kravklar

NIS2 Samsvarsvurdering

Nordmann Teknologi AS

23. mars 2026

Vurdering gjennomført: 23. mars 2026
Anbefalt ny vurdering innen: 23. september 2026

59%

Under arbeid

Basert på egenvurdering gjennomført 23. mars 2026

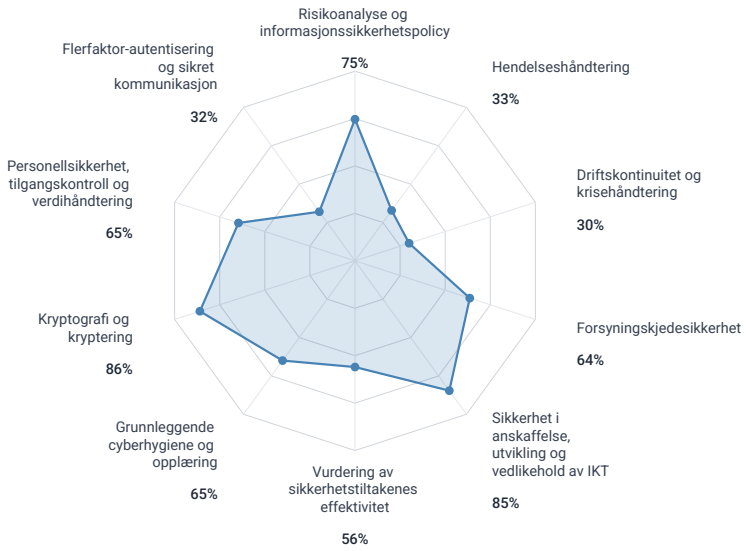
Erstatter ikke uavhengig revisjon eller juridisk rådgivning — se side 2.

Sammendrag

59% Virksomhetens samlede modenhetsnivå er vurdert til 59% (under arbeid). Vurderingen dekker 10 NIS2-kategorier basert på artikkel 21.

Vurdering gjennomført: 23. mars 2026 | Anbefalt ny vurdering innen: 23. september 2026

Modenhetsprofil per NIS2-kategori



Sterkeste kategorier

Kryptografi og kryptering: 86%

Sikkerhet i anskaffelse, utvikling og vedlikehold av IKT: 85%

Risikoanalyse og informasjonssikkerhetspolicy: 75%

Svakeste kategorier

Driftskontinuitet og krisehåndtering: 30%

Flerfaktor-autentisering og sikret kommunikasjon: 32%

Hendelseshåndtering: 33%

Denne rapporten er basert på en egenvurdering gjennomført 23. mars 2026 i Kravklar.no

Detaljert kategorioversikt

Risikoanalyse og informasjonssikkerhetspolicy — 75%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
1.1 Har virksomheten en dokumentert informasjonssikkerhetspolicy?	4 — Styrt	3 — Etablert	Ingen avvik	Utarbeid en informasjonssikkerhetspolicy som beskriver virksomhetens overordnede mål, prinsipper og ansvar for informasjonssikkerhet. Policyen bør forankres i ledelsen, godkjennes formelt og kommuniseres til alle ansatte. NSMs grunnprinsipper for IKT-sikkerhet er et godt utgangspunkt.
1.2 Gjennomfører dere regelmessige risikovurderinger av IT-systemer og data?	4 — Styrt	3 — Etablert	Ingen avvik	Gjennomfør en formell risikovurdering som dekker alle kritiske IKT-systemer, og dokumenter resultatene i et risikoregister. Bruk en enkel risikomatrise for å vurdere sannsynlighet og konsekvens, og gjenta prosessen minst årlig.
1.3 Er det tydelig definert hvem som har ansvar for informasjonssikkerhet i virksomheten?	4 — Styrt	3 — Etablert	Ingen avvik	Definer og dokumenter ansvarsfordelingen for informasjonssikkerhet, med en navngitt ansvarlig person for det daglige sikkerhetsarbeidet. Sørg for at toppledelsen er formelt involvert i sikkerhetsbeslutninger og at dette er nedfelt skriftlig.
1.4 Har dere en oversikt over virksomhetens viktigste informasjonsverdier og systemer?	4 — Styrt	3 — Etablert	Ingen avvik	Lag en strukturert oversikt over virksomhetens viktigste informasjonsverdier, systemer og datatyper. Klassifiser dem etter kritikalitet og bruk oversikten som grunnlag for å prioritere sikkerhetstiltak.
1.5 Vurderer dere risikoer knyttet til nye prosjekter eller systemendringer før de gjennomføres?	3 — Etablert	3 — Etablert	Ingen avvik	Innfør en enkel sikkerhetssjekkliste som gjennomgås ved nye prosjekter, systeminnkjøp eller vesentlige endringer. Vurder risikoer tidlig i prosessen slik at sikkerhet bygges inn fra starten.
1.6 Rapporteres risikovurderinger og sikkerhetsstatus til ledelsen?	3 — Etablert	3 — Etablert	Ingen avvik	Etabler en fast rutine for å rapportere sikkerhetsrisikoer og hendelser til ledergruppen eller styret, for eksempel kvartalsvis. Rapporten bør inkludere status på tiltak, nye risikoer og eventuelle hendelser.

