

ISO/IEC 27001:2022 + Amd 1:2024 Ledelsessystemer for informationssikkerhed (ISMS)

Informationssikkerhed, ISMS, certificerbar i hele verden

181 krav. Det er muligt at blive certificeret efter denne standard hos et akkrediteret certificeringsorgan. Udgave 07/2026.

ISO/IEC 27001 fastlægger kravene til et informationssikkerhedsledelsessystem: risikobaseret, dokumenteret og med påvist virkning. En vurdering mod standarden er en akkrediteret certificeringsaudit i to trin (dokumentgennemgang og derefter gennemgang af virkningen på stedet), efterfulgt af årlige opfølgende audits og recertificering efter tre år.

| Virksomhed | Dato | Udfyldt af |
|------------|------|------------|
|------------|------|------------|

4 Organisationens kontekst8

4.1-1

**De eksterne og interne forhold, der påvirker organisationens evne til at opnå de tilsigtede resultater af ISMS, er fastlagt og holdes ajour.**

Det taler for: Kan dokumenteres med en kontekstanalyse enten som selvstændigt dokument eller som et afsnit i ISMS-håndbogen: markedsomgivelser, kunde- og kontraktforhold, retlige rammer (GDPR, NIS2), teknologistak, antal medarbejdere, afhængighed af cloudleverandører. For små virksomheder er en tabel på en side med dato og gennemgangscyklus nok, forudsat at ledelsens evaluering viser, at den faktisk opdateres.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

4.1-2

**Organisationen har fastlagt, om klimaforandringer er et relevant forhold for den. Konklusionen er begrundet, uanset om svaret er ja eller nej.**

Det taler for: Kravet kom med Amd 1:2024, og auditorer spørger målrettet efter det. Hold en egen række i kontekstanalysen: varmeperioder med betydning for serverrum og tilgængelighed, ekstremvejr med betydning for cloudleverandørernes datacentre, elnettets stabilitet. Et begrundet resultat om, at det ikke er relevant, er acceptabelt, en manglende post er det ikke.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

4.2-1

**De interessenter, der er relevante for ISMS, er fastlagt.**

Det taler for: Interessentliste med kunder, medarbejdere, databehandlere og underdatabehandlere, tilsynsmyndigheder, forsikringsselskaber, certificeringsorganet og ejerkredsen. I små virksomheder er en tabel med interessent, forventning og kilden til forventningen tilstrækkelig.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

4.2-2

**De relevante krav fra disse interessenter er fastlagt, herunder eventuelle krav med relation til klimaforandringer.**

Det taler for: Angiv for hver interessent den konkrete kilde: kontraktbestemmelse, databehandleraftale, kundespørgeskema, retlig forpligtelse. Amd 1:2024 tilføjer en note om, at interessenter kan have krav med relation til klimaforandringer. Det er ikke et selvstændigt skal-krav, men auditorer rejser det rutinemæssigt, for eksempel bæredygtighedsspørgsmål i en storkundes leverandøraudit. En række i interessenttabellen med resultatet, herunder ingen af den slags, er nok.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

4.2-3

**Det er besluttet og sporbart, hvilke af disse krav der håndteres gennem ISMS.**

Det taler for: Tilføj en kolonne til interessenttabellen, der peger på den regel, som håndterer kravet (politik, kontrol, kontraktbilag). Det viser, at kravene ikke bare er samlet ind, men faktisk behandlet.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

|                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                         |                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 4.3-1                                                                                                                                                                                                                                                                                                                                                                   | <b>Anvendelsesområdet for ISMS er fastlagt og tager hensyn til forholdene fra 4.1, kravene fra 4.2 samt grænseflader og afhængigheder til aktiviteter, der udføres af tredjeparter.</b> |                     |
| Det taler for: Anvendelsesområdet nævner lokationer, organisatoriske enheder, produkter, systemer og netværksgrænser. Outsourcede dele (hosting, betalingsudbydere, support) beskrives som grænseflader med en klar ansvarsgrænse. Et kunstigt indsnævret anvendelsesområde, der skærer kerneprocesser fra, bliver afvist af certificeringsorganerne.                   |                                                                                                                                                                                         |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                         |                     |
| 4.3-2                                                                                                                                                                                                                                                                                                                                                                   | <b>Anvendelsesområdet foreligger som dokumenteret information og angiver ISMS-grænserne utvetydigt.</b>                                                                                 | <div>Dokument</div> |
| Det taler for: Et godkendt dokument om anvendelsesområdet med version, dato og godkendelse fra øverste ledelse. Ordlyden optræder senere på certifikatet, så den skal formuleres præcist og på en måde, der kan citeres offentligt.                                                                                                                                     |                                                                                                                                                                                         |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                         |                     |
| 4.4-1                                                                                                                                                                                                                                                                                                                                                                   | <b>ISMS er etableret, implementeret, vedligeholdt og løbende forbedret, herunder de nødvendige processer og deres samspil.</b>                                                          |                     |
| Det taler for: Et proceskort eller en procesliste, der forbinder risikostyring, hændeshåndtering, ændringsstyring, audit og ledelsens evaluering med ejere og frekvens. Levende dokumentation vejer tungere end diagrammet: sager, referater, kalenderposter.                                                                                                           |                                                                                                                                                                                         |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                         |                     |
| <b>5 Lederskab</b>                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                         |                     |
| 8                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                         |                     |
| 5.1-1                                                                                                                                                                                                                                                                                                                                                                   | <b>Øverste ledelse tager ansvar for virkningen af ISMS og sikrer, at politikken og målene er etableret og forenelige med den strategiske retning.</b>                                   |                     |
| Det taler for: Dokumentationen omfatter underskrevne godkendelser af politikken, anvendelsesområdet og erklæringen om anvendelighed, referater fra ledelsens evaluering og dokumenterede budgetbeslutninger. I meget små virksomheder er øverste ledelse ofte den samme person som ISMS-ejeren, hvilket er acceptabelt, men det skal fremgå åbent af rollebeskrivelsen. |                                                                                                                                                                                         |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                         |                     |
| 5.1-2                                                                                                                                                                                                                                                                                                                                                                   | <b>Kravene til ISMS er integreret i forretningsprocesserne, og betydningen af virksom informationssikkerhed bliver kommunikeret.</b>                                                    |                     |
| Det taler for: Vises bedst der, hvor sikkerhed ikke er et separat ringbind: et sikkerhedskriterium i definition of done, et sikkerhedstjek i salgs- eller indkøbsprocessen, et fast sikkerhedspunkt i referater fra teammøder.                                                                                                                                          |                                                                                                                                                                                         |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                         |                     |
| 5.1-3                                                                                                                                                                                                                                                                                                                                                                   | <b>Ledelsen stiller de nødvendige ressourcer til rådighed, støtter de personer, der bidrager til virkningen af ISMS, og fremmer løbende forbedring.</b>                                 |                     |
| Det taler for: Godkendt sikkerhedsbudget, afsat tid til uddannelse, brug af eksterne auditorer eller penetrationstestere. Et forbedrings- eller handlingsregister med poster over flere kvartaler viser kontinuitet frem for en enkeltstående indsats.                                                                                                                  |                                                                                                                                                                                         |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                         |                     |
| 5.2-1                                                                                                                                                                                                                                                                                                                                                                   | <b>Der er etableret en politik for informationssikkerhed, som passer til organisationens formål og udgør rammen for målene for informationssikkerhed.</b>                               | <div>Dokument</div> |
| Det taler for: Et kort godkendt politikdokument, to til tre sider er nok. Det nævner beskyttelsesmålene, anvendelsesområdet, ansvaret og princippet om en risikobaseret tilgang. Generisk skabelontekst uden forbindelse til den faktiske virksomhed springer i øjnene i auditten.                                                                                      |                                                                                                                                                                                         |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                         |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                         |                     |

**5.2-2 Politikken indeholder en forpligtelse til at opfylde gældende krav og en forpligtelse til løbende forbedring af ISMS.**[Dokument](#)

Det taler for: Begge forpligtelser skal stå som udtrykkelige sætninger i politikken, og de læses ord for ord i auditten på trin 1. Henvi desuden til de underliggende processer (lovregister, forbedringsregister).

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**5.2-3 Politikken er kommunikeret i organisationen og er tilgængelig for interessenter i det omfang, det er relevant.**[Dokument](#)

Det taler for: Dokumentation via en post på intranet eller wiki med læsekrav, en onboardingtjekliste med bekræftelse eller et offentliggjort sammendrag på hjemmesiden. En distributionsliste med kvitteringer er det enkleste solide bevis.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**5.3-1 Ansvar og beføjelser for sikkerhedsrelevante roller er tildelt og kommunikeret i organisationen.**

Det taler for: En rollematrix (RACI) med ISMS-ejer, risikoejere, aktivejere, hændelseskoodinator og kontaktperson for databeskyttelse. I enkeltmandsvirksomheder og meget små teams tildeles hver rolle til en navngiven person, og den samling af roller, det medfører, dokumenteres åbent i stedet for at blive skjult.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**5.3-2 Beføjelsen til at sikre, at ISMS er i overensstemmelse med standarden, og til at rapportere om ISMS-præstationen til øverste ledelse er tildelt en rolle.**

Det taler for: Et udnævnelsesbrev eller en rollebeskrivelse for ISMS-ejeren med en udtrykkelig rapporteringsvej til ledelsen. Rapporteringsvejen skal reelt kunne dokumenteres med referater fra ledelsens evaluering.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**6 Planlægning**

21

**6.1.1-1 Med udgangspunkt i forholdene i 4.1 og kravene i 4.2 er de risici og muligheder, der skal håndteres, fastlagt, så ISMS opnår de tilsigtede resultater, og uønskede virkninger forebygges.**

Det taler for: Et register, der forbinder kontekstforhold med risici og muligheder, ført enten særskilt eller inde i risikoregistret. Det afgørende er sporbarheden: hvert forhold fra kontekstanalysen fører synligt til en vurdering eller til en begrundet beslutning om ikke at tage det med.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**6.1.1-2 Handlingerne til at håndtere disse risici og muligheder er planlagt, integreret i ISMS-processerne, og deres virkning bliver evalueret.**

Det taler for: Handlungsplan med ansvarlig, frist og virkningskriterium. Hold evalueringen af virkningen som en egen kolonne, ellers mangler auditten bevis for, at handlingen ikke bare blev gennemført, men også verificeret.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**6.1.2-1 En proces for risikovurdering af informationssikkerheden er fastlagt og anvendes; den omfatter kriterier for risikoaccept og kriterier for at gennemføre risikovurderinger.**[Dokument](#)

