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 kontekst 8

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 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

4.3-2 **Anvendelsesområdet foreligger som dokumenteret information og angiver ISMS-grænserne utvetydigt.** Dokument

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

4.4-1 **ISMS er etableret, implementeret, vedligeholdt og løbende forbedret, herunder de nødvendige processer og deres samspil.**

Det taler for: Et proceskort eller en procesliste, der forbinder risikostyring, hændelseshåndtering, ændringsstyring, audit og ledelsens evaluering med ejere og frekvens. Levende dokumentation vejer tungere end diagrammet: sager, referater, kalenderposter.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

5 Lederskab 8

5.1-1 **Øverste ledelse tager ansvar for virkningen af ISMS og sikrer, at politikken og målene er etableret og forenelige med den strategiske retning.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

5.1-2 **Kravene til ISMS er integreret i forretningsprocesserne, og betydningen af virksom informationssikkerhed bliver kommunikeret.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

5.1-3 **Ledelsen stiller de nødvendige ressourcer til rådighed, støtter de personer, der bidrager til virkningen af ISMS, og fremmer løbende forbedring.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

5.2-1 **Der er etableret en politik for informationssikkerhed, som passer til organisationens formål og udgør rammen for målene for informationssikkerhed.** Dokument

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

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. Henvis 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, hændelseskoordinator 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: Handlingsplan 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 **Processen sikrer, at gentagne risikovurderinger giver konsistente, gyldige og sammenlignelige resultater.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

6.1.2-3 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

6.1.2-4 **De identificerede risici er analyseret: mulige konsekvenser, realistisk sandsynlighed og det resulterende risikoniveau er fastlagt.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

6.1.2-5 **Risiciene er sammenholdt med acceptkriterierne og prioriteret til behandling.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

6.1.2-6 **Processen for risikovurdering foreligger som dokumenteret information.** Dokument

Det taler for: Selve metoden er et obligatorisk dokument, ikke kun dens resultat. En godkendt politik med version og godkendelsesdato, linket fra ISMS-dokumentoversigten.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

6.1.3-1 **For hver risiko over acceptgrænsen er der valgt en passende behandlingsmulighed (reducere, undgå, overføre eller acceptere).**

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 forsikringspolicen.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

6.1.3-2 **Alle kontroller, der er nødvendige for at gennemføre de valgte behandlingsmuligheder, er fastlagt.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

6.1.3-3 **De fastlagte kontroller er sammenholdt med kontrollerne i bilag A for at verificere, at ingen nødvendig kontrol er blevet overset.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

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 registrets 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 auditydelser. 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 hændelseshåndtering 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 phishingsimulering 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 **Der foreligger passende dokumenteret information som dokumentation for kompetencen.** Dokument

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

7.3-1 **De personer, der arbejder inden for anvendelsesområdet, kender politikken for informationssikkerhed.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

7.3-2 **Medarbejderne kender deres eget bidrag til virkningen af ISMS og fordelene ved en bedre informationssikkerhedspræstation.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

7.3-3 **Medarbejderne kender konsekvenserne af ikke at overholde kravene i ISMS.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

7.4-1 **Den interne og eksterne kommunikation, der er relevant for ISMS, er fastlagt: hvad der kommunikeres, hvornår, med hvem og ad hvilken vej.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

7.5.1-1 **ISMS omfatter den dokumenterede information, som standarden kræver, samt den dokumenterede information, som organisationen har fastlagt som nødvendig for virkningen af ISMS.** Dokument

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

7.5.2-1 **Ved oprettelse og opdatering af dokumenter er passende identifikation, format og medie sikret, og dokumenterne bliver gennemgået og godkendt med hensyn til egnethed.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

7.5.3-1 **Den dokumenterede information er tilgængelig og egnet til brug, hvor og når der er behov for den.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

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. Dokumentationen 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, kontrakthenvisning 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 **Risikovurderinger bliver gennemført med planlagte intervaller og altid ved væsentlige ændringer eller hændelser, under hensyn til de fastlagte kriterier.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

8.2-2 **Resultaterne af risikovurderingerne opbevares som dokumenteret information.** Dokument

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

8.3-1 **Risikobehandlingsplanen er gennemført.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

8.3-2 **Resultaterne af risikobehandlingen opbevares som dokumenteret information.** Dokument

