A1. Styringssystem informasjonssikkerhet

Skal angi modenhet. F.eks.

- Styring i etterkant av avvik, ad hoc
- Delvis etablert, noe dokumentasjon, uklart skille mellom utøvende og kontrollerende
- Etablert roller, oppgaver og dokumentasjon i henhold til anerkjent standard
- God ledelsesforankring, regelmessige gjennomganger og kontinuerlig forbedring

A2. Risikostyring

Skal angi hvordan risikostyring brukes, er det kun for infosikkerhet eller del av helhetlig risikostyring?

- Ingen eller liten risikostyring for informasjonssikkerhet
- Risikovurdering i forkant av systemanskaffelser og etter alvorlige hendelser
- Regelmessig vurdering av risiko for informasjonssikkerhet
- Virksomhetsledelsen etterspør risiko relatert til informasjonssikkerhet som kan påvirke virksomhetens evne til å utføre oppgaver og levere tjenester

B1. Systematisk etablering av sikkerhetstiltak

I hvilken grad er tiltak etablert.

- Har ikke etablert noen av NSMs fire grunnleggende sikkerhetstiltak
- Har etablert ett til tre av NSMs fire grunnleggende sikkerhetstiltak
- Har etablert alle fire av NSMs grunnleggende sikkerhetstiltak

B2. Styring av sikkerhetstiltak

I hvilken grad det styres basert på kostnader / nytte.

- Det gjøres en årlig samlet vurdering av kostnader for sikkerhetstiltak.
- Kostnader, estimert nytteverdi og restrisiko vurderes før det skal besluttes om et sikkerhetstiltak skal etableres.
- Kostnader, estimert nytteverdi og restrisiko vurderes regelmessig for hvert enkelt sikkerhetstiltak fra det etableres til det besluttes å fase ut tiltaket.

C1. Øvelser

Modenhet.

- Virksomheten øver ikke regelmessig på uønskede hendelser som får konsekvenser for informasjonssikkerhet.
- Virksomheten øver på håndtering av uønskede hendelser som får konsekvenser for informasjonssikkerhet minst en gang i året.
- Virksomheten øver minst en gang i året og bruker erfaringer fra planlegging og gjennomføring av øvelser til å forbedre informasjonssikkerhet og risikovurderinger.

C2. Beredskapsplan

Enkel utgave (tilsvarer spørsmål fra SSB): Har virksomheten i løpet av de to siste årene oppdatert planer, rutiner eller tiltakskort for håndtering av hendelser som kan få konsekvenser for informasjonssikkerhet?

Alternativt modenhet

- Virksomheten har ikke planer eller rutiner/tiltakskort for håndtering av hendelser som kan få konsekvenser for informasjonssikkerhet
- Virksomheten har planer og rutiner/tiltakskort for håndtering av hendelser som kan få konsekvenser for informasjonssikkerhet
- Virksomheten har oppdatert planer, rutiner eller tiltakskort for håndtering av hendelser som kan for konsekvenser for informasjonssikkerheten.

C3. Hendelseshåndtering

Modenhet.

- Ad hoc (virksomheten håndterer uønskede hendelser når de oppstår)
- Virksomheten har etablert en egen gruppe som har ansvar for å lede håndtering av alvorlige uønskede hendelser som kan få konsekvenser for informasjonssikkerheten
- Virksomheten har etablert en egen gruppe som har ansvaret for fortløpende arbeid med å oppdage sikkerhetstruende hendelser og for å håndtere alvorlige hendelser som kan få konsekvenser for informasjonssikkerheten.

D1. Avhengighet (kritisk) av en eller flere nasjonale felleskomponenter

Enkel modenhet

- Virksomheten har ikke vurdert avhengighet
- Virksomheten har vurdert om den er avhengig av en eller flere nasjonale felleskomponenter for å utføre sine oppgaver eller for å levere sine egne tjenester

D2. Etablering av alternativ løsning ved midlertidig bortfall av nasjonal felleskomponent

Enkel modenhet

- Virksomheten har ikke vurdert alternative løsninger for å opprettholde virksomhetskontinuiteten ved midlertidig bortfall av en nasjonal felleskomponent.
- Virksomheten (er avhengig av en eller flere nasjonale felleskomponenter for å utføre sine oppgaver eller for å levere sine egne tjenester og) har vurdert mulige alternative løsninger for å opprettholde virksomhetskontinuiteten ved midlertidig bortfall av en nasjonal felleskomponent.

E1. Ledelsens forhold til sikkerhetskulturen i virksomheten

Modenhet

- Virksomheten har ikke kartlagt eller målt sikkerhetskulturen i egen organisasjon.
- Virksomheten har kartlagt eller målt sikkerhetskultur i egen organisasjon, men har ikke besluttet noen tiltak for å endre (forbedre) den eksisterende kulturen
- Virksomheten har kartlagt eller målt sikkerhetskultur i egen organisasjon, har planlagt eller gjennomført tiltak for å endre (forbedre) den eksisterende kulturen og målt effekten av slike tiltak.

E2. Kompetansetiltak

Modenhet

- Ad hoc (Virksomheten gjennomfører ikke noen planlagt opplæring eller kompetansehevende tiltak på området informasjonssikkerhet)
- Virksomheten har planlagt opplæring og kompetansehevende tiltak som gjennomføres for alle ansatte.
- Virksomheten har planlagt opplæring og kompetansehevende tiltak som er tilpasset de funksjoner, arbeidsoppgaver og forkunnskaper den enkelte medarbeider har.