Det taler for: En politik for risikostyring med skalaer for sandsynlighed og konsekvens, en fastlagt risikomatrix og en klar acceptgrænse. Grænsen skal være et tal eller en zone, ikke en vending som efter eget skøn.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

|                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                               |                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 6.1.2-2                                                                                                                                                                                                                                                                           | <b>Processen sikrer, at gentagne risikovurderinger giver konsistente, gyldige og sammenlignelige resultater.</b>                                                                                              |                     |
| Det taler for: Dokumenteres med en fast metode med fastlagte skalaer og ved at sammenligne to versioner af vurderingen: samme risici, samme vurderingslogik, forklarlige forskelle. En dateret version af sidste års risikoregister er den stærkeste dokumentation her.           |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |
| 6.1.2-3                                                                                                                                                                                                                                                                           | <b>Risici for informationssikkerheden er identificeret med henblik på at opdage tab af fortrolighed, integritet og tilgængelighed inden for anvendelsesområdet, og hver risiko har en tildelt risikoejer.</b> |                     |
| Det taler for: Risikoregister med henvisning til aktiver eller processer, de tre beskyttelsesmål og en navngiven risikoejer. Risikoejeren skal have beføjelse til at acceptere risikoen; i små virksomheder er det normalt direktøren.                                            |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |
| 6.1.2-4                                                                                                                                                                                                                                                                           | <b>De identificerede risici er analyseret: mulige konsekvenser, realistisk sandsynlighed og det resulterende risikoniveau er fastlagt.</b>                                                                    |                     |
| Det taler for: Kolonner til konsekvens, sandsynlighed og resulterende risikoniveau, hver med en kort begrundelse. En enkelt sætning med begrundelse for hver risiko forebygger det hyppigste auditfund, nemlig tal uden udledning.                                                |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |
| 6.1.2-5                                                                                                                                                                                                                                                                           | <b>Risiciene er sammenholdt med acceptkriterierne og prioriteret til behandling.</b>                                                                                                                          |                     |
| Det taler for: Risikoregistret skal vise, hvilke risici der ligger over acceptgrænsen, og i hvilken rækkefølge de bliver behandlet. En sorteret visning eller en prioritetskolonne er nok.                                                                                        |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |
| 6.1.2-6                                                                                                                                                                                                                                                                           | <b>Processen for risikovurdering foreligger som dokumenteret information.</b>                                                                                                                                 | <div>Dokument</div> |
| Det taler for: Selve metoden er et obligatorisk dokument, ikke kun dens resultat. En godkendt politik med version og godkendelsesdato, linket fra ISMS-dokumentoversigten.                                                                                                        |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |
| 6.1.3-1                                                                                                                                                                                                                                                                           | <b>For hver risiko over acceptgrænsen er der valgt en passende behandlingsmulighed (reducere, undgå, overføre eller acceptere).</b>                                                                           |                     |
| Det taler for: En kolonne til behandlingsmulighed i risikoregistret. Hvor en risiko accepteres, noteres begrundelsen og risikoejerens formelle godkendelse; hvor den overføres, nævnes kontrakten eller forsikringspolisen.                                                       |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |
| 6.1.3-2                                                                                                                                                                                                                                                                           | <b>Alle kontroller, der er nødvendige for at gennemføre de valgte behandlingsmuligheder, er fastlagt.</b>                                                                                                     |                     |
| Det taler for: Formulér kontrollerne konkret og verificerbart, med en ansvarlig og en frist. Det er i orden at henvise til teknisk arbejde, der allerede er i gang (udrulning af MFA, test af sikkerhedskopiering), så længe der peges på en sag eller et konfigurationsartefakt. |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |
| 6.1.3-3                                                                                                                                                                                                                                                                           | <b>De fastlagte kontroller er sammenholdt med kontrollerne i bilag A for at verificere, at ingen nødvendig kontrol er blevet overset.</b>                                                                     |                     |
| Det taler for: Sammenligningen er et selvstændigt og sporbart trin, ikke et biprodukt. Dokumenteres med en kolonne i risikoregistret, der henviser til numrene i bilag A, samt daterede referater fra sammenligningen.                                                            |                                                                                                                                                                                                               |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                        |                                                                                                                                                                                                               |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                       |                                                                                                                                                                                                               |                     |

6.1.3-4

**Der findes en erklæring om anvendelighed (SoA). Den vurderer alle 93 kontroller i bilag A enkeltvis, angiver anvendelighed med begrundelse for hver kontrol, status for implementeringen og begrundelsen for hver udelukkelse.**

Dokument

Det taler for: SoA er det centrale obligatoriske dokument og kortet over hele auditten. Det skal være fuldstændigt: kontroller, der ikke er anvendelige, står også med en begrundelse, aldrig som en tom linje. Anbefalede kolonner: kontrolnummer, titel, anvendelig ja eller nej, begrundelse, status for implementeringen, henvisning til politik eller dokumentation, kobling til risikoen. Version og ledelsens godkendelse er obligatoriske, fordi SoA bliver holdt op mod virkeligheden ved hver opfølgende audit.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

6.1.3-5

**Der er udarbejdet en risikobehandlingsplan, som samler kontroller, ansvar, frister og nødvendige ressourcer.**

Dokument

Det taler for: Det kan være et faneblad i risikoregnearket eller en projekttavle. Det afgørende er, at datoerne er realistiske, og at overskredne datoer synligt er blevet planlagt om, for det er præcis det, auditoren kontrollerer.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

6.1.3-6

**Risikobehandlingsplanen er godkendt af risikoejerne, og de tilbageværende restrisici er formelt accepteret af dem.**

Dokument

Det taler for: Underskrift, elektronisk godkendelse eller en dateret beslutning i et referat. En linje i referatet fra ledelsens evaluering med henvisning til registrats version er tilstrækkelig, forudsat at versionen er entydig.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

6.1.3-7

**Processen for risikobehandling foreligger som dokumenteret information.**

Dokument

Det taler for: Dækkes normalt i samme politikdokument som risikovurderingen. Forløbet fra vurdering over valg af mulighed til accept af restrisiko skal være beskrevet.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

6.2-1

**Der er fastlagt mål for informationssikkerhed for relevante funktioner og niveauer, målene stemmer overens med politikken, og de er målbare, hvor det er praktisk muligt.**

Det taler for: En måloversigt med tre til seks mål, hvert med et måltal, en udgangsværdi, en målværdi og en frist. Eksempel: andelen af systemer med MFA hævet fra 80 til 100 procent inden kvartalets udgang. Mål uden et tal tæller som ikke målbare.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

6.2-2

**Målene tager hensyn til de gældende krav til informationssikkerhed samt resultaterne af risikovurdering og risikobehandling.**

Det taler for: Tilføj en oprindelseskolonne til måloversigten: hvilken risiko, hvilket kundekrav eller hvilken retlig forpligtelse målet stammer fra. Det forhindrer mål, der virker vilkårlige.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

6.2-3

**Målene bliver overvåget, kommunikeret og opdateret efter behov.**

Det taler for: Kvartalsvis opfølgning på fremdriften i måloversigten samt kommunikation til teamet, for eksempel en kort note i wikien eller et punkt på dagsordenen til teammødet. Historiske versioner viser, at opdateringerne finder sted.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

**6.2-4 Målene for informationssikkerhed foreligger som dokumenteret information.**[Dokument](#)

Det taler for: Et godkendt måldokument med dato er nok. Det må gerne være en del af ledelsens evaluering, men det skal findes der som sit eget genfindelige afsnit.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**6.2-5 For hvert mål er det planlagt, hvad der skal gøres, hvilke ressourcer der kræves, hvem der er ansvarlig, hvornår det er afsluttet, og hvordan resultaterne bliver evalueret.**

Det taler for: Disse fem punkter kan verificeres enkeltvis og bliver spurgt om enkeltvis i auditten. Sæt dem op som fem kolonner i måloversigten, så er overensstemmelsen synlig med et blik.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**6.3-1 Når organisationen fastlægger, at der er behov for ændringer i ISMS, bliver disse ændringer gennemført på en planlagt måde.**

Det taler for: Dokumenteres med ændringsanmodninger, referater eller sager, der viser anledningen, konsekvensvurderingen, godkendelsen og gennemførelsen. Typiske anledninger i små virksomheder: skift af cloudleverandør, nye lokationer, den første ansættelse.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**7 Støtte**

15

**7.1-1 De ressourcer, der er nødvendige for at etablere, implementere, vedligeholde og løbende forbedre ISMS, er fastlagt og stillet til rådighed.**

Det taler for: En budgetlinje til sikkerhed, værktøjslicenser (adgangskodehåndtering, MDM, logplatform), planlagte persondage til driften af ISMS og eksterne audityder. En faktura eller en budgetgodkendelse beviser det hurtigere end nogen tekst.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**7.2-1 Den nødvendige kompetence hos de personer, hvis arbejde påvirker informationssikkerhedens præstation, er fastlagt.**

Det taler for: Kompetencematrix eller rolleprofiler med den viden, hver rolle kræver, for eksempel sikker udvikling for udviklere og hændeshåndtering for koordinatoren. I meget små teams er en række for hver person nok.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**7.2-2 Kompetencen er sikret på grundlag af passende uddannelse, oplæring eller erfaring.**

Det taler for: Certifikater, kursusbeviser, cv eller dokumenteret praktisk erfaring. Selvstudium er acceptabelt, hvis det er dokumenteret, for eksempel med gennemførelsesbeviser fra onlinekurser eller beståede interne videnstest.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**7.2-3 Hvor der er kompetencehuller, er der iværksat handlinger for at lukke dem, og virkningen af disse handlinger er evalueret.**

Det taler for: Uddannelsesplan med en sammenligning af mål og faktisk gennemførelse samt et tjek af virkningen, for eksempel et testresultat, en klikrate i en phishingssimulering eller observation i arbejdet. Tjekket af virkningen bliver ofte glemt og er et klassisk mindre auditfund.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

|                                                                                                                                                                                                                                                                         |                                                                                                                                                                                      |                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 7.2-4                                                                                                                                                                                                                                                                   | <b>Der foreligger passende dokumenteret information som dokumentation for kompetencen.</b>                                                                                           | <a href="#">Dokument</a> |
| Det taler for: En kompetence- eller uddannelsesmappe for hver person med dokumentation og datoer. I små virksomheder er en mappe med gemte PDF-registreringer plus en oversigtstabel nok.                                                                               |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |
| 7.3-1                                                                                                                                                                                                                                                                   | <b>De personer, der arbejder inden for anvendelsesområdet, kender politikken for informationssikkerhed.</b>                                                                          |                          |
| Det taler for: Bekræftelse ved onboarding og efter hver ændring af politikken, med dato og version. En læsekvitteringsfunktion i wikien eller en underskrevet liste er tilstrækkelig.                                                                                   |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |
| 7.3-2                                                                                                                                                                                                                                                                   | <b>Medarbejderne kender deres eget bidrag til virkningen af ISMS og fordelene ved en bedre informationssikkerhedspræstation.</b>                                                     |                          |
| Det taler for: Undervisningsmateriale og deltagerlister, hvor forbindelsen til den enkeltes eget arbejde er synlig. Auditorer interviewer medarbejderne direkte, så undervis med konkrete eksempler fra hverdagen frem for abstrakte citater fra standarden.            |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |
| 7.3-3                                                                                                                                                                                                                                                                   | <b>Medarbejderne kender konsekvenserne af ikke at overholde kravene i ISMS.</b>                                                                                                      |                          |
| Det taler for: Angiv konsekvenserne i undervisningsslides og arbejdsinstruktioner, og knyt dem til processen under A.6.4. Selv virksomheder uden ansatte skal dække dette for underleverandører og freelancere gennem deres kontrakter.                                 |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |
| 7.4-1                                                                                                                                                                                                                                                                   | <b>Den interne og eksterne kommunikation, der er relevant for ISMS, er fastlagt: hvad der kommunikeres, hvornår, med hvem og ad hvilken vej.</b>                                     |                          |
| Det taler for: En kommunikationsmatrix med rækker som sikkerhedshændelse til kunder, underretning af tilsynsmyndigheden inden for 72 timer og månedlig statusrapport til ledelsen. Den er grundlaget for krisekommunikationen og bliver gennemgået efter hver hændelse. |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |
| 7.5.1-1                                                                                                                                                                                                                                                                 | <b>ISMS omfatter den dokumenterede information, som standarden kræver, samt den dokumenterede information, som organisationen har fastlagt som nødvendig for virkningen af ISMS.</b> | <a href="#">Dokument</a> |
| Det taler for: En dokumentoversigt, der lister hvert ISMS-dokument med formål, ejer, version og opbevaringssted. Den viser, at de obligatoriske dokumenter er komplette, og er auditorens hurtigste indgang.                                                            |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |
| 7.5.2-1                                                                                                                                                                                                                                                                 | <b>Ved oprettelse og opdatering af dokumenter er passende identifikation, format og medie sikret, og dokumenterne bliver gennemgået og godkendt med hensyn til egnethed.</b>         |                          |
| Det taler for: Et ensartet dokumenthoved med titel, version, dato, forfatter og godkender. I Git-baserede miljøer opfylder gennemgang og godkendelse af pull requests kravet om gennemgang og godkendelse, forudsat at historikken er uforanderlig.                     |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |
| 7.5.3-1                                                                                                                                                                                                                                                                 | <b>Den dokumenterede information er tilgængelig og egnet til brug, hvor og når der er behov for den.</b>                                                                             |                          |
| Det taler for: Et centralt opbevaringssted, som alle med adgangsret kan nå, med en søgefunktion. Kan testes med stikprøver: en vilkårlig arbejdsinstruktion skal kunne findes på under et minut.                                                                        |                                                                                                                                                                                      |                          |
| <div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div>                                                                                                                                                                                  |                                                                                                                                                                                      |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                             |                                                                                                                                                                                      |                          |

7.5.3-2

Den dokumenterede information er tilstrækkeligt beskyttet, især mod tab af fortrolighed, uretmæssig brug og tab af integritet.