Hendelseshåndtering — 33%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
2.1 Har virksomheten en dokumentert plan for håndtering av sikkerhetshendelser?	2 — Grunnleggende	3 — Etablert	1	Etabler en skriftlig hendelseshåndteringsplan med definerte roller, eskaleringsrutiner og varslingsprosedyrer. Planen bør dekke hvem som tar beslutninger, hvordan skaden begrenses, og hvordan kommunikasjonen håndteres internt og eksternt.
2.2 Har dere tekniske systemer for å oppdage sikkerhetshendelser (logging, overvåking, varsling)?	1 — Ikke påbegynt	3 — Etablert	2	Implementer sentralisert logging og overvåking av kritiske systemer, med automatiserte varsler ved mistenkelig aktivitet. Vurder en EDR-løsning (Endpoint Detection and Response) som er tilpasset virksomhetens størrelse og budsjett.
2.3 Vet ansatte hvordan de skal rapportere en mistenkelig hendelse internt?	2 — Grunnleggende	3 — Etablert	1	Lag en enkel og tydelig rutine for intern rapportering av sikkerhetshendelser, med ett kontaktpunkt (e-post, telefon eller skjema). Kommuniser rutinen til alle ansatte og gjenta den i sikkerhetsopplæringen.
2.4 Kjenner dere til NIS2s varslingskrav og har dere en prosess for å varsle relevante myndigheter?	2 — Grunnleggende	3 — Etablert	1	Kartlegg NIS2s varslingskrav: tidlig varsel til relevant myndighet innen 24 timer, og detaljert rapport innen 72 timer. Utpek en ansvarlig person for myndighetsvarsling, og lag en prosedyre med kontaktinformasjon, terskelvurdering og maler for varsling.
2.5 Gjennomfører dere evaluering etter sikkerhetshendelser for å lære og forbedre?	1 — Ikke påbegynt	3 — Etablert	2	Gjennomfør en systematisk evaluering etter hver sikkerhetshendelse eller nesten-hendelse. Dokumenter hva som skjedde, hva som fungerte, hva som sviktet, og hvilke tiltak som skal iverksettes for å hindre gjentakelse.
2.6 Har dere øvd på hendelseshåndtering gjennom tabletop-øvelser eller simuleringer?	2 — Grunnleggende	3 — Etablert	1	Planlegg og gjennomfør minst én årlig bordøvelse der nøkkelpersoner simulerer håndtering av et realistisk scenario, som for eksempel et ransomware-angrep. Dokumenter læringspunkter og oppdater hendelseshåndteringsplanen basert på funn.

Driftskontinuitet og krisehåndtering — 30%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
3.1 Har dere identifisert hvilke IT-systemer og tjenester som er kritiske for virksomhetens drift?	2 — Grunnleggende	3 — Etablert	1	Gjennomfør en konsekvensanalyse (BIA) for å identifisere kritiske systemer og tjenester, med definerte mål for akseptabel nedetid (RTO) og akseptabelt datatap (RPO). Prioriter gjenopprettingsarbeidet basert på virksomhetskritikalitet.
3.2 Tar dere regelmessig backup av kritiske systemer og data?	1 — Ikke påbegynt	3 — Etablert	2	Etabler automatiserte backup-rutiner for alle kritiske systemer og data, med lagring adskilt fra produksjonsmiljøet (offsite eller i en annen skytjeneste). Dokumenter hva som sikkerhetskopieres, hvor ofte, og hvor backupen lagres.
3.3 Har dere testet at backup faktisk kan gjenopprettes?	1 — Ikke påbegynt	3 — Etablert	2	Gjennomfør regelmessige gjenopprettingstester, minst årlig for kritiske systemer. Dokumenter testresultatene og eventuell feilretting slik at dere vet at backupen faktisk fungerer når dere trenger den.
3.4 Finnes det en dokumentert plan for driftskontinuitet (BCP) eller gjenoppretting (DRP)?	2 — Grunnleggende	3 — Etablert	1	Utarbeid en driftskontinuitetsplan (BCP) som beskriver hvordan virksomheten opprettholder kritisk drift under en krise, og en gjenopprettingsplan (DRP) for IT-systemene. Start med de mest kritiske prosessene og bygg ut planen over tid.
3.5 Har dere avtaler med leverandører som sikrer støtte ved alvorlige hendelser?	2 — Grunnleggende	3 — Etablert	1	Gjennomgå avtaler med kritiske IT-leverandører for å sikre at de inkluderer responstider (SLA), ansvarsfordeling ved hendelser, og støtte under krisesituasjoner. Vurder om det er behov for beredskapsavtaler.
3.6 Er krisehåndteringsplanen kommunisert til relevante ansatte?	1 — Ikke påbegynt	3 — Etablert	2	Sørg for at krisehåndteringsplanen er kommunisert til alle nøkkelpersoner utover IT, inkludert ledelse, HR og kommunikasjonsansvarlig. Gjennomfør en kort gjennomgang minst årlig slik at alle kjenner sin rolle.

Forsyningskjedesikkerhet — 64%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
4.1 Har dere oversikt over hvilke leverandører som har tilgang til deres systemer eller data?	3 — Etablert	3 — Etablert	Ingen avvik	Lag et leverandørregister som kartlegger alle leverandører med tilgang til systemer eller data, inkludert skytjenester. Dokumenter hvilken tilgang de har, hvilke data de behandler, og vurder risikonivået for hver leverandør.
4.2 Stiller dere sikkerhetskrav til leverandører ved innkjøp av IT-tjenester?	3 — Etablert	3 — Etablert	Ingen avvik	Inkluder sikkerhetskrav i alle kontrakter for IT-tjenester, som krav til kryptering, tilgangskontroll, hendelseshåndtering og varsling. Bruk en standardisert sjekkliste ved innkjøp for å sikre at sikkerhet vurderes systematisk.
4.3 Gjennomfører dere jevnlige vurderinger av leverandørenes sikkerhetspraksis?	3 — Etablert	3 — Etablert	Ingen avvik	Innfør en årlig gjennomgang av sikkerhetspraksis hos leverandører med tilgang til systemer eller data. Bruk et standardisert spørreskjema som dekker hendelseshåndtering, tilgangskontroll og backup. Prioriter leverandører etter risikonivå.
4.4 Har dere kontraktfestede rutiner for håndtering av sikkerhetshendelser hos leverandører?	4 — Styrt	3 — Etablert	Ingen avvik	Sørg for at kontrakter med IT-leverandører inkluderer krav om rask varsling ved sikkerhetshendelser, definert ansvarsfordeling, og rutiner for håndtering av data ved kontraktslutt. Gjennomgå eksisterende avtaler og oppdater ved behov.
4.5 Vurderer dere avhengighetsrisiko — hva skjer hvis en kritisk leverandør faller bort?	3 — Etablert	3 — Etablert	Ingen avvik	Kartlegg virksomhetens avhengighet av kritiske leverandører og vurder konsekvensene dersom en leverandør faller bort. Identifiser alternative leverandører eller tiltak som kan redusere avhengigheten.

