kan møte i forbindelse med ny teknologi som de ønsker å ta i bruk, eller teknologi som de blir nødt til å forholde seg til.
Virksomheten har ikke oversikt over hvilke skytjenester de benytter, og leverandører av disse.
Virksomheten vurderer og håndterer ikke risiko knyttet til digital sikkerhet i forbindelse med tjenesteutsetting og bruk av skytjenester, eller arbeidet med dette er utilstrekkelig.

Støttemateriale

Veiledning om offentlige anskaffelser finner du her:

https://www.anskaffelser.no/

Veileder om ivaretakelse av sikkerhet i offentlige anskaffelser kan du lese her:

https://www.regjeringen.no/no/dokumenter/veileder-om-ivaretakelse-av-sikkerhet-i-offentlige-anskaffelser/id2678434/

Temarapport om tjenesteutsetting fra Nasjonal sikkerhetsmyndighet kan du laste ned her:

https://www.nsm.stat.no/aktuelt/temarapport-tjenesteutsetting/

Vedlegg A – innholdselementene

Hver del har en innledende beskrivelse av hva delen skal handle om. Deretter følger disse elementene:

Hensikt – beskriver hva du som er etatsstyrer, kan oppnå ved gjennomgang av den delen.

Overordnede spørsmål – formulerer essensen av hva denne delen skal gi innsikt i, som spørsmål. Det kan bidra til forståelse av hva denne delen dreier seg om. I tillegg kan de overordnede spørsmålene også benyttes til å lage innledende spørsmål som kan brukes i møter mellom departement og underliggende virksomhet.

Tabeller med indikatorer – inneholder en liste med utsagn eller beskrivelser av tilstand. Innholdet i den første tabellen kan benyttes som indikatorer på god styring og kontroll. I den andre tabellen beskrives forhold som kan indikere manglende styring og kontroll.

Det er ikke direkte sammenheng mellom innholdet i de to tabellene, og alt har ikke en positiv og en negativ omtale. En del typiske og kjente problemsymptomer er vektlagt i tabellen med forhold som kan indikere mangler i styring og kontroll.

Indikerer god styring og kontroll
«positive utsagn»

Kan indikere manglende styring og kontroll
«negative utsagn»

Støttemateriale – inneholder referanser til annen veiledning som kan gi nyttig bakgrunnsinformasjon eller støtte i arbeidet.