Det taler for: Rollebaserede adgangsrettigheder til ISMS-dokumenter, versionering med historik, skrivebeskyttelse af godkendte versioner og sikkerhedskopiering af dokumentarkivet. Dokumentation for sikkerhedskopieringen er den del, der oftest bliver glemt.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

7.5.3-3

Distribution, adgang, fremfinding, opbevaring, ændringsstyring samt opbevaringstid og bortskaffelse af dokumenteret information er styret.

Det taler for: En kort regel for dokumentstyring med opbevaringsperioder og sletteregler. Den skal afstemmes med retlige forpligtelser (handelsret, skatteret, GDPR) og er grundlaget for A.5.33 og A.8.10.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

7.5.3-4

Den dokumenterede information af ekstern oprindelse, som er nødvendig for at planlægge og drive ISMS, er identificeret og styret.

Det taler for: En liste over eksterne dokumenter med version og kilde: standarder, lovtekster, leverandørers hærdningsvejledninger, dokumentation for cloudsikkerhed, databehandleraftaler. Uden en versionsangivelse kan styringen ikke dokumenteres.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

8 Drift

8

8.1-1

De processer, der er nødvendige for at opfylde kravene til informationssikkerhed og for at gennemføre handlingerne fra afsnit 6, er planlagt, implementeret og styret, og der er fastlagt kriterier for disse processer.

Det taler for: En driftshåndbog eller runbooks med klare kriterier, for eksempel den maksimale tid til at udrulle kritiske rettelser, frigivelseskriterier for deployments og alarmtærskler. Kriterier uden tal er værdiløse i auditten.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

8.1-2

Der foreligger dokumenteret information i det omfang, det er nødvendigt for at have tillid til, at processerne er gennemført som planlagt.

Dokument

Det taler for: Driftsregistreringer som dokumentation: sagshistorik, kørsler i CI-pipelinen, rapporter om rettelser, logfiler fra sikkerhedskopieringen, adgangsgennemgange. Disse registreringer er den egentlige dokumentation for virkningen i auditten på trin 2.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

8.1-3

Planlagte ændringer er styret, og konsekvenserne af utilsigtede ændringer bliver gennemgået; hvor det er nødvendigt, bliver negative virkninger afbødet.

Det taler for: En ændringsproces med godkendelse og en vej tilbage, koblet til A.8.32. For utilsigtede ændringer (fejlkonfiguration, utilsigtet rettighedsudvidelse) dokumenteres hændelsen, og korrektionen underbygges med dokumentation.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

8.1-4

Eksternt leverede processer, produkter og tjenester, der er relevante for ISMS, er fastlagt og styret.

Det taler for: En leverandørliste med kritikalitet, kontrakthenviisning og status for dokumentationen (leverandørens ISO 27001-certifikat, SOC 2-rapport, databehandleraftale). For små virksomheder er det den største løftestang, fordi størstedelen af it-driften alligevel ligger eksternt.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

|                                                                                                                                                                                                                                                                      |                                                                                                                                                                  |                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 8.2-1                                                                                                                                                                                                                                                                | <b>Risikovurderinger bliver gennemført med planlagte intervaller og altid ved væsentlige ændringer eller hændelser, under hensyn til de fastlagte kriterier.</b> |                     |
| Det taler for: En rytme, typisk årlig, samt fastlagte anledninger til vurderinger uden for planen. Dokumenteres med daterede versioner af risikoregistret og poster i kalenderen eller sagssystemet.                                                                 |                                                                                                                                                                  |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                           |                                                                                                                                                                  |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                          |                                                                                                                                                                  |                     |
| 8.2-2                                                                                                                                                                                                                                                                | <b>Resultaterne af risikovurderingerne opbevares som dokumenteret information.</b>                                                                               | <div>Dokument</div> |
| Det taler for: Historiske versioner af risikoregistret med datoer, ikke kun den aktuelle tilstand. Overskrives filen, kan udviklingen ikke bevises; versionering i filsystemet eller i Git løser det.                                                                |                                                                                                                                                                  |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                           |                                                                                                                                                                  |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                          |                                                                                                                                                                  |                     |
| 8.3-1                                                                                                                                                                                                                                                                | <b>Risikobehandlingsplanen er gennemført.</b>                                                                                                                    |                     |
| Det taler for: Sammenhold plan med virkelighed: afsluttede handlinger med gennemførelsesdato og et konkret artefakt (konfiguration, politik, kontrakt). Åbne handlinger kræver en dokumenteret begrundelse og en ny måldato.                                         |                                                                                                                                                                  |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                           |                                                                                                                                                                  |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                          |                                                                                                                                                                  |                     |
| 8.3-2                                                                                                                                                                                                                                                                | <b>Resultaterne af risikobehandlingen opbevares som dokumenteret information.</b>                                                                                | <div>Dokument</div> |
| Det taler for: Statusrapporter eller afsluttede handlinger med henvisning til dokumentationen. Registret alene er nok, hvis hver række bærer en afslutningsdato og et link til dokumentationen.                                                                      |                                                                                                                                                                  |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                           |                                                                                                                                                                  |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                          |                                                                                                                                                                  |                     |
| <div>9 Præstationsevaluering21</div>                                                                                                                                                                                                                                 |                                                                                                                                                                  |                     |
| 9.1-1                                                                                                                                                                                                                                                                | <b>Det er fastlagt, hvad der skal overvåges og måles, herunder processerne og kontrollerne for informationssikkerhed.</b>                                        |                     |
| Det taler for: Et måleark med et overskueligt antal solide målinger: efterslæb af rettelser, MFA-dækning, tid til at lukke hændelser, resultatet af den seneste genetableringstest og åbne fund. Få målinger, der faktisk bliver indsamlet, slår en lang ønskeliste. |                                                                                                                                                                  |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                           |                                                                                                                                                                  |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                          |                                                                                                                                                                  |                     |
| 9.1-2                                                                                                                                                                                                                                                                | <b>Metoderne til overvågning, måling, analyse og evaluering er fastlagt og giver gyldige resultater.</b>                                                         |                     |
| Det taler for: Dokumentér datakilden og beregningen for hver måling, for eksempel et udtræk fra sårbarhedsscanneren eller fra identitetsudbyderens rapport. Sporbarhed til kilden er kernen i gyldigheden.                                                           |                                                                                                                                                                  |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                           |                                                                                                                                                                  |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                          |                                                                                                                                                                  |                     |
| 9.1-3                                                                                                                                                                                                                                                                | <b>Det er fastlagt, hvornår og af hvem overvågning og måling bliver udført, og hvornår resultaterne bliver analyseret og evalueret.</b>                          |                     |
| Det taler for: Tilføj kolonner til frekvens og ansvarlig i målearket. En tilbagevendende kalenderaftale til evalueringen beviser regelmæssigheden bedre end nogen beskrivelse.                                                                                       |                                                                                                                                                                  |                     |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                           |                                                                                                                                                                  |                     |
| Dokumentation / begrundelse                                                                                                                                                                                                                                          |                                                                                                                                                                  |                     |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                             |          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 9.1-4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>Resultaterne af overvågning og måling opbevares som dokumenteret information.</b>                                                                                                                                                        | Dokument |
| Det taler for: Arkiverede evalueringer, eksporterede dashboards eller et måleark, der føres som en tidsserie. En livevisning uden historik opfylder ikke kravet.                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                             |          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                             |          |
| 9.1-5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>Informationssikkerhedens præstation og virkningen af ISMS bliver evalueret på grundlag af måleresultaterne.</b>                                                                                                                          |          |
| Det taler for: En skriftlig evaluering, ikke kun tal: tendens, årsager, behov for handling. Denne evalueringstekst er samtidig et input til ledelsens evaluering.                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                             |          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                             |          |
| 9.2.1-1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Der bliver gennemført interne audits med planlagte intervaller, og de giver information om, hvorvidt ISMS er i overensstemmelse med organisationens egne krav og med kravene i standarden, og om det er virksomt implementeret.</b>      |          |
| Det taler for: Inden certificeringsauditten skal mindst en fuld intern auditcyklus, der dækker hele anvendelsesområdet, være gennemført. Uden den er certificering uden for rækkevidde; det er en af de hyppigste snublesten ved en førstegangscertificering.                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                             |          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                             |          |
| 9.2.2-1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Et auditprogram er planlagt, etableret og vedligeholdt; det fastlægger frekvens, metoder, ansvar, planlægningskrav og rapportering, og det tager hensyn til de berørte processers betydning og til resultaterne af tidligere audits.</b> |          |
| Det taler for: Et flerårigt auditprogram, der dækker alle afsnit og alle anvendelige kontroller hen over certificeringscyklussen, med højere frekvens for kritiske områder. En simpel tabel over tre år er fuldt tilstrækkelig.                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                             |          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                             |          |
| 9.2.2-2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Auditkriterier og auditomfang er fastlagt for hver audit.</b>                                                                                                                                                                            |          |
| Det taler for: En auditplan for hver dato med kriterierne (standarden, interne politikker, kontrakter) og et klart omfang. En auditplan på en side for hver audit er nok og fungerer samtidig som grundlag for rapporten.                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                             |          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                             |          |
| 9.2.2-3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Auditorer er udvalgt, og audits bliver gennemført på en måde, der sikrer objektivitet og upartiskhed. Ingen auditerer sit eget arbejde.</b>                                                                                              |          |
| Det taler for: Uafhængigheden er den svære tærskel her: den, der har skrevet politikkerne og konfigureret systemerne, må ikke auditere dem. I meget små virksomheder betyder det næsten altid en ekstern intern auditor, for eksempel en indlejet konsulent eller en kollega fra en partnervirksomhed; en auditaftale plus auditorens erklæring om uafhængighed er dokumentationen. Kun i tilstrækkeligt store teams kan rollen roteres internt til en person uden ansvar for det område, der auditeres, og det skal så fremgå af rollematrixen. |                                                                                                                                                                                                                                             |          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                             |          |
| 9.2.2-4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Auditresultaterne bliver rapporteret til den relevante ledelse.</b>                                                                                                                                                                      |          |
| Det taler for: En auditrapport med fund, afvigelser, anbefalinger og en fordelingsliste samt dokumentation for overdragelsen til ledelsen, for eksempel et punkt i et referat eller en dateret overdragelse pr. e-mail.                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                             |          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                             |          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                             |          |