Sikkerhet i anskaffelse, utvikling og vedlikehold av IKT — 85%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
5.1 Har dere rutiner for å holde programvare og systemer oppdatert (patching)?	4 — Styrt	3 — Etablert	Ingen avvik	Etabler en dokumentert rutine for regelmessig oppdatering av programvare og systemer, med prioritert håndtering av kritiske sikkerhetsfeil. Automatiser patching der det er mulig, og ha en prosess for å håndtere nødoppdateringer raskt.

Spørsmål	Nivå	Mål	Avvik	Anbefaling
5.2 Vurderes sikkerhet som en del av anskaffelsesprosessen for nye IT-løsninger?	4 — Styrt	3 — Etablert	Ingen avvik	Innfør sikkerhetsvurdering som en fast del av anskaffelsesprosessen for nye IT-løsninger. Bruk en sjekkliste som dekker kryptering, tilgangskontroll, logging, sertifiseringer og leverandørens sikkerhetsrutiner.
5.3 Hvis dere utvikler egen programvare — følger dere sikker utviklingspraksis?	4 — Styrt	3 — Etablert	Ingen avvik	Innfør grunnleggende sikker utviklingspraksis som inkluderer kodegjennomgang, bruk av OWASP Top 10 som referanse, og sikkerhetstesting før produksjonssetting. Vurder om dette også bør gjelde plugins og tilpasninger av standardprodukter.
5.4 Har dere en prosess for å fange opp og håndtere kjente sårbarheter i systemene deres?	5 — Optimalisert	3 — Etablert	Ingen avvik	Etabler en prosess for systematisk overvåking av kjente sårbarheter (CVE-er) i systemene dere bruker. Abonner på leverandørenes sikkerhetsvarsler og definer tidsfrister for patching basert på alvorlighetsgrad.
5.5 Har dere rutiner for sikker avvikling av systemer og sletting av data?	4 — Styrt	3 — Etablert	Ingen avvik	Lag en sjekkliste for avvikling av systemer som inkluderer sikker sletting av data, fjerning av tilganger, oppsigelse av lisenser og dokumentasjon av avviklingsprosessen.
5.6 Gjennomfører dere sikkerhetstesting (penetrasjonstesting, sårbarhetsskanning) av kritiske systemer?	4 — Styrt	3 — Etablert	Ingen avvik	Gjennomfør regelmessig sårbarhetsskanning av kritiske systemer og vurder behovet for penetrasjonstesting. Selv enkle automatiserte skannerverktøy kan avdekke kjente svakheter som bør utbedres.

Vurdering av sikkerhetstiltakenes effektivitet — 56%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
6.1 Evaluerer dere regelmessig om sikkerhetstiltakene fungerer som tiltenkt?	3 — Etablert	3 — Etablert	Ingen avvik	Innfør en fast årlig gjennomgang av sikkerhetstiltakenes effektivitet, der dere vurderer om tiltakene faktisk reduserer risiko som forutsatt. Kombiner gjennomgangen med resultater fra hendelser, tester og eventuelle revisjoner.
6.2 Har dere definert sikkerhetsmål eller KPI-er som dere følger opp?	3 — Etablert	3 — Etablert	Ingen avvik	Definer 3–5 enkle sikkerhetsmål eller KPI-er som følges opp regelmessig, for eksempel tid til patching, andel ansatte med gjennomført opplæring, eller antall hendelser per kvartal. Rapporter resultatene til ledelsen.
6.3 Gjennomfører dere interne eller eksterne revisjoner av informasjonssikkerheten?	2 — Grunnleggende	3 — Etablert	1	Gjennomfør en årlig intern gjennomgang av informasjonssikkerheten, eller vurder ekstern revisjon for kritiske områder. Dokumenter funn og sørg for at avvik følges opp med konkrete tiltak og frister.
6.4 Oppdaterer dere sikkerhetstiltak basert på nye trusler, hendelser, eller endringer i virksomheten?	3 — Etablert	3 — Etablert	Ingen avvik	Etabler en prosess for å vurdere og oppdatere sikkerhetstiltak ved vesentlige endringer i trusselbildet, etter hendelser, eller ved organisasjonsendringer. Koble dette til den årlige risikovurderingen.
6.5 Er det tydelig hvem som har ansvar for å følge opp at tiltak gjennomføres?	3 — Etablert	3 — Etablert	Ingen avvik	Tildel tydelig ansvar for hvert sikkerhetstiltak med navngitt eier, frist og oppfølgingspunkt. Bruk en enkel tiltakslogg som gjennomgås i faste ledermøter for å sikre at vedtatte tiltak faktisk gjennomføres.

Grunnleggende cyberhygiene og opplæring — 65%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
7.1 Gjennomfører alle ansatte regelmessig opplæring i informasjonssikkerhet?	3 — Etablert	3 — Etablert	Ingen avvik	Innfør obligatorisk sikkerhetsopplæring for alle ansatte minst årlig, med fokus på phishing, passordsikkerhet og rapportering av hendelser. Supplér med korte påminnelser eller mikrokurs gjennom året.
7.2 Har ledelsen (inkludert styret) gjennomgått opplæring i cybersikkerhet?	3 — Etablert	3 — Etablert	Ingen avvik	Gjennomfør dedikert opplæring i cybersikkerhet for ledelsen og styret, med fokus på risikoforståelse, ansvar under NIS2, og hvordan sikkerhet påvirker virksomheten. Dette bør gjøres minst årlig.
7.3 Har dere retningslinjer for passord og tilgangshåndtering som ansatte følger?	4 — Styrt	3 — Etablert	Ingen avvik	Utarbeid og distribuer retningslinjer for passord og tilgangshåndtering som inkluderer krav om sterke, unike passord og bruk av passordmanager. Sørg for at reglene er praktiske og at etterlevelse følges opp.
7.4 Gjennomfører dere phishing-tester eller andre	4 —	3 —	Ingen	Start med en enkel, simulert phishing-kampanje for å måle