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9 Præstationsevaluering 21

9.1-1 **Det er fastlagt, hvad der skal overvåges og måles, herunder processerne og kontrollerne for informationssikkerhed.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.1-2 **Metoderne til overvågning, måling, analyse og evaluering er fastlagt og giver gyldige resultater.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.1-3 **Det er fastlagt, hvornår og af hvem overvågning og måling bliver udført, og hvornår resultaterne bliver analyseret og evalueret.**

Det taler for: Tilføj kolonner til frekvens og ansvarlig i målearket. En tilbagevendende kalenderaftale til evalueringen beviser regelmæssigheden bedre end nogen beskrivelse.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.1-4 **Resultaterne af overvågning og måling opbevares som dokumenteret information.** Dokument

Det taler for: Arkiverede evalueringer, eksporterede dashboards eller et måleark, der føres som en tidsserie. En livevisning uden historik opfylder ikke kravet.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.1-5 **Informationssikkerhedens præstation og virkningen af ISMS bliver evalueret på grundlag af måleresultaterne.**

Det taler for: En skriftlig evaluering, ikke kun tal: tendens, årsager, behov for handling. Denne evalueringstekst er samtidig et input til ledelsens evaluering.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.2.1-1 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.2.2-1 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.2.2-2 **Auditkriterier og auditomfang er fastlagt for hver audit.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.2.2-3 **Auditorer er udvalgt, og audits bliver gennemført på en måde, der sikrer objektivitet og upartiskhed. Ingen auditerer sit eget arbejde.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.2.2-4 **Auditresultaterne bliver rapporteret til den relevante ledelse.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

9.2.2-5 **Dokumenteret information om auditprogrammet og auditresultaterne opbevares.** Dokument

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

9.3.1-1 **Øverste ledelse evaluerer ISMS med planlagte intervaller for at sikre, at det fortsat er egnet, tilstrækkeligt og virksomt.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

9.3.2-1 **Ledelsens evaluering behandler status for handlinger fra tidligere evalueringer.**

Det taler for: Referatet starter med en opfølgningstabel over sidste års beslutninger og deres aktuelle status. Uden denne tilbagereference tæller evalueringen som ufuldstændig.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

9.3.2-2 **Ledelsens evaluering behandler ændringer i de eksterne og interne forhold, der er relevante for ISMS, herunder relevante aspekter af klimaforandringer.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

9.3.2-3 **Ledelsens evaluering behandler ændringer i interessenternes behov og forventninger, som er relevante for ISMS.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

9.3.2-4 **Ledelsens evaluering behandler tilbagemeldinger om informationssikkerhedens præstation, herunder afvigelser og korrigerende handlinger, resultater af overvågning og måling, auditresultater og opfyldelsen af målene for informationssikkerhed.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

9.3.2-5 **Ledelsens evaluering behandler tilbagemeldinger fra interessenter.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

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 ledelseseffekten 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 overførbarhed 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 varsling 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 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.5.12 **Klassifikation af information: Information bliver klassificeret efter sit beskyttelsesbehov med hensyn til fortrolighed, integritet, tilgængelighed og retlige krav.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.5.13 **Mærkning af information: Klassifikationsniveauet er synligt på selve dokumentet, filen eller meddelelsen, så modtagerne ved, hvordan de skal håndtere den, uden først at spørge.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.5.14 **Overførsel af information: Der foreligger regler, procedurer og aftaler for overførsel af information inden for organisationen og med eksterne parter.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.5.15 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.5.16 **Identitetsstyring: Hele livscyklussen for identiteter bliver styret.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.5.17 **Autentifikationsinformation: Tildeling og styring af autentifikationsinformation er styret af en proces, der kræver, at personerne håndterer den korrekt.**

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 skærmbilleder af konfigurationen og rapporten fra adgangskodeværktøjet.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

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 databehandleraftale 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 **Vurdering af og beslutning om informationssikkerhedsbegivenheder: Sikkerhedsbegivenheder bliver vurderet, og der bliver truffet beslutning om, hvorvidt de skal klassificeres som informationssikkerhedshændelser.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.5.26 **Håndtering af informationssikkerhedshændelser: Hændelser bliver håndteret i overensstemmelse med de dokumenterede procedurer.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.5.27 **Læring af informationssikkerhedshændelser: Viden fra hændelser bliver brugt til at styrke sikkerhedskontrollerne.**