|                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                         |                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 9.2.2-5                                                                                                                                                                                                                                                                                                                                                                                   | <b>Dokumenteret information om auditprogrammet og auditresultaterne opbevares.</b>                                                                                                                                                                      | <a href="#">Dokument</a> |
| Det taler for: Hold auditprogram, auditplaner, auditrapporter og de handlinger, de fører til, samlet ét sted. Forbindelsen fra et fund til en korrigerende handling (afsnit 10.2) skal være synlig hele vejen.                                                                                                                                                                            |                                                                                                                                                                                                                                                         |                          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                         |                          |
| 9.3.1-1                                                                                                                                                                                                                                                                                                                                                                                   | <b>Øverste ledelse evaluerer ISMS med planlagte intervaller for at sikre, at det fortsat er egnet, tilstrækkeligt og virksomt.</b>                                                                                                                      |                          |
| Det taler for: Mindst en gang om året og planlagt før den eksterne audit. Selv i meget små virksomheder skal der foreligge daterede og underskrevne referater, også hvor ledelsen og ISMS-ejeren er den samme person.                                                                                                                                                                     |                                                                                                                                                                                                                                                         |                          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                         |                          |
| 9.3.2-1                                                                                                                                                                                                                                                                                                                                                                                   | <b>Ledelsens evaluering behandler status for handlinger fra tidligere evalueringer.</b>                                                                                                                                                                 |                          |
| Det taler for: Referatet starter med en opfølgningstabel over sidste års beslutninger og deres aktuelle status. Uden denne tilbagereference tæller evalueringen som ufuldstændig.                                                                                                                                                                                                         |                                                                                                                                                                                                                                                         |                          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                         |                          |
| 9.3.2-2                                                                                                                                                                                                                                                                                                                                                                                   | <b>Ledelsens evaluering behandler ændringer i de eksterne og interne forhold, der er relevante for ISMS, herunder relevante aspekter af klimaforandringer.</b>                                                                                          |                          |
| Det taler for: Et selvstændigt dagsordenspunkt med henvisning til den opdaterede kontekstanalyse. Klimaforandringer nævnes ikke udtrykkeligt i teksten til dette afsnit (Amd 1:2024 ændrer kun 4.1 og 4.2), men de kommer ind her gennem ændringer i forholdene under 4.1, og auditorer forventer det. Selv et resultat om, at det er uændret og ikke relevant, hører hjemme i referatet. |                                                                                                                                                                                                                                                         |                          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                         |                          |
| 9.3.2-3                                                                                                                                                                                                                                                                                                                                                                                   | <b>Ledelsens evaluering behandler ændringer i interessenternes behov og forventninger, som er relevante for ISMS.</b>                                                                                                                                   |                          |
| Det taler for: Nye kundekrav fra kontrakter og sikkerhedsspørgeskemaer, nye retlige forpligtelser og krav fra certificeringsorganet. Notér dem som en liste med kilder i referatet.                                                                                                                                                                                                       |                                                                                                                                                                                                                                                         |                          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                         |                          |
| 9.3.2-4                                                                                                                                                                                                                                                                                                                                                                                   | <b>Ledelsens evaluering behandler tilbagemeldinger om informationssikkerhedens præstation, herunder afvigelser og korrigerende handlinger, resultater af overvågning og måling, auditresultater og opfyldelsen af målene for informationssikkerhed.</b> |                          |
| Det taler for: Behandl disse fire blokke som separate dagsordenspunkter, ellers mangler en af dem senere i referatet. Vedhæft målearket, auditrapporten og måloversigten som bilag.                                                                                                                                                                                                       |                                                                                                                                                                                                                                                         |                          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                         |                          |
| 9.3.2-5                                                                                                                                                                                                                                                                                                                                                                                   | <b>Ledelsens evaluering behandler tilbagemeldinger fra interessenter.</b>                                                                                                                                                                               |                          |
| Det taler for: Reklamationer fra kunder med en sikkerhedsvinkel, resultater af kundeaudits, indberetninger fra whistleblowerkanalen og tilbagemeldinger fra tjenesteleverandører. Notér det i referatet, også hvor konklusionen er, at der ikke kom nogen.                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| <div>ÅbentI gangOpfyldtIkke relevant</div>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                         |                          |
| Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                         |                          |

9.3.2-6    **Ledelsens evaluering behandler resultaterne af risikovurderingen og status for risikobehandlingsplanen.**

Det taler for: Vedhæft det aktuelle risikoregister og status for gennemførelsen af behandlingsplanen med udtrykkelig bekræftelse af risikoejernes accept af restrisikoen.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

9.3.2-7    **Ledelsens evaluering behandler muligheder for løbende forbedring.**

Det taler for: Et dagsordenspunkt med konkrete forbedringsideer og en beslutning om hver af dem. Accepterede ideer flytter over i forbedringsregistret som poster med frister.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

9.3.3-1    **Resultaterne af ledelsens evaluering omfatter beslutninger om muligheder for løbende forbedring og om eventuelle behov for ændringer i ISMS.**

Det taler for: Referatet slutter med et beslutningsafsnit: beslutning, ansvarlig, frist. Referater uden beslutninger er et fund i auditten, fordi ledelseeffekten så mangler.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

9.3.3-2    **Der opbevares dokumenteret information som dokumentation for resultaterne af ledelsens evaluering.**

Dokument

Det taler for: Underskrevne referater med dato, deltagere, input, evaluering og beslutninger. Det er et af de første dokumenter, et certificeringsorgan beder om på trin 1.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

10 Forbedring

7

10.1-1    **ISMS bliver løbende forbedret med hensyn til egnethed, tilstrækkelighed og virkning.**

Det taler for: Et forbedringsregister, der fødes fra flere kilder (audits, hændelser, ideer, afvigelser i målinger), med synlig fremdrift over tid. Kontinuiteten over flere måneder er beviset, ikke antallet af poster.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

10.2-1    **Når der opstår en afvigelse, reagerer organisationen på den: den styrer og korrigerer afvigelsen og håndterer konsekvenserne.**

Det taler for: En afvigelsesrapport med en straksforanstaltning og en dato. Kilderne er interne audits, eksterne audits, hændelser og observationer fra den daglige drift; de føder alle det samme register.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

10.2-2    **Det er vurderet, om der er behov for handlinger, der fjerner årsagerne, så afvigelsen ikke gentager sig eller opstår andre steder; det omfatter en kontrol af, om lignende afvigelser findes eller kan opstå.**

Det taler for: Dokumentér grundårsagsanalysen, for eksempel med 5 hvorfor eller Ishikawa, samt en udtrykkelig udtalelse om overførbarheden til andre systemer eller processer. Trinnet om overførbarehed er det, der oftest bliver sprunget over.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

10.2-3    **Nødvendige korrigerende handlinger er gennemført, og deres virkning er gennemgået.**

Det taler for: Notér for hver handling gennemførelsesdatoen, dokumentationsartefaktet og en senere gennemgang af virkningen med sin egen dato. To datofelter i hver række er den enkleste måde ikke at miste gennemgangen af virkningen.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

10.2-4    **Hvor det er nødvendigt, er der foretaget ændringer i ISMS som følge af afvigelsen.**

Det taler for: Fører en afvigelse tilbage til et hul i en politik, i risikoregistret eller i SoA, skal ændringen blive synlig der. En henvisning fra afvigelsen til den opdaterede dokumentversion lukker kæden.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

10.2-5    **De korrigerende handlinger står i forhold til virkningerne af de afvigelser, der er konstateret.**

Det taler for: En alvorlighedsvurdering i registret, som proportionaliteten i handlingen fremgår af. Hverken bagateller håndteret som et projekt eller alvorlige afvigelser besvaret med blot en påmindelse pr. e-mail.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

10.2-6    **Der opbevares dokumenteret information om afvigelsernes art, de handlinger, der er truffet som svar, og resultaterne af de korrigerende handlinger.**

Dokument

Det taler for: Et register over afvigelser og korrigerende handlinger med kolonner til art, årsag, handling, ansvarlig, frist og resultatet af gennemgangen af virkningen. Det er obligatorisk dokumentation og bliver trukket frem ved hver opfølgende audit.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

A.5 Bilag A: Organisatoriske kontroller

37

A.5.1    **Politikker for informationssikkerhed: En overordnet politik for informationssikkerhed og emnespecifikke politikker er fastlagt, godkendt af ledelsen, kommunikeret og gennemgået med planlagte intervaller og ved væsentlige ændringer.**

Dokument

Det taler for: Et sæt politikker med version, godkendelsesdato og næste gennemgangsdato samt dokumentation for bekræftelsen. For små virksomheder er en rammepolitik og en håndfuld emnepolitikker (adgang, kryptografi, fjernarbejde, hændelser) nok.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

A.5.2    **Roller og ansvar for informationssikkerhed: Roller og ansvar for informationssikkerhed er fastlagt og tildelt efter organisationens behov.**

Det taler for: En rollematrix med navne, stedfortrædere og opgaver. I meget små virksomheder anføres åbent, hvor flere roller samler sig hos en person, og det kobles til de kompenserende kontroller under A.5.3.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

A.5.3    **Funktionsadskillelse: Opgaver og ansvarsområder, der er tænkt til at kontrollere hinanden, ligger ikke hos en enkelt person. Målet er, at ingen på egen hånd kan igangsætte, godkende og skjule en ændring.**

Det taler for: I en lille virksomhed er fuld funktionsadskillelse strukturelt umulig; en bred påstand om, at kravet er opfyldt, falder med det samme i auditinterviewet. Det, der holder, er en ærlig analyse: hvilke kombinationer af opgaver der er kritiske (udvikle og frigive, tildele rettigheder og bruge dem, igangsætte og godkende betalinger), hvilke af dem der ligger hos en person, og hvilke kompenserende kontroller der gælder. Gennemprøvede greb er uforanderlige auditlogfiler, som en tredjepart har adgang til, MFA på privilegerede konti, automatiske tjek i CI og beskyttede grene i stedet for fireøjeprincippet, en periodisk loggennemgang foretaget af en ekstern person og separat godkendelse af betalinger. Hold analysen og de kompenserende kontroller som et selvstændigt dateret dokument, og link til det fra SoA.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

A.5.4

**Ledelsens ansvar: Ledelsen kræver, at alle medarbejdere anvender informationssikkerhed i overensstemmelse med de fastlagte politikker og procedurer.**

Det taler for: En forpligtelse i ansættelses- og konsulentaftaler, bekræftelse af politikkerne ved onboarding og regelmæssige påmindelser fra ledelsen. Dokumentation: underskrevne forpligtelseserklæringer og mødereferater.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

A.5.5

**Kontakt med myndigheder: Der holdes passende kontakt til relevante myndigheder, og kontaktpunkterne kan nås, når der er behov for det.**

Det taler for: En kontaktliste med den kompetente datatilsynsmyndighed, politiet eller enheden for cyberkriminalitet, det nationale rapporteringspunkt for cybersikkerhed og, hvor det er omfattet, rapporteringskanalerne under NIS2. Notér fristerne, for eksempel de 72 timer i GDPR, direkte i listen.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

A.5.6

**Kontakt med særlige interessegrupper: Der holdes kontakt med særlige interessegrupper, sikkerhedsfora og faglige sammenslutninger.**

