HJORT

	NIS 1	NIS 2	CER	DORA	CRA	CSA
EU kortnavn	NIS Directive	NIS 2 Directive	Critical Entities Resilience Directive	Digital Operational Resilience Act	Cyber Resilience Act	Cyber Security Act
Formål	Sikre et høyt felles digitalt sikkerhetsnivå for nettverks- og informasjonssystemer (NIS) i EU.	Styrke sikkerhetskravene og samarbeidet ytterligere sammenlignet med NIS 1.	Styrke kritiske enheters, og fremme samarbeid innen EU.	Styrke digital motstandsdyktighet i finanssektoren.	Styrke sikkerheten til produkter med digitale elementer.	Sikre et høyt nivå av digital sikkerhet, og øke tilliten til IKT-produkter og -tjenester i EU, gjennom sertifisering og samarbeid
Type rettsakt	Direktiv	Direktiv	Direktiv	Forordning	Forordning	Forordning
Harmoniserings-nivå	Minimumskrav	Minimumskrav	Minimumskrav	Fullharmonisering	Fullharmonisering	Fullharmonisering
Vedtakelse EU	6. juli 2016	14. desember 2022	14. desember 2022	14. desember 2022	10. desember 2024	17. april 2019
Frist EU	Innen 10. mai 2018	Innen 17. april 2025 (etablere liste over essensielle og viktige enheter).	Innen 17. januar 2026 (for strategi).	Fra 17. januar 2025 (første rapport om sentralisering av rapportering).	Noen rapporteringskrav fra 20. november 2024, men de fleste fra 11. desember 2027	I kraft
Status Norge	Implementert gjennom Digitalsikkerhetsloven, som snart vil tre i kraft.	Ikke implementert eller inntatt i EØS-avtalen, men vurdert som EØS-relevant	Ikke implementert eller inntatt i EØS-avtalen, men vurdert som EØS-relevant	Foreslått implementert gjennom lov om digital motstandsdyktighet i finanssektoren, som ennå ikke er vedtatt.	Ikke implementert eller inntatt i EØS-avtalen, men vurdert som EØS-relevant	Ikke implementert eller inntatt i EØS-avtalen, men vurdert som EØS-relevant
Sektorer som omfattes	Energi, transport, bank, finansmarkedsinfrastruktur, helse, noen typer digital infrastruktur. Noen typer digitale tjenester.	I tillegg til NIS 1-sektorene: Flere typer digital infrastruktur og IKT-tjenester; offentlig forvaltning; romfart; avfallshåndtering; vannforsyning; produksjon og distribusjon av mat, kjemikalier, visse typer varer; forskning.	I hovedsak sektorer som er vurdert som vesentlige etter NIS 2.	Finanssektoren (kredittinstitusjoner, betalingsinstitusjoner, verdipapirforetak, forsikringsselskaper, etc.)	Elektronikk og programvare	Sektorer som benytter IKT-produkter og--tjenester og -prosesser, med fokus på samfunnsviktige sektorer.
Aktører som omfattes	Tilbydere av samfunnsvikrige tjenester innen angitte sektorer. Visse digitale tjenestetilbydere, som nærmere definert.	Store og mellomstore virksomheter innen de angitte sektorer, med visse unntak.	Nasjonale myndigheter, men også enheter som har kritisk infrastruktur i EU.	Virksomheter innen finanssektoren og deres leverandører.	Produsenter, importører og distributører av produkter med digitale elementer.	Produsenter og leverandører av IKT-produkter, IKT-tjenester og IKT-prosesser. Organisasjoner som utvikler eller bruker slike produkter, tjenester eller prosesser. Sertifiseringsorganer og akkrediteringsorganer.
Kjerneforpliktelser	Etablere sikkerhetstiltak, rapportere hendelser.	Etablere sikkerhetstiltak, rapportere hendelser, samarbeide med myndigheter og andre, leverandørstyring. Ulike krav til «vesentlige» og «viktige» enheter.	Foreta risikovurdering, gjøre tiltak for å styrke motstandsdyktigheten mot digitale hendelser.	IKT-risikostyrisng, hendelsesrapportering, digital motstandsdyktighet, leverandørstyring.	Oppfylle essensielle krav til digital sikkerhet for produkter med digitale elementer. Rapportere digitale sårbarheter og hendelser.	Regler om markedsføring og produktdesign. Krav om innebygget sikkerhet i produkter og innstillinger, livssyklussikkerhet, informasjon og åpenhet, serfisieringsordninger.
Risikotilnærming	Egnete og proporsjonale tiltak. Krav om å foreta risikovurderinger og implementere sikkerhetstiltak.	Proporsjonale og effektive tiltak. Krav om å foreta risikovurderinger og implementere sikkerhetstiltak.	Effektivitet og ansvarlighet. Krav om å foreta risikovurderinger og utvikle strategier.	Effektiv og forsvarlig håndtering av risiko. Krav om å foreta risikovurderinger.	Oppfylle essensielle krav til digital sikkerhet. Krav om å foreta kontinuerlige risikovurderinger.	Ulike sikkerhetsnivåer for sertifisering, tilpasset risikonivået.
Rapportering	Krav om å melde om hendelser som har en betydelig innvirkning på kontinuiteten	Krav om å melde om signifikante hendelser som har en betydelig innvirkning på tjenestene, samt digitale trusler og «nesten-hendelser».	Krav om at medlemsstatene skal rapportere til EU	Krav om å rapportere alvorlige IKT-relaterte hendelser.	Krav om å rapportere aktive utnyttede sårbarheter og alvorlige hendelser.	Produsenter skal gjøre EU-samsvarserklæring og teknisk dokumentasjon tilgjengelig for nasjonale myndigheter, Nasjonale myndigheter skal rapportere til EU.
Leverandørstyring	Ingen eksplisitte krav.	Krav om å implementere risikostyringstiltak, inkludert retningslinjer, for leverandørkjeden.	Ingen eksplisitte krav.	Krav om å styre risikoen knyttet til IKT tredjeparts tjenesteleverandører. Kritiske IKT-tredjepartsleverandører underlegges direkte tilsyn.	Ingen eksplisitte krav.	Ingen eksplisitte krav.
Utpeking og registrering	Medlemsstatene skal etablere en liste over tilbydere av samfunnsviktige tjenester.	Medlemsstatene skal etablere en liste over vesentlige og viktige enheter.	Medlemsstatene skal identifisere kritiske enheter.	Krav om å registrere avtaler med IKT tredjeparts tjenesteleverandører.	Ingen spesifikk utpeking eller registreringsplikt, men produktene må oppfylle kravene før markedsføring.	Medlemsstatene skal utpeke nasjonale sertifiseringsmyndigheter, og sertifiseringsorganer skal akkrediteres av nasjonale akkrediteringsorganer.
EU organer	ENISA, Computer Security Incident Response Team (CSIRT)-nettverk for samarbeid	ENISA, CSIRT-nettverk for samarbeid	Critical Entities Resilience Group	ESAs	ENISA (European Union Agency for Cybersecurity)	ENISA (European Union Agency for Cybersecurity), ECCG (European Cybersecurity Certification Group)
Tilsynsorgan Norge	NSM og ulike sektortilsyn	Antakelig videreføres NIS 1.	Ikke aktuelt	Finanstilsynet	Ikke bestemt	Ikke bestemt