Det taler for: En gennemgang efter hændelsen uden skyldsplacering med grundårsagsanalyse og udledte handlinger, koblet til forbedringsregistret og, hvor der er behov, til risikoregistret.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.5.28 **Indsamling af beviser: Det er styret, hvordan spor, der vedrører en sikkerhedsbegivenhed, bliver identificeret, sikret og opbevaret, så de fortsat kan bruges senere.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.5.29 **Informationssikkerhed under driftsforstyrrelser: Organisationen planlægger, hvordan informationssikkerheden bliver opretholdt på et passende niveau under en driftsforstyrrelse.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.5.30 **IKT-beredskab til forretningskontinuitet: IKT-beredskabet er planlagt, implementeret, vedligeholdt og testet på grundlag af mål for forretningskontinuitet og krav til IKT-kontinuitet.**

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.5.31 **Juridiske, lovgivningsmæssige, regulatoriske og kontraktlige krav: De relevante krav og fremgangsmåden til at opfylde dem er identificeret, dokumenteret og holdt ajour.** Dokument

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.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

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 skatterelevante 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, databehandleraftaler, 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 hærdningsbaseline, stikprøver af dokumentmærkningen og automatiske politiktjek i cloudmiljøet. Afvigelser går videre til registret over korrigerende 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 opsige 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 diskkryptering, 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 sikkerhedsperimetre: Sikkerhedsperimetre er fastlagt og bliver brugt til at beskytte områder, der rummer information og informationsbehandlingsfaciliteter.**

Det taler for: En beskrivelse af perimetrene med en skitse eller fotos: bygning, kontor, serverskab. På et hjemmekontor er perimeteren 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 adgangsoplysninger) 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 diskkryptering, 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 **Kabelsikkerhed: Kabler til strøm, data og kommunikation er beskyttet mod aflytning, forstyrrelse og skade.**

Det taler for: Ejes 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 destruktion), eller et destruktionscertifikat fra en leverandør. For krypterede enheder er den dokumenterede destruktion 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 hærdningsbaseline 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 gruppemedlemskaber. 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 repositoriet 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 kapacitetseftersyn 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 begrunder 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 slettelogfiler. 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 adgangsoplysninger 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 **Forebyggelse af datalækage: Foranstaltninger til at forebygge datalækage bliver anvendt på systemer, netværk og enheder, der behandler, lagrer eller overfører følsom information.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8.13 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8.14 **Redundans i informationsbehandlingsfaciliteter: Informationsbehandlingsfaciliteter er indrettet med nok redundans til at opfylde kravene til tilgængelighed.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8.15 **Logning: Sikkerhedsrelevante aktiviteter efterlader spor. Logfiler bliver dannet, opbevaret, beskyttet mod ændring og faktisk analyseret, ikke kun samlet ind.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8.16 **Overvågningsaktiviteter: Netværk, systemer og applikationer bliver overvåget for unormal adfærd, og der bliver truffet passende handlinger for at vurdere mulige sikkerhedshændelser.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8.17 **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.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8.18 **Brug af privilegerede hjælpeprogrammer: Brugen af hjælpeprogrammer, der kan tilsidesætte systembeskyttelser, er begrænset og stramt styret.**

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.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

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 nøglehvælvet.

◯ 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: Outsourcede 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 adgangsoplysninger 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

ISO/IEC 27018:2025, Informationssikkerhed, cybersikkerhed og beskyttelse af privatlivets fred: Vejledning i beskyttelse af personoplysninger (PII) i offentlige cloudtjenester i rollen som databehandler af personoplysninger (3. udgave, 2025-08)

Beskyttelse af personoplysninger (PII) i den offentlige cloud

36 krav. For denne standard findes intet akkrediteret certifikat. Udgave 07/2026.

ISO/IEC 27018 er ikke en standard for ledelsessystemer, men en vejledning med udvidede kontroller oven på ISO/IEC 27002:2022. Der findes intet selvstændigt akkrediteret certifikat efter ISO/IEC 27018. Kontrollerne optages i erklæringen om anvendelighed for et system efter ISO/IEC 27001, og certifikatet udstedes derefter efter ISO/IEC 27001 med henvisning til ISO/IEC 27018. Standarden retter sig mod leverandøren af en offentlig cloudtjeneste, der behandler personoplysninger på vegne af sine cloudkunder. En virksomhed, der alene bruger cloudtjenester, påtager sig ikke denne rolle og vurderer med fordel kravene over for sine leverandører, ikke over for sig selv. For Leanshift er denne liste derfor først og fremmest et vurderingsskema for leverandører. Hvert punkt kan stilles som spørgsmål til leverandøren og sikres gennem databehandleraftalen efter artikel 28 i GDPR. Resultatet af en sådan vurdering er en intern registrering om overensstemmelse eller en vurderingsprofil for leverandøren, ikke et certifikat. Om nummereringen: Afsnit A.2 til A.12 følger databeskyttelsesprincipperne i bilag A til standarden, punkter med numre som A.11.6 er de supplerende kontroller, der er anført der. Punkter med numre som 8.10 eller 5.34 henviser til kontroller fra ISO/IEC 27002:2022, som standarden gør specifikke for cloud. Punkter med tilføjelsen (Grundsatz), altså princip, udledes af afsnittets eget princip, hvor bilag A ikke har en selvstændig supplerende kontrol.