Det taler for: Medlemskaber, abonnerede varslinger (nationalt CERT, leverandørfeeds) og deltagelse i interessegrupper. Et enkelt bevis: en liste over abonnementer plus et eksempel på, hvordan en varslings førte til en handling.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

A.5.7

**Trusselsefterretninger: Information om trusler mod informationssikkerheden bliver indsamlet og analyseret, så der kan udledes passende handlinger af den.**

Det taler for: Nyt i udgaven fra 2022. Praktisk for små virksomheder: abonnér på varslinger fra det nationale CERT og fra leverandørerne, og hold derefter en kort månedlig gennemgang med en relevansbeslutning og sager udledt af den. Dokumentationen er analysen, ikke abonnementet.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

A.5.8

**Informationssikkerhed i projektledelse: Informationssikkerhed er integreret i projektledelsen uanset projekttype.**

Det taler for: Sikkerhedspunkter i projekttjeklisten: beskyttelsesbehov, risikogennemgang, tjek af databeskyttelsen og sikkerhedsgodkendelse før idriftsættelse. I agile teams forankres de som faste punkter i definition of ready og definition of done.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

A.5.9

**Fortegnelse over information og andre tilknyttede aktiver: Der er oprettet og bliver vedligeholdt en fortegnelse over information og andre tilknyttede aktiver med navngivne ejere.**

Det taler for: En aktivfortegnelse med hardware, software, cloudtjenester, datalagre, domæner og konti, hver med en ejer og sit beskyttelsesbehov. I små virksomheder kan den samles automatisk fra et MDM-udtræk, en licensliste og cloudkonsollen; en aktuel dato er obligatorisk.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

A.5.10

**Acceptabel brug af information og andre tilknyttede aktiver: Regler for acceptabel brug og håndtering af information og andre tilknyttede aktiver er identificeret, dokumenteret og implementeret.**

Dokument

Det taler for: En politik for acceptabel brug af enheder, netværk, cloudkonti og AI-værktøjer, med bekræftelse. Private enheder og eksterne AI-tjenester bør være udtrykkeligt dækket, for det er der, de fleste lækager sker.

Åbent

I gang

Opfyldt

Ikke relevant

Dokumentation / begrundelse

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5.11 | <b>Tilbagelevering af aktiver: Når et samarbejde ophører eller ændrer sig, er det styret og bekræftet skriftligt, at alle udleverede enheder, nøgler, konti og dokumenter bliver leveret tilbage.</b><br><br>Det taler for: En offboardingtjekliste med kvittering for tilbagelevering af bærbar computer, tokens, nøgler, certifikater og lagringsmedier samt deaktivering af konti samme dag. Det gælder freelancere og praktikanter i lige så høj grad.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                              |
| A.5.12 | <b>Klassifikation af information: Information bliver klassificeret efter sit beskyttelsesbehov med hensyn til fortrolighed, integritet, tilgængelighed og retlige krav.</b><br><br>Det taler for: En enkel model med tre eller fire niveauer (offentlig, intern, fortrolig, strengt fortrolig) og konkrete håndteringsregler for hvert niveau. Notér tildelingen i aktivfortegnelsen eller i fortegnelsen over behandlingsaktiviteter.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                                  |
| A.5.13 | <b>Mærkning af information: Klassifikationsniveauet er synligt på selve dokumentet, filen eller meddelelsen, så modtagerne ved, hvordan de skal håndtere den, uden først at spørge.</b><br><br>Det taler for: Mærkning i dokumenthovedet, i filnavnet, i emnefeltet i e-mailen eller med følsomhedsmærker i cloudkontorpakken. Dokumenteres med stikprøver af dokumenter, der faktisk er mærket, ikke kun med reglen.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                                                   |
| A.5.14 | <b>Overførsel af information: Der foreligger regler, procedurer og aftaler for overførsel af information inden for organisationen og med eksterne parter.</b><br><br>Det taler for: En regel for, hvilken kanal der er tilladt til hvilket klassifikationsniveau: krypteret e-mail eller et datarum til fortroligt indhold, ingen forsendelse via private beskedtjenester. Understøt fortrolige overførsler med hemmeligholdelsesaftaler.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                               |
| A.5.15 | <b>Adgangsstyring: Regler for at styre fysisk og logisk adgang til information og andre tilknyttede aktiver er etableret og implementeret på grundlag af forretningsmæssige og sikkerhedsmæssige krav.</b><br><br>Det taler for: En politik for adgangsstyring efter princippet om adgang efter behov og mindst mulige rettigheder, med en kobling fra rolle til rettigheder. Dokumenteres med den faktiske rettighedskonfiguration hos identitetsudbyderen, ikke med politikken alene.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse |
| A.5.16 | <b>Identitetsstyring: Hele livscyklussen for identiteter bliver styret.</b><br><br>Det taler for: En proces fra oprettelse over ændring til deaktivering, ideelt centraliseret hos en identitetsudbyder med single sign-on. Ingen delte gruppekonti; hvor det teknisk er uundgåeligt, navngives kontoen, begrundes den, og brugen bliver logget.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                                                                                                                        |
| A.5.17 | <b>Autentifikationsinformation: Tildeling og styring af autentifikationsinformation er styret af en proces, der kræver, at personerne håndterer den korrekt.</b><br><br>Det taler for: Et obligatorisk værktøj til håndtering af adgangskoder, en politik for adgangskodekvalitet og MFA, sikker førstegangsadgang og en nulstillingsprocedure med identitetskontrol. Dokumenteres med skærbilleder af konfigurationen og rapporten fra adgangskodeværktøjet.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                           |

**A.5.18 Adgangsrettigheder: Adgangsrettigheder bliver tildelt, gennemgået, ændret og fjernet i overensstemmelse med politikken for adgangsstyring.**

Det taler for: En periodisk adgangsgennemgang mindst en gang om året med et dokumenteret resultat for hver konto og dokumentation for de rettigheder, der er fjernet. Fjernelse på fratrædelsesdagen er et punkt, auditorer gerne sporer gennem en konkret sag.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.5.19 Informationssikkerhed i leverandørforhold: Processer og procedurer til at styre de sikkerhedsrisici, der opstår ved brug af tredjeparters produkter og tjenester, er fastlagt og implementeret.**

Det taler for: En leverandørliste med kritikalitetsniveau og dybden af vurderingen. For kritiske leverandører indhentes dokumentation (ISO 27001-certifikat, SOC 2-rapport) frem for at gennemføre egne audits, hvilket er den eneste realistiske vej for små virksomheder.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.5.20 Håndtering af informationssikkerhed i leverandøraftaler: Relevante sikkerhedskrav er aftalt med hver leverandør og skrevet ind i kontrakterne.**

Det taler for: Et kontraktbilag om informationssikkerhed med underretningspligt ved hændelser, regler om underdatabehandlere, sletteforpligtelser og auditrettigheder. For standardtjenester er leverandørens vilkår plus en databehandlertale tilstrækkeligt, forudsat at indholdet er gennemgået og dokumenteret.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.5.21 Styring af informationssikkerhed i IKT-forsyningskæden: Processer til at styre sikkerhedsrisiciene i forsyningskæden for informations- og kommunikationsteknologi er fastlagt og implementeret.**

Det taler for: Det dækker softwareafhængigheder og leverandørernes egne underleverandører. I praksis: en stykliste over software (SBOM) eller en afhængighedsliste, automatiske tjek for sårbare pakker i CI og indkøb af software udelukkende fra signerede eller officielle kanaler.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.5.22 Overvågning, gennemgang og ændringsstyring af leverandørydelser: Ændringer i leverandørydelser bliver regelmæssigt overvåget, gennemgået og styret.**

Det taler for: En årlig leverandørgennemgang med blik for hændelser, tilgængelighedsrapporter og certifikaternes gyldighed samt en kanal til leverandørens meddelelser om ændringer. Notér resultatet som en kort note for hver leverandør.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.5.23 Informationssikkerhed ved brug af cloudtjenester: Processer for at anskaffe, bruge, styre og forlade cloudtjenester er etableret i overensstemmelse med sikkerhedskravene.**

Det taler for: Nyt i udgaven fra 2022 og den centrale kontrol for små cloudbaserede virksomheder. Dokumenteres med en cloudpolitik med en godkendelsesproces for nye tjenester, en dokumenteret model for delt ansvar for hver tjeneste, hærdningsindstillinger og en exitstrategi med tilbagelevering af data og bekræftelse af sletningen.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.5.24 Planlægning og forberedelse af håndtering af informationssikkerhedshændelser: Processer, roller og ansvar for hændelseshåndtering er planlagt og etableret.**

Dokument

Det taler for: En beredskabsplan for hændelser med rapporteringsvej, roller, eskaleringsniveauer, kontakter uden for arbejdstid og skabeloner til kommunikation. Realistisk for små teams: en side, men øvet.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5.25 | <b>Vurdering af og beslutning om informationssikkerhedsbegivenheder: Sikkerhedsbegivenheder bliver vurderet, og der bliver truffet beslutning om, hvorvidt de skal klassificeres som informationssikkerhedshændelser.</b><br><br>Det taler for: Triagekriterier med en alvorlighedsmatrix og et begivenhedsregister, hvor også afviste begivenheder står med en begrundelse. Adskillelsen mellem begivenhed og hændelse skal være synlig i registret.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                                                            |
| A.5.26 | <b>Håndtering af informationssikkerhedshændelser: Hændelser bliver håndteret i overensstemmelse med de dokumenterede procedurer.</b><br><br>Det taler for: Hændelsessager med tidslinje, de udførte handlinger, de involverede personer og beslutningen om at lukke sagen. Har der endnu ikke været en reel hændelse, er en dokumenteret skrivebordsøvelse den bedste tilgængelige dokumentation.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                                                                                                                |
| A.5.27 | <b>Læring af informationssikkerhedshændelser: Viden fra hændelser bliver brugt til at styrke sikkerhedskontrollerne.</b><br><br>Det taler for: En gennemgang efter hændelsen uden skyldsplacering med grundårsagsanalyse og udledte handlinger, koblet til forbedringsregistret og, hvor der er behov, til risikoregistret.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                                                                                                                                                                                      |
| A.5.28 | <b>Indsamling af beviser: Det er styret, hvordan spor, der vedrører en sikkerhedsbegivenhed, bliver identificeret, sikret og opbevaret, så de fortsat kan bruges senere.</b><br><br>Det taler for: En kort procedure for bevissikring: genopbyg ikke systemer for tidligt, sikr images og logfiler, dokumentér sporbarhedskæden. For små virksomheder er det nok at fastlægge, fra hvilket alvorlighedsniveau en ekstern leverandør af it-efterforskning bliver tilkaldt, sammen med kontaktoplysningerne.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                       |
| A.5.29 | <b>Informationssikkerhed under driftsforstyrrelser: Organisationen planlægger, hvordan informationssikkerheden bliver opretholdt på et passende niveau under en driftsforstyrrelse.</b><br><br>Det taler for: Nødløsninger må ikke slå sikkerheden fra. Dokumentér, at MFA, logning og adgangsbegrænsninger også gælder i nøddrift, og at nødkonti (break-glass-konti) er forseglede, dokumenterede og bliver gennemgået bagefter.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                                                                               |
| A.5.30 | <b>IKT-beredskab til forretningskontinuitet: IKT-beredskabet er planlagt, implementeret, vedligeholdt og testet på grundlag af mål for forretningskontinuitet og krav til IKT-kontinuitet.</b><br><br>Det taler for: Nyt i udgaven fra 2022. Dokumenteres med fastlagte mål for genetableringstid (RTO) og for acceptabelt datatab (RPO) for hvert kritisk system, en genetableringsprocedure og mindst en dokumenteret test om året. En vellykket genetableringstest med dato og varighed er det stærkeste enkeltstående bevis.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse |
| A.5.31 | <b>Juridiske, lovgivningsmæssige, regulatoriske og kontraktlige krav: De relevante krav og fremgangsmåden til at opfylde dem er identificeret, dokumenteret og holdt ajour.</b> <div>Dokument</div><br><br>Det taler for: Et lovregister med GDPR, telelovgivning, handels- og skatteret og, hvor det er relevant, NIS2 eller branchespecifikke regler, hver med den regel, der gennemfører kravet, og datoen for gennemgangen. En årlig gennemgang er tilstrækkelig, men den skal være dateret.<br><br><div><div>Åbent</div><div>I gang</div><div>Opfyldt</div><div>Ikke relevant</div></div><br>Dokumentation / begrundelse                                 |

A.5.32    **Immaterielle rettigheder: Der er implementeret passende procedurer til at beskytte immaterielle rettigheder.**

Det taler for: En licensfortegnelse over den software, der er i brug, et tjek af open source-licenser i produktet (en licensscanner i CI) og en regel for håndtering af tredjepartskode og genereret kode. Dokumentation: licensrapporten fra buildet.