Spørsmål	Nivå	Mål	Avvik	Anbefaling
bevissthetskampanjer?	Styrt	Etablert	avvik	bevisstheten blant ansatte. Bruk resultatene til målrettet opplæring, og gjenta testen kvartalsvis for å spore forbedring.
7.5 Har nyansatte en onboarding-prosess som dekker informasjonssikkerhet?	3 — Etablert	3 — Etablert	Ingen avvik	Inkluder en fast modul om informasjonssikkerhet i onboarding-prosessen for nyansatte, som dekker virksomhetens sikkerhetsregler, rapporteringsrutiner og forventninger til sikker atferd.
7.6 Er det klare regler for bruk av private enheter (BYOD) og hjemmekontor?	3 — Etablert	3 — Etablert	Ingen avvik	Utarbeid retningslinjer for bruk av private enheter og hjemmekontor som dekker krav til enhetsikkerhet, VPN-bruk og håndtering av sensitiv informasjon utenfor kontoret.

Kryptografi og kryptering — 86%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
8.1 Er data kryptert under overføring (f.eks. HTTPS, VPN, kryptert e-post)?	4 — Styrt	3 — Etablert	Ingen avvik	Sørg for at all ekstern kommunikasjon skjer over krypterte kanaler: HTTPS for nettsider, VPN for fjerntilgang, og TLS for e-post. Verifiser at konfigurasjonene er oppdaterte og bruker sterke krypteringsalgoritmer.
8.2 Er sensitive data kryptert ved lagring (at rest)?	5 — Optimalisert	3 — Etablert	Ingen avvik	Verifiser at sensitive data er kryptert ved lagring i databaser, filsystemer og backup-løsninger. For skytjenester, bekreft at kryptering er aktivert og forstå hvem som kontrollerer krypteringsnøklene.
8.3 Har dere en policy for bruk av kryptografi som beskriver når og hvordan kryptering skal brukes?	4 — Styrt	3 — Etablert	Ingen avvik	Utarbeid en enkel krypteringspolicy som definerer minimumskrav for når og hvordan kryptering skal brukes, hvem som er ansvarlig, og hvilke algoritmer og nøkkellengder som er godkjent.
8.4 Har dere rutiner for håndtering av krypteringsnøkler (key management)?	4 — Styrt	3 — Etablert	Ingen avvik	Etabler rutiner for sikker håndtering av krypteringsnøkler, inkludert hvem som har tilgang, hvordan de oppbevares, og hvor ofte de roteres. For skytjenester, avklar ansvarsfordelingen med leverandøren.
8.5 Bruker dere krypterte kanaler for deling av sensitiv informasjon internt og eksternt?	5 — Optimalisert	3 — Etablert	Ingen avvik	Innfør en godkjent løsning for sikker deling av sensitiv informasjon internt og eksternt, og kommuniser til alle ansatte at klartekst-e-post ikke skal brukes for sensitive data.

Personellsikkerhet, tilgangskontroll og verdihåndtering — 65%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
9.1 Har dere en oversikt over hvem som har tilgang til hvilke systemer og data?	3 — Etablert	3 — Etablert	Ingen avvik	Lag en tilgangsmatrise som dokumenterer hvem som har tilgang til hvilke kritiske systemer og data. Oppdater matrisen ved personellendringer og gjennomgå den regelmessig.
9.2 Praktiserer dere prinsippet om minste privilegium (least privilege)?	3 — Etablert	3 — Etablert	Ingen avvik	Innfør prinsippet om minste privilegium ved å gjennomgå eksisterende tilganger og fjerne unødvendige rettigheter. Definer standardtilganger per rolle, og gi kun utvidede rettigheter ved dokumentert behov.
9.3 Har dere en rutine for å fjerne tilganger når ansatte slutter eller bytter rolle?	3 — Etablert	3 — Etablert	Ingen avvik	Etabler en sjekkliste for offboarding som sikrer at alle systemtilganger fjernes umiddelbart når ansatte slutter. Integrer prosessen med HR slik at IT varsles automatisk ved oppsigelser og rolleendringer.
9.4 Gjennomfører dere bakgrunnssjekk for ansatte i sensitive roller?	4 — Styrt	3 — Etablert	Ingen avvik	Vurder behovet for bakgrunnssjekk for roller med tilgang til spesielt sensitive systemer eller data, tilpasset virksomhetens bransje og risikonivå. Dokumenter kriteriene for hvilke roller dette gjelder.
9.5 Har dere en oppdatert oversikt over virksomhetens IT-verdier (hardware, programvare, data)?	4 — Styrt	3 — Etablert	Ingen avvik	Opprett og vedlikehold en oppdatert oversikt over virksomhetens IT-verdier (hardware, programvare, lisenser og data). Bruk en enkel inventarliste eller et CMDB-verktøy, og definer eierskap for hvert element.
9.6 Gjennomgår dere tilganger regelmessig (access review)?	3 — Etablert	3 — Etablert	Ingen avvik	Innfør regelmessig tilgangsgjennomgang, for eksempel kvartalsvis for kritiske systemer og årlig for øvrige. Dokumenter gjennomgangen og sørg for at unødvendige tilganger fjernes fortløpende.