Virksomhed	Dato	Udfyldt af

A.2 Samtykke og valgmulighed 2

A.2.1 **Cloudleverandøren støtter cloudkunden i at opfylde de registreredes rettigheder, for eksempel indsigt, berigtigelse, sletning og indsigelse. Ansvar og frister er fastlagt i aftalen.** Dokument

Det taler for: Dokumentationen er databehandleraftalen efter artikel 28 i GDPR med en klausul om bistand ved de registreredes rettigheder, sammen med de tekniske midler i selve tjenesten: funktioner til eksport, rettelse og sletning eller en dokumenteret supportprocedure med svarfrist. Spørgsmål til leverandøren: Hvilken funktion eller hvilken proces tilbyder I, så vi kan behandle en anmodning om indsigt eller sletning inden for en måned?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.2 (Grundsatz) **Cloudkundernes personoplysninger behandles udelukkende efter kundens dokumenterede instruks. At indhente samtykke fra de registrerede er fortsat kundens opgave i rollen som dataansvarlig, og leverandøren foregriber det ikke.**

Det taler for: Dokumentationen er instruksklausulen i databehandleraftalen plus et bevis for, at leverandøren ikke gør nogen egen sekundær brug af oplysningerne, for eksempel tjenestens privatlivspolitik og produktdokumentationen. Spørgsmål til leverandøren: Behandler I vores kundedata på nogen måde uden for vores instruks, for eksempel til produktforbedring eller modeltræning?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.3 Formålets lovlighed og angivelse 2

A.3.1 **Formålet med leverandørens behandling af personoplysninger er begrænset til at levere den aftalte tjeneste og er angivet i aftalen. Der sker ingen behandling til leverandørens egne formål.** Dokument

Det taler for: Dokumentationen er databehandleraftalen med genstand, karakter, formål og varighed af behandlingen samt kategorierne af registrerede efter artikel 28, stk. 3, i GDPR. Spørgsmål til leverandøren: Send det aftalebilag, der beskriver formålet med behandlingen udtømmende. For en lille virksomhed er leverandørens standardbilag om databehandling nok, forudsat at det indeholder disse oplysninger.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.3.2 **Personoplysninger, der er betroet leverandøren, bruges ikke til reklame, markedsføring eller andre kommercielle formål hos leverandøren uden forudgående udtrykkeligt samtykke. Leveringen af tjenesten gøres ikke afhængig af et sådant samtykke.**

Det taler for: Dokumentationen er en udtrykkelig aftaleklausul, der udelukker kommerciel sekundær brug, sammen med brugsvilkårene. Spørgsmål til leverandøren: Bekræft skriftligt, at kundedata ikke bruges til reklame, profilering eller træning af AI-modeller. Mangler tilsagnet, er tjenesten uegnet til personoplysninger.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.4 Begrænset indsamling 1

A.4 (Grundskud) **Ud over de oplysninger, kunden lægger ind i tjenesten, indsamler leverandøren ikke yderligere personoplysninger til egne formål, for eksempel telemetri, brugsprofiler eller indholdsanalyse. Driftsdata og metadata, der indsamles, er angivet og begrundet.**

Det taler for: Dokumentationen er en liste over de oplysninger, tjenesten registrerer ved siden af indholdsdata (adgangslogge, telemetri, diagnosedata) med formål og opbevaringsperiode, plus et skærmbillede af den indstilling, der slår valgfri telemetri fra. Spørgsmål til leverandøren: Hvilke data om brug, telemetri og diagnostik indsamler I derudover, hvad bruger I dem til, og kan vi slå indsamlingen fra?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.5 Dataminimering 2

A.5.1 **Midlertidige filer, der opstår ved behandling af personoplysninger, for eksempel arbejdslager, caches eller tilbagerulningsjournaler, slettes sikkert inden for en fastlagt periode.**