Åbent    I gang    Opfyldt    Ikke relevant

Dokumentation / begrundelse

A.5.33    **Beskyttelse af registreringer: Forretnings- og bevisregistreringer bliver opbevaret, så de ikke kan gå tabt, ikke kan ændres ubemærket og ikke kan falde i de forkerte hænder, og det gælder i hele opbevaringsperioden.**

Det taler for: En opbevaringsplan med de lovbestemte perioder, manipulationssikker opbevaring, begrænset adgang og sikkerhedskopiering. For skatter relevante registreringer nævnes de lovbestemte opbevaringsperioder udtrykkeligt, for det tjekker auditorer gerne målrettet.

Åbent    I gang    Opfyldt    Ikke relevant

Dokumentation / begrundelse

A.5.34    **Privatlivsbeskyttelse og beskyttelse af PII: Kravene til privatlivsbeskyttelse og til beskyttelse af personoplysninger (PII) er identificeret og opfyldt i overensstemmelse med gældende ret.**

Det taler for: Fortegnelse over behandlingsaktiviteter, databehandlaftaler, et slettekoncept, en proces for de registreredes rettigheder og, hvor det er påkrævet, en konsekvensanalyse vedrørende databeskyttelse. En kobling til ISMS gennem en fælles aktivliste undgår, at alt skal vedligeholdes to gange.

Åbent    I gang    Opfyldt    Ikke relevant

Dokumentation / begrundelse

A.5.35    **Uafhængig gennemgang af informationssikkerhed: Organisationens tilgang til at styre informationssikkerheden bliver gennemgået uafhængigt med planlagte intervaller og ved væsentlige ændringer.**

Det taler for: Dokumenteres med den interne audit udført af en uafhængig auditor, med eksterne penetrationstest eller med selve certificeringsauditten. Uafhængig betyder, at gennemgangen ikke udføres af den person, der er ansvarlig for det område, der bliver gennemgået.

Åbent    I gang    Opfyldt    Ikke relevant

Dokumentation / begrundelse

A.5.36    **Overholdelse af politikker, regler og standarder for informationssikkerhed: Overholdelsen af organisationens egne sikkerhedspolitikker og af de gældende regler bliver gennemgået regelmæssigt.**

Det taler for: Overholdelsestjek med dato og resultat, for eksempel et konfigurationstjek mod virksomhedens egen hærtningsbaseline, stikprøver af dokumentmærkningen og automatiske politikstjek i cloudmiljøet. Afvigelser går videre til registret over korregerende handlinger.

Åbent    I gang    Opfyldt    Ikke relevant

Dokumentation / begrundelse

A.5.37    **Dokumenterede driftsprocedurer: Driftsprocedurer for informationsbehandlingsfaciliteter er dokumenteret og gjort tilgængelige for de personer, der har brug for dem.**

Dokument

Det taler for: Runbooks til sikkerhedskopiering og genetablering, deployment, brugeradministration, rettelser og hændelseshåndtering. En kort og aktuel runbook slår en omfattende og forældet; en dato for seneste ændring i hver runbook er obligatorisk.

Åbent    I gang    Opfyldt    Ikke relevant

Dokumentation / begrundelse

## A.6 Bilag A: Personrelaterede kontroller

8

**A.6.1 Screening: Kandidater, der skal arbejde for organisationen, bliver screenet på forhånd inden for lovens rammer og i et omfang, der står mål med beskyttelsesbehovet; for følsomme roller bliver screeningen gentaget under ansættelsen.**

Det taler for: Uden ansatte kan denne kontrol begrundes som ikke anvendelig i øjeblikket, men fremgangsmåden for det tilfælde, at der ansættes nogen, bør alligevel være fastlagt og noteret i erklæringen om anvendelighed som planlagt. Et brugbart omfang: kontrol af identitet, cv og referencer samt eksamens- og kursusbeviser; en straffeattest kun hvor beskyttelsesbehovet berettiger det, og loven tillader det. Stil det samme krav til freelancere og underleverandører gennem deres kontrakter, ellers åbner hullet sig præcis der.

|       |        |         |               |
|-------|--------|---------|---------------|
| Åbent | I gang | Opfyldt | Ikke relevant |
|-------|--------|---------|---------------|

Dokumentation / begrundelse

**A.6.2 Ansættelsesvilkår: De kontraktlige aftaler angiver medarbejdernes og organisationens ansvar for informationssikkerheden.**

Det taler for: En sikkerhedsklausul i ansættelses- eller serviceaftalen med henvisning til de gældende politikker. For freelancere den samme klausul i konsulentaftalen plus en hemmeligholdelsesaftale.

|       |        |         |               |
|-------|--------|---------|---------------|
| Åbent | I gang | Opfyldt | Ikke relevant |
|-------|--------|---------|---------------|

Dokumentation / begrundelse

**A.6.3 Bevidsthed, uddannelse og træning i informationssikkerhed: Medarbejdere og relevante eksterne parter får passende bevidstgørelse og træning samt regelmæssige opdateringer om organisationens politikker.**

Det taler for: Årlig træning med deltagerdokumentation og dato, suppleret med phishingsimuleringer med en evalueret klikrate. Selv soloselvstændige har brug for dokumentation for deres egen efteruddannelse, for eksempel kursusbeviser.

|       |        |         |               |
|-------|--------|---------|---------------|
| Åbent | I gang | Opfyldt | Ikke relevant |
|-------|--------|---------|---------------|

Dokumentation / begrundelse

**A.6.4 Disciplinær proces: Der findes en formel og kommunikeret proces for at skride ind over for personer, der har overtrådt sikkerhedspolitikkerne.**

Det taler for: Uden ansatte kan dette begrundes som ikke anvendeligt i øjeblikket, men processen skal alligevel være fastlagt for det tilfælde, at der ansættes nogen; kun anvendelsen bortfalder, ikke reglen. Det, der kræves, er en trinvis og kommunikeret skala af reaktioner (samtale, påtale, formel advarsel, opsigelse) i overensstemmelse med ansættelsesretten og reglerne om medarbejderrepræsentation. For underleverandører afspejles sanktionsniveauet i kontrakten, for eksempel en konventionalbod eller en ret til at opsiges aftalen.

|       |        |         |               |
|-------|--------|---------|---------------|
| Åbent | I gang | Opfyldt | Ikke relevant |
|-------|--------|---------|---------------|

Dokumentation / begrundelse

**A.6.5 Ansvar efter ansættelsens ophør eller ændring: Sikkerhedsansvar og pligter, der fortsat gælder efter ophør eller et rolleskifte, er fastlagt, håndhævet og kommunikeret til de berørte personer.**

Det taler for: En offboardingtjekliste med fjernelse af rettigheder, tilbagelevering af aktiver, overdragelse og en udtrykkelig påmindelse om de fortsatte fortrolighedsforpligtelser. En underskrevet registrering fra fratrædelsessamtalen er den enkleste dokumentation.

|       |        |         |               |
|-------|--------|---------|---------------|
| Åbent | I gang | Opfyldt | Ikke relevant |
|-------|--------|---------|---------------|

Dokumentation / begrundelse

**A.6.6 Fortroligheds- eller hemmeligholdelsesaftaler: Det er fastlagt, hvem der skal underskrive en fortrolighedsaftale. Indholdet svarer til informationens beskyttelsesbehov, aftalerne er underskrevet, arkiveret og bliver gennemgået regelmæssigt, så de forbliver aktuelle.**

Det taler for: Underskrevne fortrolighedsaftaler for ansatte, freelancere, tjenesteleverandører og praktikanter med en efterfølgende gyldighedsperiode. En oversigtstabel med modpart, dato og gyldighed gør porteføljen mulig at auditere.

|       |        |         |               |
|-------|--------|---------|---------------|
| Åbent | I gang | Opfyldt | Ikke relevant |
|-------|--------|---------|---------------|

Dokumentation / begrundelse

#### A.6.7 Fjernarbejde: Der er implementeret sikkerhedsforanstaltninger, hvor personer arbejder uden for organisationens lokaler og undervejs tilgår organisationens information.

Det taler for: En politik for hjemmearbejde og fjernarbejde med krav til diskryptering, skærmlås, sikkert trådløst net, brug af VPN eller zero trust-adgang, privatlivsfiltre til skærmen og forbud mod at bruge private enheder uden godkendelse. Dokumenteres med MDM-rapporten om overholdelse for endepunkterne.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

#### A.6.8 Rapportering af informationssikkerhedsbegivenheder: Der findes en mekanisme, hvor personer rettidigt kan rapportere observerede eller formodede sikkerhedsbegivenheder.

Det taler for: En tydeligt kommunikeret rapporteringskanal (postkasse, chatkanal, telefonnummer) med en forsikring om ingen sanktioner ved rapporter i god tro. Dokumentation: antallet af rapporter i begivenhedsregistret; et permanent tomt register er et advarselstegn i auditten.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

### A.7 Bilag A: Fysiske kontroller

14

#### A.7.1 Fysiske sikkerhedspærimeretre: Sikkerhedspærimeretre er fastlagt og bliver brugt til at beskytte områder, der rummer information og informationsbehandlingsfaciliteter.

Det taler for: En beskrivelse af pærimeretrene med en skitse eller fotos: bygning, kontor, serverskab. På et hjemmekontor er pærimereten det aflåselige arbejdsværelse eller, hvis det ikke findes, et aflåseligt skab; beskriv det frem for at udelade det.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

#### A.7.2 Fysisk adgang: Sikre områder er beskyttet med passende adgangskontroller og adgangspunkter.

Det taler for: Et nøgle- eller adgangskortregister med udlevering og tilbagelevering samt en besøgsregel med ledsagelse og en log. Bruges et kontorfællesskab eller et datacenter, tages operatørens adgangskontroller som dokumentation, og de sikres kontraktligt.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

#### A.7.3 Sikring af kontorer, lokaler og faciliteter: Den fysiske sikkerhed for kontorer, lokaler og faciliteter er udformet og implementeret.

Det taler for: Aflåselige døre, vinduessikring i stueetagen, ingen fortrolige skærme synlige udefra, intet firmaskilt på følsomme områder. En kort beskrivelse plus et foto er nok som dokumentation.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

#### A.7.4 Fysisk sikkerhedsovervågning: Lokalerne bliver løbende overvåget for uautoriseret fysisk adgang.

Det taler for: Nyt i udgaven fra 2022. Mulighederne er et alarmanlæg, bevægelsessensorer, videoovervågning eller adgangslogfiler. Videoovervågning skal tjekkes for overholdelse af databeskyttelsen; på et hjemmekontor er det begrundede alternativ en kombination af et alarmanlæg, et aflåst rum og konstateringen af, at der ikke står følsomme servere dér.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

#### A.7.5 Beskyttelse mod fysiske og miljømæssige trusler: Der er beskyttelse mod fysiske og miljømæssige trusler som naturkatastrofer og forsætlig eller uforsætlig skade.

Det taler for: En gennemgang af brand, vand, varme, strømsvigt og indbrud sammen med de foranstaltninger, der er på plads (røgalarmer, ildslukkere, intet udstyr under vandrør, sikkerhedskopi opbevaret på en anden lokation). Det er her, fastlæggelsen om klimaforandringer fra 4.1 hænger sammen med resten.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.6 Arbejde i sikre områder: Foranstaltninger for arbejde i sikre områder er udformet og implementeret.**

Det taler for: Regler for serverrummet eller områder med høj fortrolighed: ingen uovervåget adgang for tredjeparter, ingen optagelse med kameraer eller mobile enheder, logning af det udførte arbejde. Findes der ingen sikre områder, kan det begrundes med henvisning til ren clouddrift.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.7 Ryddeligt skrivebord og ryddelig skærm: Regler for et ryddeligt skrivebord med hensyn til papirer og flytbare medier og for låste skærme er fastlagt og bliver fulgt.**

Det taler for: Det gælder fuldt ud også på hjemmekontoret og må derfor ikke erklæres ikke anvendeligt. Dokumenteres med en kort regel (lås dokumenter inde, skærmlås efter fem minutter, ingen sedler med adgangsplysninger) plus den teknisk håndhævede lås via enhedspolitikken, hvis konfiguration kan eksporteres.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.8 Placering og beskyttelse af udstyr: Udstyr er placeret sikkert og beskyttet.**

Det taler for: Placering væk fra gennemgangszoner og offentlige områder, intet indblik udefra, beskyttelse mod varme og fugt, kabellåse til mobile enheder. En kort beskrivelse i politikken for hjemmekontor eller kontor er nok.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.9 Sikkerhed for aktiver uden for virksomhedens lokaler: Aktiver, der befinder sig uden for lokalerne, er beskyttet.**

Det taler for: I små virksomheder er det først og fremmest den bærbare computer, smartphonen og eksterne medier, og det kan ikke bortforklares. Dokumentation: håndhævet diskryptering, fjernsletning aktiveret gennem MDM, en regel mod at efterlade enheder i køretøjer og mod at bruge offentlige netværk uden VPN samt en vej til at melde tab. MDM-rapporten om overholdelse med krypteringsstatus for hver enhed er det mest solide enkeltstående bevis.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.10 Lagringsmedier: Lagringsmedier bliver styret gennem hele deres livscyklus i overensstemmelse med klassifikationsmodellen og håndteringskravene, fra anskaffelse over brug og transport til bortskaffelse.**

Det taler for: Det gælder selv ved rent mobilt arbejde, for USB-nøgler, eksterne diske og medier til sikkerhedskopiering findes. Dokumentation: et medieregister, krypterede medier, et teknisk håndhævet forbud mod ikke godkendte flytbare medier, sikker opbevaring på et aflåseligt sted og overdragelse til A.7.14 ved udløbet levetid.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.11 Understøttende forsyninger: Informationsbehandlingsfaciliteter er beskyttet mod svigt i de understøttende forsyninger, især strømforsyningen.**

Det taler for: Drives der servere internt, en nødstrømsforsyning med en dokumenteret test. I et rent cloudopsæt er dokumentationen henvisningen til leverandørens tilsagn plus en regel for, hvordan arbejdet fortsætter under et lokalt strøm- eller internetsvigt (mobil deling af netværk, alternativ lokation).

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.12 Kablesikkerhed: Kabler til strøm, data og kommunikation er beskyttet mod aflytning, forstyrrelse og skade.**

Det taler for: Ejers kablingen selv, beskyttelse mod skade og mod uautoriseret adgang til patchpaneler. På små kontorer og hjemmekontorer er begrundelsen kortfattet, men den skal gives: router og netværksstik er ikke offentligt tilgængelige, og ubrugte porte er slået fra.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.13 Vedligeholdelse af udstyr: Udstyr bliver vedligeholdt korrekt for at sikre informationens tilgængelighed, integritet og fortrolighed.**

Det taler for: En vedligeholdelsesplan eller status for leverandørsupport for hver enhed og en regel for reparationer udført af tredjeparter (tag lagringsenheden ud først eller slet dataene, og indgå en fortrolighedsaftale med leverandøren). Følg datoerne for supportophør i aktivfortegnelsen.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.7.14 Sikker bortskaffelse eller genbrug af udstyr: Inden en enhed med lagring bliver givet videre, solgt eller skrottet, er det kontrolleret og registreret, at ingen beskyttede data og ingen licenseret software kan genskabes på den.**

Det taler for: Det gælder også på hjemmekontoret og for udrangerede private enheder, der har været brugt i arbejdet. Dokumentation: en sletteregistrering for hver enhed med serienummer, dato og metode (kryptosletning på krypterede SSD-diske, overskrivning, fysisk destruktionscertifikat fra en leverandør. For krypterede enheder er den dokumenterede destruktions af nøglen nok, forudsat at fremgangsmåden er beskrevet.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8 Bilag A: Teknologiske kontroller****34****A.8.1 Brugerenheder: Information, der er lagret på, behandles af eller er tilgængelig via brugerenheder, er beskyttet.**

Det taler for: En hærtningsbaseline for hvert operativsystem, central administration via MDM, diskkryptering, automatiske opdateringer og skærmlås. MDM-rapporten om overholdelse med en status for hver enhed dokumenterer det hele på en gang.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.2 Privilegerede adgangsrettigheder: Tildeling og brug af privilegerede adgangsrettigheder er begrænset og styret.**

Det taler for: En liste over alle administratorkonti med en begrundelse, separate administratorkonti, der ikke bruges til dagligt arbejde, håndhævet MFA, tidsbegrænset rettighedsforhøjelse hvor det er muligt, og periodisk gennemgang. I små virksomheder er det den vigtigste kompenserende kontrol for A.5.3.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.3 Begrænsning af adgang til information: Adgangen til information og andre tilknyttede aktiver er begrænset i overensstemmelse med den fastlagte politik for adgangsstyring.**

Det taler for: Et rettighedskoncept bygget på roller og grupper frem for enkelttildelinger, dokumenteret med et udtræk af gruppe-medlemskaber. Gennemgå offentlige delelinks i cloudlageret regelmæssigt, og lad dem udløbe.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.4 Adgang til kildekode: Læse- og skriveadgang til kildekode, udviklingsværktøjer og softwarebiblioteker er styret på passende vis.**

Det taler for: Rettigheder i repositoret efter rolle, beskyttede hovedgrene, håndhævede gennemgange eller håndhævede statustjek og ingen direkte push til hovedgrenen. Dokumenteres med konfigurationen af grenbeskyttelsen og organisationens medlemsliste.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.5 Sikker autentifikation: Sikre teknologier og procedurer til autentifikation er implementeret på grundlag af adgangsbegrænsningerne og den emnespecifikke politik.**

Det taler for: MFA på al ekstern adgang og alle administratorkonti, phishingresistente metoder (passkeys, FIDO2) hvor det er muligt, og spærring efter mislykkede forsøg. Dokumenteres med identitetsudbyderens rapport om MFA-dækning.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.6 Kapacitetsstyring: Lagring, regnekraft, båndbredde og licenser bliver overvåget, og behovet bliver justeret så tidligt, at flaskehalse aldrig truer tilgængeligheden.**

Det taler for: Overvågning af lagerplads, beregningsbelastning, licenskvoter og cloudbudgetter med alarmer ved tærskler. I små virksomheder er en alarm på diskforbrug og på omkostningsgrænser plus et årligt kapacitets eftersyn nok.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.7 Beskyttelse mod skadelig software: De tekniske forsvar mod skadelig software er aktive og opdaterede, og de personer, der bruger enhederne, er tilstrækkeligt trænet til ikke at undergrave forsvaret.**

Det taler for: Aktiv endepunktsbeskyttelse med en central statusoversigt, et mailfilter, der kontrollerer vedhæftede filer og links, og en regel mod at køre software, der ikke er godkendt. Den daterede statusrapport fra beskyttelsesløsningen er den direkte dokumentation.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.8 Styring af tekniske sårbarheder: Organisationen holder sig aktivt orienteret om sårbarheder i den teknologi, den bruger, afgør for hvert fund, hvor udsat den er, og lukker hullet inden for fastlagte frister eller begrundet en anden reaktion.**

Det taler for: Sårbarhedsstyring med en kilde (scanner, afhængighedstjek i CI, leverandørvarslinger), en alvorlighedsvurdering og fastlagte frister for hvert niveau, for eksempel kritisk inden for 7 dage. Dokumentation: scanningsrapporter fra flere tidspunkter, der viser faldet i åbne fund.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.9 Konfigurationsstyring: Konfigurationer af hardware, software, tjenester og netværk, herunder sikkerhedskonfigurationer, er etableret, dokumenteret, implementeret, overvåget og gennemgået.**

Det taler for: Nyt i udgaven fra 2022. Dokumenteres med fastlagte baselinekonfigurationer (hærdningsbaselines) og håndhævelsen af dem, ideelt som infrastruktur som kode i versionsstyring eller gennem MDM-profiler. Registrering af afdrift og en periodisk sammenligning af konfigurationerne runder det af.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.10 Sletning af information: Information, der er lagret i informationssystemer, på enheder og på lagringsmedier, bliver slettet, når der ikke længere er brug for den.**

Det taler for: Nyt i udgaven fra 2022 og tæt knyttet til GDPR. Dokumenteres med et slettekoncept med opbevaringsperioder for hver datakategori, teknisk implementerede opbevaringsregler i cloudtjenester og databaser samt slette logfiler. Sikkerhedskopier og logarkiver har også brug for en opbevaringsperiode.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.11 Datamaskering: Datamaskering bliver anvendt i overensstemmelse med den emnespecifikke politik for adgangsstyring og med de forretningsmæssige og retlige krav.**

Det taler for: Nyt i udgaven fra 2022. I praksis: ingen produktionsdata i test- og udviklingsmiljøer, men anonymiserede eller syntetiske data i stedet; pseudonymisering i analyser; maskering af kontonumre og adgangsuplysninger i logfiler og supportgrænseflader. Dokumenteres med det script eller den procedure, der genererer testdataene.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.8.12 | <b>Forebyggelse af data-lækage: Foranstaltninger til at forebygge data-lækage bliver anvendt på systemer, netværk og enheder, der behandler, lagrer eller overfører følsom information.</b><br><br>Det taler for: Nyt i udgaven fra 2022. Realistisk i små virksomheder: styring af delelinks i cloudlageret, blokering af ikke godkendte flytbare medier, regler mod videresendelse til private postkasser, kontrol med indtastning af fortrolige data i eksterne AI-tjenester og scanning for hemmeligheder i kildekoden. Dokumenteres med konfigurationen og med gennemgange af fundene.                                                                                |
|        | <div>Åbent</div> <div>I gang</div> <div>Opfyldt</div> <div>Ikke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.8.13 | <b>Sikkerhedskopiering af information: Der findes sikkerhedskopier af data, software og systemer efter en fastlagt regel (omfang, frekvens, opbevaringstid, placering), og genetablering fra dem bliver faktisk testet med regelmæssige mellemrum.</b><br><br>Det taler for: En politik for sikkerhedskopiering med frekvens, opbevaringstid og en kopi på en anden lokation efter 3-2-1-princippet, kryptering af sikkerhedskopierne og beskyttelse mod overskrivning ved ransomware (uforanderlige sikkerhedskopier). Det afgørende er den dokumenterede genetableringstest med dato og resultat, for en utestet sikkerhedskopi tæller som ikke eksisterende i auditten. |
|        | <div>Åbent</div> <div>I gang</div> <div>Opfyldt</div> <div>Ikke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.8.14 | <b>Redundans i informationsbehandlingsfaciliteter: Informationsbehandlingsfaciliteter er indrettet med nok redundans til at opfylde kravene til tilgængelighed.</b><br><br>Det taler for: Redundansen skal svare til målene for tilgængelighed, ikke til det maksimalt mulige. Dokumenteres med en arkitekturbeskrivelse med redundante instanser eller zoner, reserveenheder og en begrundet beslutning om, hvor redundansen bevidst mangler.                                                                                                                                                                                                                             |
|        | <div>Åbent</div> <div>I gang</div> <div>Opfyldt</div> <div>Ikke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.8.15 | <b>Logning: Sikkerhedsrelevante aktiviteter efterlader spor. Logfiler bliver dannet, opbevaret, beskyttet mod ændring og faktisk analyseret, ikke kun samlet ind.</b><br><br>Det taler for: Log som minimum pålogninger og mislykkede forsøg, ændringer af rettigheder, administrative handlinger og adgang til fortrolige data. Logfilerne er beskyttet mod ændring og har en fastlagt opbevaringstid; i små virksomheder er uforanderlige logfiler samtidig kompensationen for den manglende funktionsadskillelse under A.5.3.                                                                                                                                           |
|        | <div>Åbent</div> <div>I gang</div> <div>Opfyldt</div> <div>Ikke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.8.16 | <b>Overvågningsaktiviteter: Netværk, systemer og applikationer bliver overvåget for unormal adfærd, og der bliver truffet passende handlinger for at vurdere mulige sikkerhedshændelser.</b><br><br>Det taler for: Nyt i udgaven fra 2022. Brugbart uden et eget sikkerhedsteam: alarmer fra identitetsudbyderen om umulige rejser og om serier af mislykkede forsøg, alarmer fra cloudplatformen om usædvanligt forbrug eller ændringer af rettigheder, videresendt til en overvåget postkasse med en fastlagt reaktionstid. Dokumenteres med alarmreglerne plus eksempler på alarmer, der er blevet håndteret.                                                           |
|        | <div>Åbent</div> <div>I gang</div> <div>Opfyldt</div> <div>Ikke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.8.17 | <b>Tidssynkronisering: Alle systemer, der skriver logfiler, henter deres tid fra en fastlagt og betroet kilde, så begivenheder kan sættes i den rigtige rækkefølge på tværs af systemer.</b><br><br>Det taler for: NTP-konfiguration på servere og endepunkter og en ensartet tidszone i logfilerne (ideelt UTC). Uden synkroniseret tid holder rekonstruktionen af en hændelse under A.5.28 ikke; et konfigurationsudtræk er nok som dokumentation.                                                                                                                                                                                                                       |
|        | <div>Åbent</div> <div>I gang</div> <div>Opfyldt</div> <div>Ikke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.8.18 | <b>Brug af privilegerede hjælpeprogrammer: Brugen af hjælpeprogrammer, der kan tilsidesætte systembeskyttelser, er begrænset og stramt styret.</b><br><br>Det taler for: En liste over godkendte administrationsværktøjer, begrænsning af lokale administratorrettigheder, applikationsstyring (allowlisting) hvor det er muligt, og logning af brugen. Dokumentation: politikken plus konfigurationen af rettighedsstyringen.                                                                                                                                                                                                                                             |
|        | <div>Åbent</div> <div>I gang</div> <div>Opfyldt</div> <div>Ikke relevant</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | Dokumentation / begrundelse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**A.8.19 Installation af software på produktionssystemer: Procedurer og foranstaltninger til sikker styring af softwareinstallation på produktionssystemer er implementeret.**

Det taler for: Kun godkendt software fra betroede kilder, installation gennem central distribution eller et værktøj til pakkehåndtering, en vej tilbage og opbevaring af den forrige version. Dokumenteres med godkendelseslisten og deploymentlogfilerne.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.20 Netværkssikkerhed: Netværk og aktive netværksenheder har en navngiven ejer, en hærdet konfiguration og et sporbart regelsæt, der fastlægger, hvilken trafik der overhovedet er tilladt.**

Det taler for: Et firewallregelsæt efter princippet afvis som standard, dokumenterede åbne porte med en begrundelse, en sikker konfiguration af det trådløse net og ændrede fabriksadgangskoder på netværksenhederne. Dokumenteres med et udtræk af regelsættet og en ekstern portscanning.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.21 Sikkerhed for netværkstjenester: Sikkerhedsmekanismer, serviceniveauer og styringskrav for netværkstjenester er identificeret, implementeret og overvåget.**

Det taler for: Dokumentér for hver netværkstjeneste i brug (VPN, DNS, mail, CDN) sikkerhedstilsagnene og virksomhedens egen konfiguration, herunder kryptering under transport og leverandørens tilsagn om serviceniveau. Dokumentation: en konfigurationsoversigt plus kontrakten eller ydelsesbeskrivelsen.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.22 Netværksadskillelse: Netværket er delt op i zoner, så tjenester, brugergrupper og systemer med forskellige beskyttelsesbehov ikke kan nå hinanden ufiltreret.**

Det taler for: Separate netværkssegmenter eller VLAN til gæster, administration og produktion; i cloudmiljøet separate konti eller virtuelle netværk med sikkerhedsgrupper. På et hjemmekontor er den brugbare løsning et separat netværk eller VLAN til arbejdsenhederne, holdt adskilt fra private enheder og smarthjemteknologi.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.23 Webfiltrering: Adgangen til eksterne websteder bliver styret for at mindske eksponeringen for skadeligt indhold.**

Det taler for: Nyt i udgaven fra 2022. Kan opnås med lille indsats gennem en filtrerende DNS-tjeneste eller den webfiltrering, der følger med endepunktsbeskyttelsen, med blokerede kategorier og logning af blokerede forespørgsler. Dokumenteres med filterkonfigurationen og et rapportudtræk.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.24 Brug af kryptografi: Det er bindende fastlagt, hvor kryptering bliver anvendt, med hvilke algoritmer, og hvordan nøgler bliver dannet, opbevaret, udskiftet og destrueret gennem hele deres livscyklus.**

Dokument

Det taler for: En kryptografipolitik med godkendte algoritmer og mindste nøglelængder, kryptering under transport (TLS) og i hvile samt en procedure for nøglestyring, der dækker dannelse, opbevaring, udskiftning og destruktion. Dokumenteres med politikken plus konfigurationen af nøgletjenesten eller nøglehvelvet.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.25 Sikker udviklingslivscyklus: Regler for sikker udvikling af software og systemer er etableret og bliver anvendt.**

Det taler for: En beskrivelse af udviklingsprocessen med sikkerhedsberøringspunkter i hver fase: krav, design, implementering, test, frigivelse, drift. For små teams er en enkelt side med henvisning til de konkrete tjek i CI og gennemgangspligten nok.

Åbent I gang Opfyldt Ikke relevant

Dokumentation / begrundelse

**A.8.26 Sikkerhedskrav til applikationer: Sikkerhedskrav til applikationer er identificeret, specificeret og godkendt under udvikling og anskaffelse.**

Det taler for: Sikkerhedskrav som udtrykkelige punkter i kravlisten eller som en genbrugelig tjekliste, for eksempel med udgangspunkt i udbredte standarder for verifikation af applikationssikkerhed. Dokumenteres med sager eller kravdokumenter med en sikkerhedsvinkel.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.27 Sikker systemarkitektur og tekniske principper: Principper for sikker systemudvikling er etableret, dokumenteret og bliver anvendt på udviklingsaktiviteterne.**

Det taler for: Dokumenterede principper som mindst mulige rettigheder, forsvar i dybden, sikre standardindstillinger, dataminimering og en zero trust-tilgang sammen med synlig anvendelse af dem i arkitekturskitser eller beslutningsnotater.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.28 Sikker kodning: Principper for sikker kodning bliver anvendt i softwareudviklingen.**

Det taler for: Nyt i udgaven fra 2022. Dokumenteres med bindende koderegler, statisk kodeanalyse og scanning for hemmeligheder som obligatoriske tjek i CI, brug af efterprøvede biblioteker og dokumenterede kodegennemgange. Hvor funktionsadskillelse er umulig, træder håndhævede automatiske tjek i stedet for fireøjeprincippet; begrund det, og dokumentér det med pipelinekonfigurationen.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.29 Sikkerhedstest i udvikling og accept: Processer for sikkerhedstest er fastlagt og implementeret inden for udviklingslivscyklussen.**

Det taler for: Automatiske sikkerhedstest i pipelinen (afhængighedstjek, statisk og dynamisk analyse) plus en periodisk penetrationstest, hvor beskyttelsesbehovet er forhøjet. Dokumenteres med daterede testrapporter og opfølgningen på fundene.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.30 Outsourcet udvikling: Outsourcete udviklingsaktiviteter bliver styret, overvåget og gennemgået.**

Det taler for: Er udviklingen outsourcet, fastsættes sikkerhedskravene i kontrakten, ejerskabet til koden og retten til gennemgang sikres, og der køres kodegennemgange og sikkerhedstest før accept. Uden outsourcet udvikling skal den manglende anvendelighed begrundes sammenhængende i SoA.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.31 Adskillelse af udviklings-, test- og produktionsmiljøer: Udviklings-, test- og produktionsmiljøer er adskilt og beskyttet.**

Det taler for: Separate konti, projekter eller navnerum, separate adgangsuplysninger og separate datasæt. Sammen med A.8.11 sikres det, at ingen produktionsdata havner i miljøer uden for produktionen. Dokumenteres med miljøoversigten og rettighedstildelingen.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.32 Ændringsstyring: Ændringer i informationsbehandlingsfaciliteter og informationssystemer er underlagt procedurer for ændringsstyring.**

Det taler for: En ændringsproces med anmodning, konsekvensvurdering, test, godkendelse, gennemførelse og en vej tilbage. I udviklingsteams opfylder en pipeline med pull requests, håndhævede tjek og loggede deployments dette punkt, forudsat at historikken er uforanderlig.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.33 Testinformation: Testinformation bliver udvalgt, beskyttet og styret på passende vis.**

Det taler for: Princippet: ingen rigtige personoplysninger i testsystemer. Er det uundgåeligt, dokumenteres godkendelsen, maskeringen, adgangsbegrænsningen og sletningen efter testen. Dokumenteres med testdatakonceptet og slettelogfilerne.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse

**A.8.34 Beskyttelse af informationssystemer under audittest: Audittest, der indebærer adgang til produktionssystemer, er planlagt og aftalt med ledelsen for at undgå forstyrrelser i driften.**

Det taler for: En auditaftale med et tidsvindue, et omfang, skrivebeskyttet adgang hvor det er muligt, logning af auditadgangen og godkendelse fra ledelsen. Det gælder også penetrationstest: en skriftlig testtilladelse med tidsvindue og en nødkontakt er dokumentationen.

Åbent      I gang      Opfyldt      Ikke relevant

Dokumentation / begrundelse