Flerfaktor-autentisering og sikret kommunikasjon — 32%

Spørsmål	Nivå	Mål	Avvik	Anbefaling
10.1 Er flerfaktor-autentisering (MFA) aktivert for tilgang til kritiske systemer?	2 — Grunnleggende	3 — Etablert	1	Aktiver flerfaktor-autentisering (MFA) for alle kritiske systemer, med prioritet på e-post, VPN, admin-kontoer og skyportaler. Bruk app-basert MFA (f.eks. Microsoft Authenticator eller lignende) fremfor SMS der det er mulig.
10.2 Er MFA aktivert for alle brukere, eller kun utvalgte?	2 — Grunnleggende	3 — Etablert	1	Utvid MFA til å gjelde alle brukere i virksomheten, ikke bare IT-personell og administratorer. Et kompromittert vanlig brukerkonto kan brukes som springbrett for videre angrep.
10.3 Bruker dere sikrede kommunikasjonskanaler for sensitiv intern kommunikasjon?	1 — Ikke påbegynt	3 — Etablert	2	Velg og standardiser en kryptert kommunikasjonskanal for sensitiv intern kommunikasjon (f.eks. Teams, Slack med enterprise-kryptering, eller Signal). Kommuniser til alle ansatte hvilken kanal som skal brukes for sensitiv informasjon.
10.4 Har dere en plan for nødkommunikasjon hvis primære kommunikasjonskanaler er utilgjengelige?	1 — Ikke påbegynt	3 — Etablert	2	Utarbeid en plan for nødkommunikasjon som inkluderer alternative kontaktmetoder (telefonnumre, kryptert meldingsapp) for nøkkelpersonell. Distribuer listen og test at den fungerer minst årlig.
10.5 Har dere vurdert og begrenset bruken av SMS som autentiseringsmetode?	2 — Grunnleggende	3 — Etablert	1	Vurder risikoen ved SMS-basert MFA for høy-risiko tilganger og migrer til app-basert eller hardware-basert autentisering der det er mulig. Behold SMS-basert MFA kun for systemer der bedre alternativer ikke er tilgjengelige.

Prioritert handlingsplan

Tiltak sortert etter prioritet (vekting × avvik). Høyest prioritet øverst.

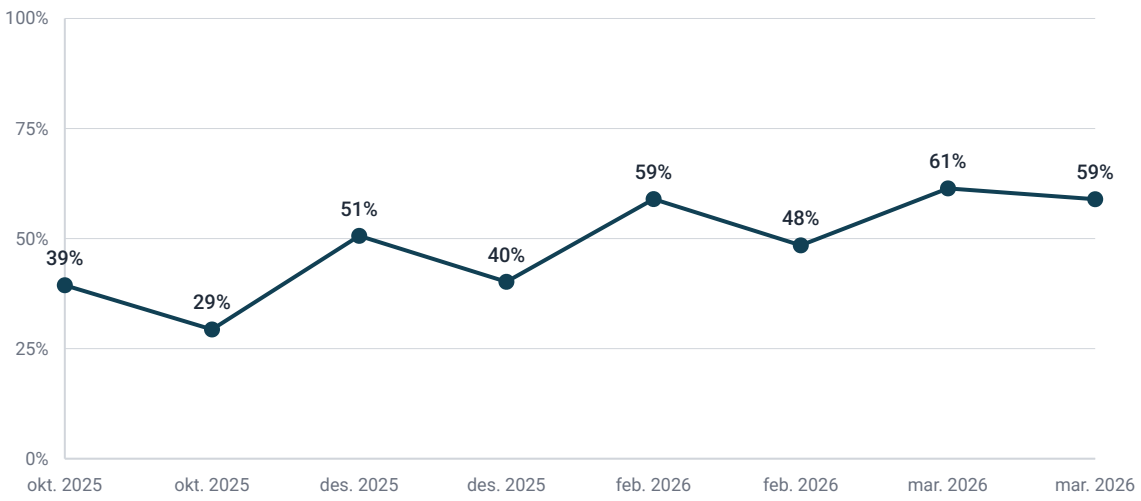
#	Kategori	Tiltak	Nåværende	Mål	Vekting
1	Hendelseshåndtering	2.2 Har dere tekniske systemer for å oppdage sikkerhetshendelser (logging, overvåking, varsling)? Implementer sentralisert logging og overvåking av kritiske systemer, med automatiserte varsler ved mistenkelig aktivitet. Vurder en EDR-løsning (Endpoint Detection and Response) som er tilpasset virksomhetens størrelse og budsjett.	1 — Ikke påbegynt	3 — Etablert	Kritisk
2	Driftskontinuitet og krisehåndtering	3.2 Tar dere regelmessig backup av kritiske systemer og data? Etabler automatiserte backup-rutiner for alle kritiske systemer og data, med lagring adskilt fra produksjonsmiljøet (offsite eller i en annen skytjeneste). Dokumenter hva som sikkerhetskopieres, hvor ofte, og hvor backupen lagres.	1 — Ikke påbegynt	3 — Etablert	Kritisk
3	Driftskontinuitet og krisehåndtering	3.3 Har dere testet at backup faktisk kan gjenopprettes? Gjennomfør regelmessige gjenopprettingstester, minst årlig for kritiske systemer. Dokumenter testresultatene og eventuell feilretting slik at dere vet at backupen faktisk fungerer når dere trenger den.	1 — Ikke påbegynt	3 — Etablert	Kritisk
4	Hendelseshåndtering	2.5 Gjennomfører dere evaluering etter sikkerhetshendelser for å lære og forbedre? Gjennomfør en systematisk evaluering etter hver sikkerhetshendelse eller nesten-hendelse. Dokumenter hva som skjedde, hva som fungerte, hva som sviktet, og hvilke tiltak som skal iverksettes for å hindre gjentakelse.	1 — Ikke påbegynt	3 — Etablert	Viktig
5	Flerfaktor-autentisering og sikret kommunikasjon	10.3 Bruker dere sikrede kommunikasjonskanaler for sensitiv intern kommunikasjon? Velg og standardiser en kryptert kommunikasjonskanal for sensitiv intern kommunikasjon (f.eks. Teams, Slack med enterprise-kryptering, eller Signal). Kommuniser til alle ansatte hvilken kanal som skal brukes for sensitiv informasjon.	1 — Ikke påbegynt	3 — Etablert	Viktig
6	Flerfaktor-autentisering og sikret kommunikasjon	10.4 Har dere en plan for nødkommunikasjon hvis primære kommunikasjonskanaler er utilgjengelige? Utarbeid en plan for nødkommunikasjon som inkluderer alternative kontaktmetoder (telefonnumre, kryptert meldingsapp) for nøkkelpersonell. Distribuer listen og test at den fungerer minst årlig.	1 — Ikke påbegynt	3 — Etablert	Viktig
7	Hendelseshåndtering	2.1 Har virksomheten en dokumentert plan for håndtering av sikkerhetshendelser? Etabler en skriftlig hendelseshåndteringsplan med definerte roller, eskaleringsrutiner og varslingsprosedyrer. Planen bør dekke hvem som tar beslutninger, hvordan skaden begrenses, og hvordan kommunikasjonen håndteres internt og eksternt.	2 — Grunnleggende	3 — Etablert	Kritisk
8	Hendelseshåndtering	2.4 Kjenner dere til NIS2s varslingskrav og har dere en prosess for å varsle relevante myndigheter? Kartlegg NIS2s varslingskrav: tidlig varsel til relevant myndighet innen 24 timer, og detaljert rapport innen 72 timer. Utpek en ansvarlig person for myndighetsvarsling, og lag en prosedyre med kontaktinformasjon, terskelvurdering og maler for varsling.	2 — Grunnleggende	3 — Etablert	Kritisk
9	Driftskontinuitet og krisehåndtering	3.1 Har dere identifisert hvilke IT-systemer og tjenester som er kritiske for virksomhetens drift? Gjennomfør en konsekvensanalyse (BIA) for å identifisere kritiske systemer og tjenester, med definerte mål for akseptabel nedetid (RTO) og akseptabelt datatap (RPO). Prioriter gjenopprettingsarbeidet basert på virksomhetskritikalitet.	2 — Grunnleggende	3 — Etablert	Kritisk
10	Flerfaktor-autentisering og sikret kommunikasjon	10.1 Er flerfaktor-autentisering (MFA) aktivert for tilgang til kritiske systemer? Aktiver flerfaktor-autentisering (MFA) for alle kritiske systemer, med prioritet på e-post, VPN, admin-kontoer og skyportaler. Bruk app-basert MFA (f.eks. Microsoft Authenticator eller lignende) fremfor SMS der det er mulig.	2 — Grunnleggende	3 — Etablert	Kritisk
11	Hendelseshåndtering	2.3 Vet ansatte hvordan de skal rapportere en mistenkelig hendelse internt? Lag en enkel og tydelig rutine for intern rapportering av sikkerhetshendelser, med ett kontaktpunkt (e-post, telefon eller skjema). Kommuniser rutinen til alle ansatte og gjenta den i sikkerhetsopplæringen.	2 — Grunnleggende	3 — Etablert	Viktig