Det taler for: Dokumentationen er en procedure for drift eller sletning med angivet opbevaringsperiode for midlertidige data, understøttet af systemkonfigurationen, for eksempel en cachetid (TTL) eller et planlagt oprydningsjob med tilhørende kørselslog. Spørgsmål til leverandøren: Efter hvor lang tid slettes caches, midlertidige filer og mellemliggende tilstande, og hvordan overvåges det?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

8.11 **Hvor drift, test eller support ikke kræver produktionsdata, er personoplysninger maskeret, pseudonymiseret eller anonymiseret. Mængden af behandlede oplysninger er begrænset til det, tjenesten faktisk har brug for.**

Det taler for: Dokumentationen er en regel om, hvilke miljøer der må se produktionsdata, plus skærmbilleder eller scripts for den maskering, der bruges i systemer til test og udvikling. Spørgsmål til leverandøren: Arbejder jeres teams for support og udvikling med produktionsdata, og i givet fald under hvilke sikringsforanstaltninger? For en lille virksomhed er en regel om, at testsystemer udelukkende kører på genererede eksempeldata, nok.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.6 Begrænset brug, opbevaring og videregivelse 3

A.6.1 **Modtager leverandøren en juridisk bindende anmodning om at videregive personoplysninger, for eksempel fra en myndighed, oplyser leverandøren cloudkunden om det på forhånd, så vidt loven tillader det.**

Det taler for: Dokumentationen er en underretningsklausul i aftalen og en intern proces for myndighedsanmodninger med en navngiven ansvarlig. Spørgsmål til leverandøren: Underretter I os, før I udleverer data, og offentliggør I en gennemsigtighedsrapport om anmodninger fra myndigheder? En aktuel gennemsigtighedsrapport er stærk dokumentation.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.6.2 **Videregiver leverandøren personoplysninger til tredjeparter, registreres hændelsen, så den kan spores: hvem der modtog oplysningerne, hvornår det skete, hvilke oplysninger der indgik, og på hvilket grundlag videregivelsen hviler.** Dokument

Det taler for: Dokumentationen er et register over videregivelser eller en sagshistorik med disse felter, også selv om det ikke indeholder poster. Et tomt, men vedligeholdt register er acceptabelt og er den praktiske vej for en lille virksomhed. Spørgsmål til leverandøren: Fører I et register over videregivelser af data, og kan vi få udtræk fra det?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

8.10 **Personoplysninger slettes, når den aftalte opbevaringsperiode udløber, eller aftalen ophører, herunder kopier i sikkerhedskopier efter deres rotationscyklus.**

Det taler for: Dokumentationen er en sletteplan med opbevaringsperioder for hver datakategori, opbevaringsperioden for sikkerhedskopier og en slettelog eller en bekræftelse på sletning. Spørgsmål til leverandøren: Hvor længe lever vores data videre i jeres sikkerhedskopier efter opsigelse, og modtager vi en skriftlig bekræftelse på sletningen?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.7 Rigtighed og kvalitet 2

A.7 (Grundskud) **Leverandøren ændrer ikke på eget initiativ de personoplysninger, der er betroet leverandøren. Rettelser og opdateringer sker udelukkende efter instruks fra cloudkunden eller gennem funktioner, som kunden selv betjener.**

Det taler for: Dokumentationen er tjenestens redigeringsfunktioner sammen med deres ændringshistorik, plus instruksklausulen i databehandleraftalen. Spørgsmål til leverandøren: Kan vi selv rette registreringer, og logges hver ændring, så den kan spores?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

8.13 **Integriteten af personoplysninger er beskyttet ved lagring, ved overførsel og ved genetablering. Der findes sikkerhedskopier, og det er testet, at de kan genetableres.**

Det taler for: Dokumentationen er konfigurationen af sikkerhedskopieringen, kontrolsum eller integritetsmekanismer og mindst en dokumenteret genetableringstest om året med dato og resultat. Spørgsmål til leverandøren: Hvor ofte tester I genetablering, og hvilken genetableringstid forpligter I jer til i serviceniveauet?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8 Åbenhed, gennemsigtighed og oplysning 2

A.8.1 **Brugen af underdatabehandlere, der behandler personoplysninger, oplyses, inden aftalen indgås. Ændringer i listen meddeles kunden i god tid, så kunden kan gøre indsigelse eller opsige.** Dokument

Det taler for: Dokumentationen er en aktuel liste over underdatabehandlere, offentliggjort eller stillet til rådighed i aftalen, med navn, land og formålet med behandlingen, plus en regel om underretning efter artikel 28, stk. 2, i GDPR. Spørgsmål til leverandøren: Hvor finder vi jeres liste over underdatabehandlere, hvor lang tid i forvejen varsler I ændringer, og hvordan kan vi gøre indsigelse?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.8 (Grundskud) **Inden aftalen indgås, stiller leverandøren forståelig information til rådighed om, hvordan personoplysninger behandles, hvilke sikringsforanstaltninger der findes, og i hvilke jurisdiktioner behandlingen sker.**

Det taler for: Dokumentationen er privatlivspolitikken, et sikkerhedswhitepaper, en side med sikkerhedsoplysninger (trust center) og databehandleraftalen med de tekniske og organisatoriske foranstaltninger som bilag. Spørgsmål til leverandøren: Send den aktuelle liste over tekniske og organisatoriske foranstaltninger som aftalebilag, ikke kun markedsføringsmateriale.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.9 Den enkeltes inddragelse og indsigt 2

A.9 (Grundskrav) **Tjenesten giver cloudkunden de tekniske midler til selv at behandle anmodninger om indsigt, berigtigelse og sletning fra de registrerede, for eksempel gennem funktioner til eksport, søgning og sletning.**

Det taler for: Dokumentationen er produktdokumentationen for funktionerne til eksport og sletning, understøttet af en intern prøvekørsel: en anmodning om indsigt gennemføres fra ende til anden, og tidsforbruget noteres. Spørgsmål til leverandøren: Kan vi finde, eksportere og slette alle data om en enkelt person uden jeres hjælp?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

5.34 **Kan kunden ikke selv håndtere en anmodning fra en registreret, bistår leverandøren inden for en aftalt frist. Anmodninger, som registrerede sender direkte til leverandøren, videresendes til kunden i stedet for at blive besvaret af leverandøren.**

Det taler for: Dokumentationen er den tilsvarende klausul i databehandleraftalen med en konkret svarfrist, plus en historik over supportsager som et virkeligt eksempel. Spørgsmål til leverandøren: Hvilken frist forpligter I jer til ved bistand til de registreredes rettigheder, og hvad koster det?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.10 Ansvarlighed 4

A.10.1 Dokument **Brud på sikkerheden, der omfatter personoplysninger, meddeles cloudkunden uden unødig forsinkelse med angivelse af omfang, berørte oplysninger, årsag og de trufne foranstaltninger. En underretningsproces med ansvar og frister er fastlagt.**

Det taler for: Dokumentationen er beredskabsplanen for hændelser med tilhørende eskaleringskæde, den aftalte underretningsfrist (24 til 48 timer fungerer i praksis, så kunden stadig kan overholde fristen på 72 timer efter artikel 33 i GDPR) og registreringer om tidligere hændelser eller om en øvelse. Spørgsmål til leverandøren: Inden for hvilken frist melder I en hændelse, gennem hvilken kanal, og hvilke oplysninger leverer I sammen med den?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.10.2 Dokument **Sikkerhedspolitikker, driftsprocedurer og de tilhørende registreringer opbevares i en fastlagt periode, så behandlingen kan rekonstrueres efterfølgende.**

Det taler for: Dokumentationen er en opbevaringsregel med versionshistorikken for politikkerne, for eksempel gennem et dokumentregister eller et versionsstyringssystem med godkendelsesdatoen. Spørgsmål til leverandøren: Hvor længe opbevarer I versioner af politikker og de tilhørende registreringer, og får vi adgang til dem ved en audit?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.10.3 Dokument **Der findes en fastlagt ordning for tilbagelevering, overførsel og destruktion af personoplysninger ved aftalens ophør, med angivelse af formater, frister og håndteringen af kopier.**

Det taler for: Dokumentationen er exitklausulen i databehandleraftalen plus en bekræftelse på sletning efter aftalens ophør. Spørgsmål til leverandøren: I hvilket format og inden for hvilken frist får vi vores data tilbage, hvornår destrueres alle kopier, og modtager vi en skriftlig bekræftelse?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

5.35 **Virkningen af sikringsforanstaltningerne gennemgås uafhængigt med regelmæssige intervaller, for eksempel gennem interne audits, penetrationstest eller erklæringer fra tredjepart. Resultaterne stilles til rådighed for cloudkunden i en egnet form.**

Det taler for: Dokumentationen er et ISO/IEC 27001-certifikat med en erklæring om anvendelighed, der omfatter kontrollerne fra ISO/IEC 27018, eller en SOC 2-rapport, sammen med aktuelle sammenfatninger af penetrationstest. Spørgsmål til leverandøren: Send certifikatet, dets anvendelsesområde og en bekræftelse på, at ISO/IEC 27018 er afspejlet i erklæringen om anvendelighed. Det er værd at kontrollere, om anvendelsesområdet virkelig dækker den anvendte tjeneste.