#	Kategori	Tiltak	Nåværende	Mål	Vekting
12	Driftskontinuitet og krisehåndtering	3.4 Finnes det en dokumentert plan for driftskontinuitet (BCP) eller gjenoppretting (DRP)? Utarbeid en driftskontinuitetsplan (BCP) som beskriver hvordan virksomheten opprettholder kritisk drift under en krise, og en gjenopprettingsplan (DRP) for IT-systemene. Start med de mest kritiske prosessene og bygg ut planen over tid.	2 — Grunnleggende	3 — Etablert	Viktig
13	Driftskontinuitet og krisehåndtering	3.5 Har dere avtaler med leverandører som sikrer støtte ved alvorlige hendelser? Gjennomgå avtaler med kritiske IT-leverandører for å sikre at de inkluderer responstider (SLA), ansvarsfordeling ved hendelser, og støtte under krisesituasjoner. Vurder om det er behov for beredskapsavtaler.	2 — Grunnleggende	3 — Etablert	Viktig
14	Flerfaktor-autentisering og sikret kommunikasjon	10.2 Er MFA aktivert for alle brukere, eller kun utvalgte? Utvid MFA til å gjelde alle brukere i virksomheten, ikke bare IT-personell og administratorer. Et kompromittert vanlig brukerkonto kan brukes som springbrett for videre angrep.	2 — Grunnleggende	3 — Etablert	Viktig
15	Vurdering av sikkerhetstiltakenes effektivitet	6.3 Gjennomfører dere interne eller eksterne revisjoner av informasjonssikkerheten? Gjennomfør en årlig intern gjennomgang av informasjonssikkerheten, eller vurder ekstern revisjon for kritiske områder. Dokumenter funn og sørg for at avvik følges opp med konkrete tiltak og frister.	2 — Grunnleggende	3 — Etablert	Viktig
16	Driftskontinuitet og krisehåndtering	3.6 Er krisehåndteringsplanen kommunisert til relevante ansatte? Sørg for at krisehåndteringsplanen er kommunisert til alle nøkkelpersoner utover IT, inkludert ledelse, HR og kommunikasjonsansvarlig. Gjennomfør en kort gjennomgang minst årlig slik at alle kjenner sin rolle.	1 — Ikke påbegynt	3 — Etablert	Støttende
17	Hendelseshåndtering	2.6 Har dere øvd på hendelseshåndtering gjennom tabletop-øvelser eller simuleringer? Planlegg og gjennomfør minst én årlig bordøvelse der nøkkelpersoner simulerer håndtering av et realistisk scenario, som for eksempel et ransomware-angrep. Dokumenter læringspunkter og oppdater hendelseshåndteringsplanen basert på funn.	2 — Grunnleggende	3 — Etablert	Støttende
18	Flerfaktor-autentisering og sikret kommunikasjon	10.5 Har dere vurdert og begrenset bruken av SMS som autentiseringsmetode? Vurder risikoen ved SMS-basert MFA for høy-risiko tilganger og migrer til app-basert eller hardware-basert autentisering der det er mulig. Behold SMS-basert MFA kun for systemer der bedre alternativer ikke er tilgjengelige.	2 — Grunnleggende	3 — Etablert	Støttende

Generert av Kravklar.no — 23. mars 2026

Utvikling over tid

Basert på 8 gjennomførte vurderinger.



Kategori	Forrige (23. mars 2026)	Nåværende (23. mars 2026)	Endring
Samlet score	**61%**	**59%**	**-2 pp**
Risikoanalyse og informasjonssikkerhetspolicy	67%	75%	+8 pp
Hendelseshåndtering	49%	33%	-16 pp
Driftskontinuitet og krisehåndtering	36%	30%	-6 pp
Forsyningskjedesikkerhet	64%	64%	±0 pp
Sikkerhet i anskaffelse, utvikling og vedlikehold av IKT	83%	85%	+2 pp
Vurdering av sikkerhetstiltakenes effektivitet	50%	56%	+6 pp
Grunnleggende cyberhygiene og opplæring	67%	65%	-2 pp
Kryptografi og kryptering	86%	86%	±0 pp
Personellsikkerhet, tilgangskontroll og verdihåndtering	68%	65%	-3 pp
Flerfaktor-autentisering og sikret kommunikasjon	46%	32%	-14 pp

Samlet modenhet har falt fra 61% til 59% (-2 pp) siden forrige vurdering (23. mars 2026). Størst forbedring er registrert innen Risikoanalyse og informasjonssikkerhetspolicy (+8 pp). OBS: Hendelseshåndtering har gått ned med 16 pp siden forrige vurdering.

ISO 27001 Annex A-kartlegging

Din NIS2-vurdering berører 62 av 93 ISO 27001 Annex A-kontroller.

Risikostyring og informasjonssikkerhetspolicyer — 75% — Dekket

Godt samsvar. Din sterke NIS2-score her reflekteres direkte i ISO 27001-dekning.

Kontroll-ID	Kontrollnavn
A.5.1	Policyer for informasjonssikkerhet
A.5.2	Roller og ansvar for informasjonssikkerhet
A.5.7	Trusselinformasjon
A.5.36	Etterlevelse av policyer, regler og standarder

God dekning. ISO 27001 sitt rammeverk for risikostyring (klausul 6.1, 8.2, 8.3) dekker NIS2 sine krav til risikoanalyse direkte. Sørg for at policyer eksplisitt refererer til «nettverks- og informasjonssystemsikkerhet» — ikke bare «informasjonssikkerhet» generelt.

Hendelseshåndtering — 33% — Delvis dekket

Du scorer lavt på Hendelseshåndtering, og dette er et område der NIS2 stiller strengere krav enn ISO 27001. Prioriter dette området for begge rammeverk.

Kontroll-ID	Kontrollnavn
A.5.24	Planlegging og forberedelse av hendelseshåndtering
A.5.25	Vurdering og beslutning om informasjonssikkerhetshendelser
A.5.26	Respons på informasjonssikkerhetshendelser
A.5.27	Læring av informasjonssikkerhetshendelser
A.5.28	Innsamling av bevis
A.5.29	Informasjonssikkerhet under avbrudd
A.6.8	Rapportering av informasjonssikkerhetshendelser
A.8.15	Logging
A.8.16	Overvåkingsaktiviteter

ISO 27001 dekker hele hendelseshåndteringssyklusen internt. NIS2 stiller imidlertid krav som går utover ISO 27001: varsling til CSIRT innen 24 timer, detaljert melding innen 72 timer, og sluttrapport innen én måned (Art. 23). ISO 27001 definerer heller ikke terskler for «vesentlige hendelser» som utløser rapporteringsplikten.

Driftskontinuitet og krisehåndtering — 30% — Delvis dekket

Du scorer lavt på Driftskontinuitet og krisehåndtering, og dette er et område der NIS2 stiller strengere krav enn ISO 27001. Prioriter dette området for begge rammeverk.

Kontroll-ID	Kontrollnavn
A.5.29	Informasjonssikkerhet under avbrudd
A.5.30	IKT-beredskap for forretningskontinuitet
A.8.13	Sikkerhetskopiering
A.8.14	Redundans i informasjonsbehandlingsfasiliteter

ISO 27001 dekker forretningskontinuitet og sikkerhetskopiering godt. NIS2 skiller imidlertid mellom «krisehåndtering» og «forretningskontinuitet» — det krever en egen styringsstruktur for kriser med definerte roller, beslutningsmyndighet og krisekommunikasjonsplaner, samt cyberøvelser. Dette går utover det A.5.29/A.5.30 normalt dekker.

Leverandørkjedesikkerhet — 64% — Delvis dekket

Du scorer middels på Leverandørkjedesikkerhet. NIS2 stiller strengere krav enn ISO 27001 her — vær oppmerksom på gapene.

Kontroll-ID	Kontrollnavn
A.5.19	Informasjonssikkerhet i leverandørforhold
A.5.20	Håndtering av informasjonssikkerhet i leverandøravtaler
A.5.21	Håndtering av informasjonssikkerhet i IKT-leverandørkjeden
A.5.22	Overvåking, gjennomgang og endringshåndtering av leverandørtjenester
A.5.23	Informasjonssikkerhet ved bruk av skytjenester

ISO 27001 gir et solid grunnlag for leverandørstyring. NIS2 Art. 21(2)(d) krever imidlertid vurdering av leverandørenes cybersikkerhetspraksis og produktkvalitet, samt leverandørspesifikk sårbarhetsvurdering. Art. 21(3) krever også at virksomheter tar hensyn til sårbarheter i leverandørkjeden som helhet.

Sikkerhet ved anskaffelse, utvikling og vedlikehold — 85% — Delvis dekket

Du scorer bra på Sikkerhet ved anskaffelse, utvikling og vedlikehold for NIS2, men vær oppmerksom på at ISO 27001 ikke dekker alle NIS2-kravene her.

Kontroll-ID	Kontrollnavn
A.8.4	Tilgang til kildekode
A.8.8	Håndtering av tekniske sårbarheter
A.8.9	Konfigurasjonsstyring
A.8.25	Sikker utviklingslivssyklus
A.8.26	Krav til applikasjonssikkerhet
A.8.27	Sikker systemarkitektur og utviklingsprinsipper
A.8.28	Sikker koding
A.8.29	Sikkerhetstesting i utvikling og akseptanse
A.8.30	Utkontraktert utvikling
A.8.31	Separasjon av utviklings-, test- og produksjonsmiljøer
A.8.32	Endringshåndtering
A.8.33	Testinformasjon

Sterk dekning av sikker utvikling, sårbarhetshåndtering og konfigurasjonsstyring. NIS2 forventer imidlertid deltakelse i koordinert sårbarhetsrapportering (Art. 12), inkludert publisert policy for sårbarhetsrapportering, kontaktpunkt for eksterne forskere, og koordinering med CSIRT. ISO 27001 A.8.8 dekker intern sårbarhetshåndtering, men ikke denne utadrettede koordineringen.

Vurdering av effektiviteten av sikkerhetstiltak — 56% — Dekket

Moderat score på Vurdering av effektiviteten av sikkerhetstiltak. ISO 27001 og NIS2 er godt samstemte, så videre forbedring gir uttelling i begge rammeverk.

Kontroll-ID	Kontrollnavn
A.5.35	Uavhengig gjennomgang av informasjonssikkerhet
A.5.36	Etterlevelse av policyer, regler og standarder

Sterkeste samsvar. ISO 27001 sitt PDCA-rammeverk, obligatoriske internrevisjonsprogram (klausul 9.2), ledelsens gjennomgang (klausul 9.3) og krav til kontinuerlig forbedring (klausul 10) dekker NIS2 sitt krav til effektivitetsvurdering direkte.

Grunnleggende cyberhygiene og opplæring — 65% — Delvis dekket

Du scorer middels på Grunnleggende cyberhygiene og opplæring. NIS2 stiller strengere krav enn ISO 27001 her — vær oppmerksom på gapene.

Kontroll-ID	Kontrollnavn
A.5.10	Akseptabel bruk av informasjon og andre tilknyttede eiendeler
A.5.17	Autentiseringsinformasjon
A.6.3	Bevissthet, utdanning og opplæring innen informasjonssikkerhet
A.8.5	Sikker autentisering
A.8.7	Beskyttelse mot skadelig programvare
A.8.19	Installasjon av programvare på driftssystemer

ISO 27001 dekker sikkerhetsbevissthet og opplæring generelt. NIS2 er mer spesifikk: Art. 20(2) krever at ledelsen gjennomfører cybersikkerhetsopplæring og tilbyr tilsvarende opplæring til ansatte regelmessig. «Grunnleggende cyberhygiene» må formelt defineres — ikke bare generelle bevissthetsprogrammer. Art. 20(2) innfører også personlig ansvar for ledelsen.

Kryptografi og kryptering — 86% — Dekket

Godt samsvar. Din sterke NIS2-score her reflekteres direkte i ISO 27001-dekning.

Kontroll-ID	Kontrollnavn
A.8.24	Bruk av kryptografi

God dekning. A.8.24 dekker kryptografipolicy, nøkkelhåndtering og passende bruk av kryptering. Sørg for at policyen eksplisitt dekker data i hvile og under overføring. Nasjonale tilpasninger (f.eks. digitalsikkerhetsloven) kan stille ytterligere krypteringskrav.

Personellsikkerhet, tilgangskontroll og aktivaforvaltning — 65% — Dekket

Moderat score på Personellsikkerhet, tilgangskontroll og aktivaforvaltning. ISO 27001 og NIS2 er godt samstemte, så videre forbedring gir uttelling i begge rammeverk.

Kontroll-ID	Kontrollnavn
A.5.3	Funksjonsfordeling
A.5.9	Oversikt over informasjon og andre tilknyttede eiendeler
A.5.10	Akseptabel bruk av informasjon og andre tilknyttede eiendeler
A.5.11	Tilbakelevering av eiendeler
A.5.12	Klassifisering av informasjon
A.5.13	Merking av informasjon
A.5.14	Informasjonsoverføring
A.5.15	Tilgangskontroll
A.5.16	Identitetshåndtering
A.5.17	Autentiseringsinformasjon
A.5.18	Tilgangsrettigheter
A.6.1	Bakgrunnssjekk
A.6.2	Vilkår og betingelser for ansettelse
A.6.3	Bevissthet, utdanning og opplæring innen informasjonssikkerhet
A.6.4	Disiplinærprosess
A.6.5	Ansvar etter opphør eller endring av ansettelsesforhold
A.6.6	Konfidensialitets- eller taushetserklæringer

Kontroll-ID	Kontrollnavn
A.8.1	Brukerendepunktsenheter
A.8.2	Privilegerte tilgangsrettigheter
A.8.3	Begrensning av informasjonstilgang
A.8.5	Sikker autentisering

Bredeste samsvar. ISO 27001 gir omfattende dekning av personellsikkerhet (bakgrunnssjekk → ansettelse → NDA → opplæring → disiplinærtiltak → avslutning), identitets- og tilgangsstyring, og aktivaforvaltning. NIS2 tilfører ikke vesentlige krav utover dette.

Flerfaktorautentisering og sikret kommunikasjon — 32% — Delvis dekket

Du scorer lavt på Flerfaktorautentisering og sikret kommunikasjon, og dette er et område der NIS2 stiller strengere krav enn ISO 27001. Prioriter dette området for begge rammeverk.

Kontroll-ID	Kontrollnavn
A.5.14	Informasjonsoverføring
A.8.5	Sikker autentisering
A.8.20	Nettverkssikkerhet
A.8.21	Sikkerhet for nettverkstjenester
A.8.22	Nettverkssegmentering
A.8.24	Bruk av kryptografi

ISO 27001 A.8.5 krever «sikker autentisering», men nevner ikke eksplisitt flerfaktorautentisering. NIS2 er mer spesifikk: eksplisitt krav om MFA eller kontinuerlig autentisering, sikret tale-/video-/tekstkommunikasjon, og sikrede nødkommunikasjonssystemer som fungerer uavhengig av primærkanalene. Det siste har ingen direkte Annex A-ekvivalent.

Viktig informasjon

Denne kartleggingen viser samsvar mellom NIS2 og ISO 27001 — ikke likeverdighet. ISO 27001-sertifisering betyr ikke automatisk NIS2-etterlevelse.

NIS2 stiller også krav utenfor Artikkel 21 som ISO 27001 ikke dekker: hendelsesrapportering til CSIRT (Art. 23), personlig ledelsesansvar (Art. 20), og registrering hos tilsynsmyndighet (Art. 3).

Generert av Kravklar.no — 23. mars 2026