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11 Informationssikkerhed 13

A.11.1 **Alle med adgang til personoplysninger er pålagt tavshedspligt, uanset om de er ansat direkte eller tilknyttet eksternt.** Dokument

Det taler for: Dokumentationen er underskrevne fortrolighedsaftaler eller tavshedserklæringer, der fortsat gælder efter tilknytningens ophør. Spørgsmål til leverandøren: Er alle medarbejdere og leverandører med adgang til data skriftligt pålagt tavshedspligt?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.2 **Udskrifter og andre papirkopier med personoplysninger fremstilles kun, hvor det er strengt nødvendigt. Det tilladte omfang er fastlagt i en regel.**

Det taler for: Dokumentationen er en regel om håndtering af udskrifter, som i datacentre typisk er et generelt forbud mod at printe i områder med kundedata. Spørgsmål til leverandøren: Printes kundedata overhovedet i jeres drift, og i givet fald under hvilke betingelser?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.3 **Genetableringer fra sikkerhedskopier godkendes på forhånd og logges, herunder den person, der udløste genetableringen, og de berørte oplysninger.** Dokument

Det taler for: Dokumentationen er genetableringsloggen med tidsstempel, hvem der udløste den, og omfang, som regel dannet automatisk af værktøjet til sikkerhedskopiering. Spørgsmål til leverandøren: Logger I hver genetablering, og kan vi se disse logge ved en audit?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.4 **Lagringsmedier med personoplysninger, der forlader lokaliteterne, er beskyttet mod uautoriseret adgang og tab, som regel gennem kryptering og en transportregistrering.**

Det taler for: Dokumentationen er et bevis for kryptering (fuld mediekryptering), registreringer af transport og overdragelse samt en fortegnelse over medier. Spørgsmål til leverandøren: Forlader medier med kundedata nogensinde jeres lokaliteter, for eksempel til sikkerhedskopiering, og hvordan er de beskyttet under transporten?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.5 **Brugen af ukrypterede bærbare medier og enheder til personoplysninger er forbudt eller begrænset til begrundede undtagelser med dokumenteret godkendelse.**

Det taler for: Dokumentationen er en politik for flytbare medier plus teknisk håndhævelse, for eksempel gennemtvunget kryptering af enheder eller USB-porte, der er spærret gennem enhedsstyring. Spørgsmål til leverandøren: Kan medarbejdere kopiere kundedata over på ukrypterede enheder, og hvad forhindrer det teknisk?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.6 **Personoplysninger, der overføres over offentlige net, er krypteret. De anvendte mekanismer svarer til det aktuelle tekniske niveau.**

Det taler for: Dokumentationen er TLS-konfigurationen (aktuel protokolversion, ingen forældede krypteringsalgoritmer) og en ekstern test af konfigurationen som rapport. Praktisk for en lille virksomhed: en gratis TLS-scanning køres en gang om året, og resultatet arkiveres. Spørgsmål til leverandøren: Hvilken transportkryptering håndhæver I, og er kryptering af lagrede data aktiv?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.7 **Papirregistreringer med personoplysninger destrueres på en måde, der udelukker rekonstruktion.**

Det taler for: Dokumentationen er makulatorer med et tilstrækkeligt sikkerhedsniveau eller destruktionscertifikater fra en leverandør, der arbejder efter DIN 66399 eller en tilsvarende standard. Spørgsmål til leverandøren: Hvordan destruerer I papirregistreringer om kunder, og er destruktionscertifikaterne arkiveret?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.8 **Hvert bruger-id er tildelt entydigt til en enkelt person og bliver hverken genudstedt eller delt. Fælleskonti findes kun i begrundede undtagelser og med yderligere sporbarhed.**

Det taler for: Dokumentationen er en brugerliste fra identitetssystemet uden gruppekonti, sammen med reglen om, at administrativt arbejde udføres under en personlig konto. Spørgsmål til leverandøren: Arbejder jeres driftsmedarbejdere med personlige konti, og er flerfaktorgodkendelse obligatorisk?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.9 **Leverandøren kan til enhver tid oplyse, hvilke personer eller roller der må tilgå personoplysninger, og holder oversigten opdateret.** Dokument

Det taler for: Dokumentationen er en oversigt over adgangsrettigheder efter rolle, understøttet af en tilbagevendende gennemgang af adgange med dato og resultat. For en lille virksomhed er et halvårligt udtræk af brugerlisten med godkendelse nok. Spørgsmål til leverandøren: Hvor mange af jeres medarbejdere kan tilgå vores data, og hvor ofte gennemgår I det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.10 **Brugerkonti styres gennem hele deres livscyklus: oprettelse, ændring og hurtig deaktivering ved fratrædelse eller rolleskift.**

Det taler for: Dokumentationen er en procedure for tiltrædelse og fratrædelse med en tjekliste, plus logge over deaktiverede konti med tidsstempler. Spørgsmål til leverandøren: Inden for hvilken frist inddrager I adgangen for medarbejdere, der fratræder, og hvordan dokumenterer I det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.11 **Leverandørens forpligtelser til sikkerhed og databeskyttelse er fastlagt i aftalen, herunder de tekniske og organisatoriske foranstaltninger, den bindende virkning af kundens instruks og kundens ret til audit.** Dokument

Det taler for: Dokumentationen er den underskrevne databehandleraftale efter artikel 28 i GDPR med bilaget over foranstaltninger og en ret til audit eller information. Spørgsmål til leverandøren: Send den underskrevne databehandleraftale med bilag, ikke blot en henvisning til generelle brugsvilkår.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.12 **Underdatabehandlere, der behandler personoplysninger, er underlagt mindst de samme forpligtelser som leverandøren selv. Udvælgelsen og den løbende overvågning af dem følger en fastlagt proces.**

Det taler for: Dokumentationen er videreførelsen af forpligtelserne i aftalerne med underdatabehandlere (artikel 28, stk. 4, i GDPR) og en leverandørvurdering med dato. Spørgsmål til leverandøren: Hvordan vurderer I jeres underdatabehandlere, og hvilken dokumentation kræver I af dem?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.13 **Inden lagerplads genbruges, er det sikret, at ingen data fra tidligere brugere fortsat er tilgængelige, hverken på fysiske medier eller i virtualiserede miljøer.**

Det taler for: Dokumentationen er proceduren for rensning eller overskrivning, når lagerplads frigives, registreringer om destruktion af medier og den adskillelse mellem kunder (tenants), der er beskrevet i arkitekturdokumentet. Spørgsmål til leverandøren: Hvordan sikrer I, at genbrugt lagerplads ikke indeholder restdata fra andre kunder?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.12 Overholdelse af databeskyttelse 3

A.12.1 **De lande, hvor personoplysninger lagres og behandles, er angivet og kendt af cloudkunden. Ændringer af lagringsstederne meddeles.** Dokument

Det taler for: Dokumentationen er leverandørens oversigt over lokaliteter og regioner, i aftalen eller i dokumentationen, plus et skærmbillede af regionsindstillingen for den anvendte tjeneste. Spørgsmål til leverandøren: I hvilke lande ligger vores data i hvile, fra hvilke lande tilgås de, for eksempel i support, og kan vi fastlåse regionen?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.12.2 **Overførsler af personoplysninger til tredjelande er kendte, begrundede og dækket af fornødne garantier.** Dokument

Det taler for: Dokumentationen er standardkontraktbestemmelser eller en afgørelse om tilstrækkeligt beskyttelsesniveau, understøttet af en vurdering af overførslens konsekvenser, som for en lille virksomhed kan være kort: berørte datakategorier, modtagerland, risiko, trufne supplerende foranstaltninger. Spørgsmål til leverandøren: På hvilket retsgrundlag overfører I data til tredjelande, og hvilke supplerende foranstaltninger anvender I?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

5.31 **De lovmæssige og aftalemæssige krav til behandlingen af personoplysninger er identificeret og holdes aktuelle, når retstilstanden ændrer sig. Modstridende jurisdiktioner er vurderet.**

Det taler for: Dokumentationen er en oversigt over de gældende krav (GDPR, nationale regler, branchespecifikke pligter) med en ansvarlig og en dato for gennemgang. I en lille virksomhed er en liste på en side, der gennemgås en gang om året, nok. Spørgsmål til leverandøren: Er I eller jeres underdatabehandlere underlagt jurisdiktioner, der giver myndigheder adgang til vores data, og hvordan håndterer I det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse