ISO/IEC 27001:2022 + Amd 1:2024 Informatiebeveiligingsmanagementsystemen (ISMS)

Informatiebeveiliging, ISMS, wereldwijd certificeerbaar

181 eisen. Deze norm is certificeerbaar door een geaccrediteerde instelling. Versie van 07/2026.

ISO/IEC 27001 stelt de eisen vast voor een informatiebeveiligingsmanagementsysteem: risicogebaseerd, gedocumenteerd en aantoonbaar effectief. Een beoordeling ertegen is een geaccrediteerde certificatie audit in twee fasen (documentbeoordeling, gevolgd door een beoordeling van de effectiviteit ter plaatse), gevolgd door jaarlijkse surveillance audits en hercertificering na drie jaar.

Bedrijf	Datum	Opgesteld door

4 Context van de organisatie 8

4.1-1 De externe en interne kwesties die van invloed zijn op het vermogen van de organisatie om de beoogde resultaten van het ISMS te bereiken, zijn vastgesteld en worden actueel gehouden.

Waaraan je het vaststelt: Aangetoond via een contextanalyse, hetzij als zelfstandig document, hetzij als onderdeel van het ISMS handboek: marktomgeving, klant en contractsituatie, wettelijk kader (AVG, NIS2), technologiestack, personeelsbezetting, afhankelijkheid van cloudleveranciers. Voor kleine organisaties volstaat een tabel van een pagina met datum en beoordelingscyclus, mits de directiebeoordeling laat zien dat deze daadwerkelijk wordt bijgewerkt.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

4.1-2 De organisatie heeft bepaald of klimaatverandering een relevante kwestie voor haar is. De vaststelling is onderbouwd, ongeacht of het antwoord ja of nee is.

Waaraan je het vaststelt: Deze eis is geintroduceerd door Amd 1:2024 en auditors vragen er specifiek naar. Houd een aparte regel in de contextanalyse aan: hitteperiodes die van invloed zijn op serverruimtes en beschikbaarheid, extreem weer dat datacenters van cloudleveranciers raakt, stabiliteit van het elektriciteitsnet. Een onderbouwde uitkomst van niet relevant is aanvaardbaar, een ontbrekende regel niet.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

4.2-1 De belanghebbenden die relevant zijn voor het ISMS zijn vastgesteld.

Waaraan je het vaststelt: Belanghebbendenlijst met klanten, medewerkers, verwerkers en subverwerkers, toezichthouders, verzekeraars, de certificatie instelling en aandeelhouders. In kleine organisaties volstaat een tabel met partij, verwachting en bron van de verwachting.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

4.2-2 De relevante eisen van deze belanghebbenden zijn vastgesteld, met inbegrip van eisen die verband houden met klimaatverandering.

Waaraan je het vaststelt: Noem voor elke partij de concrete bron: contractbepaling, verwerkersovereenkomst, klantvragenlijst, wettelijke verplichting. Amd 1:2024 voegt een noot toe dat belanghebbenden eisen kunnen hebben die verband houden met klimaatverandering. Het is geen zelfstandige moet eis, maar auditors brengen het regelmatig ter sprake, bijvoorbeeld duurzaamheidsvragen in de leveranciersaudit van een grote klant. Een regel in de belanghebbendentabel met het resultaat (inclusief geen van dien aard) volstaat.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

4.2-3 Er is bepaald en traceerbaar welke van deze eisen via het ISMS worden geadresseerd.

Waaraan je het vaststelt: Voeg een kolom toe aan de belanghebbendentabel die verwijst naar de regel die de eis adresseert (beleid, beheersmaatregel, contractbijlage). Dit toont aan dat eisen niet alleen zijn verzameld maar ook daadwerkelijk zijn verwerkt.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

4.3-1 **De reikwijdte van het ISMS is vastgesteld en houdt rekening met de kwesties uit 4.1, de eisen uit 4.2 alsmede raakvlakken en afhankelijkheden met activiteiten die door derden worden uitgevoerd.**

Waaraan je het vaststelt: De reikwijdte noemt locaties, organisatie-eenheden, producten, systemen en netwerkgrenzen. Uitbestede onderdelen (hosting, betaalproviders, support) worden beschreven als raakvlakken met een duidelijke verantwoordelijkheidsgrens. Een kunstmatig versmalde reikwijdte die kernprocessen wegdefinieert wordt door certificatie instellingen afgewezen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

4.3-2 **De reikwijdte is beschikbaar als gedocumenteerde informatie en geeft de grenzen van het ISMS ondubbelzinnig aan.** Document

Waaraan je het vaststelt: Een goedgekeurd reikwijdtedocument met versie, datum en akkoord van de directie. De exacte bewoording verschijnt later op het certificaat, formuleer het dus precies en op een manier die publiekelijk geciteerd kan worden.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

4.4-1 **Het ISMS, met inbegrip van de benodigde processen en hun onderlinge samenhang, wordt vastgesteld, geimplementeerd, onderhouden en voortdurend verbeterd.**

Waaraan je het vaststelt: Een procesoverzicht of proceslijst die risicomanagement, incidentafhandeling, wijzigingsbeheer, auditing en directiebeoordeling koppelt aan eigenaren en frequentie. Levend bewijs telt zwaarder dan het schema: tickets, notulen, agenda items.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5 Leiderschap 8

5.1-1 **De directie neemt verantwoordelijkheid voor de effectiviteit van het ISMS en zorgt ervoor dat het beleid en de doelstellingen worden vastgesteld en verenigbaar zijn met de strategische richting.**

Waaraan je het vaststelt: Bewijs omvat ondertekende goedkeuringen van het beleid, de reikwijdte en de Verklaring van Toepasselijkheid, notulen van de directiebeoordeling en gedocumenteerde budgetbeslissingen. In zeer kleine organisaties is de directie vaak dezelfde persoon als de ISMS eigenaar, wat aanvaardbaar is mits dit openlijk wordt vermeld in de roldefinitie.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5.1-2 **De eisen van het ISMS worden geintegreerd in de bedrijfsprocessen en het belang van effectieve informatiebeveiliging wordt gecommuniceerd.**

Waaraan je het vaststelt: Het beste zichtbaar waar beveiliging geen apart mapje is: een beveiligingscriterium in de definitie van klaar, een beveiligingscheck in het verkoop of inkoopproces, een terugkerend beveiligingsonderwerp in teamvergadering notulen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5.1-3 **De directie stelt de nodige middelen beschikbaar, ondersteunt de mensen die bijdragen aan de effectiviteit van het ISMS en bevordert voortdurende verbetering.**

Waaraan je het vaststelt: Goedgekeurd beveiligingsbudget, tijd voor training, inzet van externe auditors of pentesters. Een verbeter of actieregister met vermeldingen over meerdere kwartalen toont continuiteit in plaats van een eenmalige inspanning.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5.2-1 **Er is een informatiebeveiligingsbeleid vastgesteld dat past bij het doel van de organisatie en een kader biedt voor de informatiebeveiligingsdoelstellingen.** Document

Waaraan je het vaststelt: Een kort goedgekeurd beleidsdocument, twee tot drie pagina's volstaan. Het noemt de beschermingsdoelen, de reikwijdte, de verantwoordelijkheden en het principe van een risicogebaseerde aanpak. Generieke sjabloontekst zonder link naar de daadwerkelijke bedrijfsvoering valt op tijdens de audit.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5.2-2 **Het beleid omvat een toezegging om aan toepasselijke eisen te voldoen en een toezegging tot voortdurende verbetering van het ISMS.** Document

Waaraan je het vaststelt: Beide toezeggingen moeten als expliciete zinnen in het beleid staan, en ze worden woordelijk voorgelezen in de stage 1 audit. Verwijs daarnaast naar de onderliggende processen (wettelijk register, verbeterregister).

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5.2-3 **Het beleid wordt binnen de organisatie gecommuniceerd en is waar passend beschikbaar voor belanghebbenden.** Document

Waaraan je het vaststelt: Bewijs via een intranet of wiki vermelding met leesplicht, een onboarding checklist met bevestiging, of een gepubliceerde samenvatting op de website. Een verspreidingslijst met leesbevestigingen is het eenvoudigste solide bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5.3-1 **Verantwoordelijkheden en bevoegdheden voor beveiligingsrelevante rollen zijn toegewezen en binnen de organisatie gecommuniceerd.**

Waaraan je het vaststelt: Een rolmatrix (RACI) met de ISMS eigenaar, risico eigenaren, asset eigenaren, de incidentcoordinator en het aanspreekpunt gegevensbescherming. Wijs in eenmansbedrijven of zeer kleine teams elke rol toe aan een met naam genoemde persoon en documenteer de daaruit voortvloeiende rolstapeling openlijk in plaats van te verbergen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

5.3-2 **De bevoegdheid om ervoor te zorgen dat het ISMS voldoet aan de norm en om over de ISMS prestaties te rapporteren aan de directie is aan een rol toegewezen.**

Waaraan je het vaststelt: Een benoemingsbrief of roloomschrijving voor de ISMS eigenaar met een expliciete rapportagelijn naar de directie. De rapportagelijn moet daadwerkelijk blijken uit notulen van de directiebeoordeling.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6 Planning 21

6.1.1-1 **Uitgaande van de kwesties in 4.1 en de eisen in 4.2 worden de risico's en kansen bepaald die aangepakt moeten worden, zodat het ISMS zijn beoogde resultaten bereikt en ongewenste effecten worden voorkomen.**

Waaraan je het vaststelt: Een register dat contextkwesties koppelt aan risico's en kansen, hetzij apart bijgehouden, hetzij binnen het risicoregister. Het gaat om traceerbaarheid: elke kwestie uit de contextanalyse leidt zichtbaar naar een beoordeling of naar een onderbouwd besluit om deze niet in aanmerking te nemen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.1-2 **De acties om deze risico's en kansen aan te pakken worden gepland, geintegreerd in de ISMS processen, en de effectiviteit ervan wordt geevalueerd.**

Waaraan je het vaststelt: Actieplan met eigenaar, streefdatum en effectiviteitscriterium. Houd de effectiviteitsevaluatie als eigen kolom aan, anders ontbreekt in de audit het bewijs dat de actie niet alleen is uitgevoerd maar ook geverifieerd.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.2-1 **Er is een proces voor informatiebeveiligingsrisicobeoordeling gedefinieerd en toegepast; het omvat risicoacceptatiecriteria en criteria voor het uitvoeren van risicobeoordelingen.** Document

Waaraan je het vaststelt: Een risicomanagementbeleid met schalen voor waarschijnlijkheid en impact, een gedefinieerde risicomatrix en een duidelijke acceptatiedrempel. De drempel moet een getal of een zone zijn, geen zinsnede als naar eigen inzicht.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.2-2 **Het proces zorgt ervoor dat herhaalde risicobeoordelingen consistente, geldige en vergelijkbare resultaten opleveren.**

Waaraan je het vaststelt: Aangetoond via een vaste methodiek met gedefinieerde schalen en door twee beoordelingsversies te vergelijken: dezelfde risico's, dezelfde beoordelingslogica, verklaarbare verschillen. Een gedateerde versie van het risicoregister van vorig jaar is hier het sterkste bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.2-3 **Informatiebeveiligingsrisico's worden geidentificeerd om verlies van vertrouwelijkheid, integriteit en beschikbaarheid binnen de reikwijdte te detecteren, en aan elk risico wordt een risico eigenaar toegewezen.**

Waaraan je het vaststelt: Risicoregister dat verwijst naar assets of processen, de drie beschermingsdoelen en een met naam genoemde risico eigenaar. De risico eigenaar moet bevoegd zijn het risico te accepteren; in kleine organisaties is dit doorgaans de directeur.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.2-4 **De geidentificeerde risico's worden geanalyseerd: mogelijke gevolgen, realistische waarschijnlijkheid en het resulterende risiconiveau worden bepaald.**

Waaraan je het vaststelt: Kolommen voor impact, waarschijnlijkheid en resulterend risiconiveau, elk met een korte onderbouwing. Een zin toelichting per risico voorkomt de meest voorkomende auditbevinding, namelijk getallen zonder herleiding.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.2-5 **De risico's worden vergeleken met de acceptatiecriteria en geprioriteerd voor behandeling.**

Waaraan je het vaststelt: Het risicoregister moet laten zien welke risico's boven de acceptatiedrempel liggen en in welke volgorde ze behandeld worden. Een gesorteerde weergave of een prioriteitskolom volstaat.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.2-6 **Het proces voor risicobeoordeling is beschikbaar als gedocumenteerde informatie.** Document

Waaraan je het vaststelt: De methodiek zelf is een verplicht document, niet alleen de uitkomst ervan. Een goedgekeurd beleid met versie en goedkeuringsdatum, gekoppeld vanuit de ISMS documentindex.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.3-1 **Voor elk risico boven de acceptatiedrempel wordt een passende behandeloptie gekozen (verminderen, vermijden, overdragen of accepteren).**

Waaraan je het vaststelt: Een behandeloptiekolom in het risicoregister. Wanneer een risico wordt geaccepteerd, leg de onderbouwing en de formele goedkeuring van de risico eigenaar vast; bij overdracht noem het contract of de verzekeringspolis.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.3-2 **Alle beheersmaatregelen die nodig zijn om de gekozen risicobehandelopties te implementeren worden bepaald.**

Waaraan je het vaststelt: Formuleer beheersmaatregelen concreet en verifieerbaar, met een eigenaar en een streefdatum. Verwijzen naar technisch werk dat al gaande is (MFA uitrol, back uptest) is prima zolang het verwijst naar een ticket of een configuratie artefact.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.3-3 **De bepaalde beheersmaatregelen worden vergeleken met de maatregelen in Bijlage A om te verifieren dat geen noodzakelijke maatregel over het hoofd is gezien.**

Waaraan je het vaststelt: De vergelijking is een aparte, traceerbare stap, geen bijproduct. Aangetoond door een mapping kolom in het risicoregister die verwijst naar Bijlage A nummers, plus gedateerde notulen van de vergelijking.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.3-4 **Er bestaat een Verklaring van Toepasselijkheid (VvT). Deze beoordeelt alle 93 beheersmaatregelen uit Bijlage A afzonderlijk, geeft per maatregel de toepasselijkheid met onderbouwing aan, de implementatiestatus, en de onderbouwing voor elke uitsluiting.** Document

Waaraan je het vaststelt: De VvT is het centrale verplichte document en de plattegrond van de hele audit. Deze moet volledig zijn: maatregelen die niet van toepassing zijn verschijnen ook met een onderbouwing, nooit als lege regel. Aanbevolen kolommen: maatregelnummer, titel, van toepassing ja of nee, onderbouwing, implementatiestatus, verwijzing naar beleid of bewijs, koppeling naar het risico. Versie en goedkeuring door de directie zijn verplicht, omdat de VvT bij elke surveillance audit tegen de werkelijkheid wordt getoetst.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.3-5 **Er wordt een risicobehandelplan opgesteld dat beheersmaatregelen, verantwoordelijkheden, streefdata en benodigde middelen samenbrengt.** Document

Waaraan je het vaststelt: Dit kan een tabblad in het risicospreadsheet of een projectbord zijn. Wat telt is dat de data realistisch zijn en dat gemiste data zichtbaar zijn herpland, want dat is precies wat de auditor controleert.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.3-6 **Het risicobehandelplan wordt goedgekeurd door de risico eigenaren en de resterende restrisico's worden door hen formeel geaccepteerd.** Document

Waaraan je het vaststelt: Handtekening, elektronische goedkeuring of een gedateerd besluit in notulen. Een regel in de notulen van de directiebeoordeling die naar de versie van het register verwijst volstaat, mits de versie ondubbelzinnig is.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.1.3-7 **Het proces voor risicobehandeling is beschikbaar als gedocumenteerde informatie.** Document

Waaraan je het vaststelt: Meestal opgenomen in hetzelfde beleidsdocument als de risicobeoordeling. De stroom van beoordeling via optiekeuze tot restrisicoacceptatie moet worden beschreven.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.2-1 **Informatiebeveiligingsdoelstellingen worden vastgesteld voor relevante functies en niveaus, zijn consistent met het beleid, en zijn waar praktisch haalbaar meetbaar.**

Waaraan je het vaststelt: Een doelstellingenoverzicht met drie tot zes doelstellingen, elk met een meetwaarde, een uitgangspunt, een streefwaarde en een deadline. Voorbeeld: aandeel systemen met MFA verhoogd van 80 naar 100 procent tegen het einde van het kwartaal. Doelstellingen zonder getal tellen als niet meetbaar.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.2-2 **De doelstellingen houden rekening met de toepasselijke informatiebeveiligingseisen alsook met de resultaten van risicobeoordeling en risicobehandeling.**

Waaraan je het vaststelt: Voeg een herkomstkolom toe aan het doelstellingenoverzicht: van welk risico, welke klanteis of welke wettelijke verplichting de doelstelling afkomstig is. Dit voorkomt doelstellingen die willekeurig lijken.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6.2-3 **De doelstellingen worden bewaakt, gecommuniceerd en waar nodig bijgewerkt.**

Waaraan je het vaststelt: Kwartaalgewijze voortgangsbewaking in het doelstellingenoverzicht plus communicatie naar het team, bijvoorbeeld een korte notitie in de wiki of een agendapunt in de teamvergadering. Historische versies tonen aan dat updates plaatsvinden.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

6.2-4 **De informatiebeveiligingsdoelstellingen zijn beschikbaar als gedocumenteerde informatie.** Document

Waaraan je het vaststelt: Een goedgekeurd doelstellingendocument met datum volstaat. Het kan onderdeel zijn van de directiebeoordeling, maar moet daar als eigen terugvindbaar onderdeel bestaan.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

6.2-5 **Voor elke doelstelling wordt gepland wat er gedaan wordt, welke middelen nodig zijn, wie verantwoordelijk is, wanneer het voltooid wordt en hoe de resultaten worden geevalueerd.**

Waaraan je het vaststelt: Deze vijf punten zijn afzonderlijk verifieerbaar en worden afzonderlijk bevraagd in de audit. Zet ze op als vijf kolommen in het doelstellingenoverzicht, dan is conformiteit in een oogopslag zichtbaar.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

6.3-1 **Wanneer de organisatie vaststelt dat wijzigingen aan het ISMS nodig zijn, worden die wijzigingen op een geplande manier uitgevoerd.**

Waaraan je het vaststelt: Aangetoond door wijzigingsverzoeken, notulen of tickets die de aanleiding, de impactbeoordeling, de goedkeuring en de uitvoering tonen. Typische aanleidingen in kleine organisaties: overstap naar een andere cloudleverancier, nieuwe locaties, de eerste aanwerving.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

7 Ondersteuning 15

7.1-1 **De middelen die nodig zijn voor de totstandkoming, implementatie, onderhoud en voortdurende verbetering van het ISMS worden bepaald en beschikbaar gesteld.**

Waaraan je het vaststelt: Een beveiligingsbudgetregel, toollicenties (wachtwoordbeheerder, MDM, logplatform), geplande persoonsdagen voor ISMS onderhoud en externe auditdiensten. Een factuur of een budgetgoedkeuring bewijst dit sneller dan enige tekst.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

7.2-1 **De benodigde competentie van de mensen wier werk van invloed is op de informatiebeveiligingsprestaties wordt bepaald.**

Waaraan je het vaststelt: Competentiematrix of rolprofielen met de per rol vereiste kennis, bijvoorbeeld secure development voor ontwikkelaars, incidentafhandeling voor de coordinator. In zeer kleine teams volstaat een regel per persoon.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

7.2-2 **Competentie wordt geborgd op basis van passende opleiding, training of ervaring.**

Waaraan je het vaststelt: Certificaten, cursusbevestigingen, cv's of gedocumenteerde praktijkervaring. Zelfstudie is aanvaardbaar mits aangetoond, bijvoorbeeld via afrondingsbewijzen van online cursussen of via geslaagde interne kennistoetsen.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

7.2-3 **Waar competentiehiaten bestaan, zijn acties ondernomen om deze te dichten en is de effectiviteit van die acties geevalueerd.**

Waaraan je het vaststelt: Opleidingsplan met een vergelijking van gepland versus werkelijk en een effectiviteitscheck, bijvoorbeeld een testscore, een click rate uit een phishingsimulatie of observatie op de werkvloer. De effectiviteitscheck wordt vaak vergeten en is een klassieke minor bevinding.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.2-4 **Passende gedocumenteerde informatie is beschikbaar als bewijs van competentie.** Document

Waaraan je het vaststelt: Een competentie of opleidingsmap per persoon met bewijs en data. In kleine organisaties volstaat een map met opgeslagen PDF bewijsstukken plus een overzichtstabel.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.3-1 **De mensen die binnen de reikwijdte werken zijn zich bewust van het informatiebeveiligingsbeleid.**

Waaraan je het vaststelt: Bevestiging bij onboarding en na elke wijziging van het beleid, met datum en versie. Een leesbevestigingsfunctie in de wiki of een ondertekende lijst volstaat.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.3-2 **Mensen kennen hun eigen bijdrage aan de effectiviteit van het ISMS en de voordelen van verbeterde informatiebeveiligingsprestaties.**

Waaraan je het vaststelt: Trainingsmateriaal en aanwezigheidslijsten waarin de link naar het eigen werk zichtbaar is. Auditors interviewen medewerkers rechtstreeks, train dus met concrete, alledaagse voorbeelden in plaats van abstracte citaten uit de norm.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.3-3 **Mensen kennen de gevolgen van het niet naleven van de ISMS eisen.**

Waaraan je het vaststelt: Vermeld de gevolgen in trainingsmateriaal en werkinstructies en koppel ze aan het proces onder A.6.4. Zelfs organisaties zonder werknemers moeten dit via hun contracten regelen voor zzp'ers en freelancers.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.4-1 **Interne en externe communicatie die relevant is voor het ISMS wordt bepaald: wat wordt gecommuniceerd, wanneer, met wie en via welke middelen.**

Waaraan je het vaststelt: Een communicatiematrix met regels zoals beveiligingsincident naar klanten, melding aan de toezichthouder binnen 72 uur, maandelijkse statusrapportage aan de directie. Dit is de basis van crisiscommunicatie en wordt na elk incident herzien.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.5.1-1 **Het ISMS omvat de door de norm vereiste gedocumenteerde informatie alsook de gedocumenteerde informatie die de organisatie noodzakelijk heeft bepaald voor de effectiviteit van het ISMS.** Document

Waaraan je het vaststelt: Een documentindex met elk ISMS document, doel, eigenaar, versie en opslaglocatie. Dit toont aan dat de verplichte documenten compleet zijn en is het snelste startpunt voor de auditor.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.5.2-1 **Bij het opstellen en bijwerken van documenten worden passende identificatie, formaat en media geborgd, en de documenten worden beoordeeld en goedgekeurd op geschiktheid.**

Waaraan je het vaststelt: Een uniforme documentkop met titel, versie, datum, auteur en goedkeurder. In Git gebaseerde omgevingen voldoen pull request beoordelingen met goedkeuring aan de beoordelings en goedkeuringseis, mits de historie onveranderlijk is.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.5.3-1 **Gedocumenteerde informatie is beschikbaar en geschikt voor gebruik waar en wanneer die nodig is.**

Waaraan je het vaststelt: Een centrale opslaglocatie die bereikbaar is voor iedereen die daartoe gerechtigd is, met een zoekfunctie. Testbaar via steekproef: een gegeven werkinstructie moet binnen een minuut vindbaar zijn.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.5.3-2 **Gedocumenteerde informatie is adequaat beschermd, in het bijzonder tegen verlies van vertrouwelijkheid, oneigenlijk gebruik en verlies van integriteit.**

Waaraan je het vaststelt: Rolgebaseerde toegangsrechten tot ISMS documenten, versiebeheer met historie, schrijfbeveiliging voor goedgekeurde versies en een back up van de documentopslag. Het bewijs van de back up wordt het vaakst vergeten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.5.3-3 **Distributie, toegang, terugvinden, opslag, wijzigingsbeheer alsook bewaartermijn en vernietiging van gedocumenteerde informatie zijn geregeld.**

Waaraan je het vaststelt: Een korte documentbeheerregel met bewaartermijnen en verwijderregels. Deze moet worden afgestemd met wettelijke verplichtingen (handelsrecht, fiscaal recht, AVG) en is de basis voor A.5.33 en A.8.10.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7.5.3-4 **Gedocumenteerde informatie van externe herkomst die nodig is voor het plannen en uitvoeren van het ISMS wordt geidentificeerd en beheerst.**

Waaraan je het vaststelt: Een lijst van externe documenten met versie en bron: normen, wetteksten, hardening richtlijnen van leveranciers, clouddocumentatie over beveiliging, verwerkersovereenkomsten. Zonder versievermelding kan beheersing niet worden aangetoond.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8 Uitvoering 8

8.1-1 **De processen die nodig zijn om aan de informatiebeveiligingseisen te voldoen en om de acties uit hoofdstuk 6 uit te voeren worden gepland, geimplementeerd en beheerst, en er worden criteria voor die processen vastgesteld.**

Waaraan je het vaststelt: Een operationeel handboek of runbooks met duidelijke criteria, bijvoorbeeld de maximale tijd om kritieke patches uit te rollen, releasecriteria voor deployments, alertdrempels. Criteria zonder getallen zijn waardeloos in de audit.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8.1-2 **Gedocumenteerde informatie is beschikbaar voor zover nodig om vertrouwen te hebben dat de processen zijn uitgevoerd zoals gepland.** Document

Waaraan je het vaststelt: Operationele registraties als bewijs: tickethistorie, CI pipeline runs, patchrapporten, back uplogs, toegangsbeoordelingen. Deze registraties zijn het daadwerkelijke effectiviteitsbewijs in de stage 2 audit.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8.1-3 **Geplande wijzigingen worden beheerst en de gevolgen van onbedoelde wijzigingen worden beoordeeld; waar nodig worden nadelige effecten beperkt.**

Waaraan je het vaststelt: Een wijzigingsproces met goedkeuring en een terugdraaipad, gekoppeld aan A.8.32. Documenteer bij onbedoelde wijzigingen (misconfiguratie, onbedoelde escalatie van rechten) het incident en toon de correctie aan.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8.1-4 **Extern geleverde processen, producten en diensten die relevant zijn voor het ISMS worden bepaald en beheerst.**

Waaraan je het vaststelt: Een leverancierslijst met kritikaliteit, contractverwijzing en de stand van het bewijs (het ISO 27001 certificaat van de leverancier, SOC 2 rapport, verwerkersovereenkomst). Voor kleine organisaties is dit de grootste hefboom, omdat het grootste deel van de IT toch extern draait.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8.2-1 **Risicobeoordelingen worden uitgevoerd met geplande tussenpozen en wanneer zich significante wijzigingen of incidenten voordoen, met inachtneming van de vastgestelde criteria.**

Waaraan je het vaststelt: Een ritme (doorgaans jaarlijks) plus vastgestelde triggers voor ongeplande beoordelingen. Aangetoond door gedateerde versies van het risicoregister en vermeldingen in de agenda of het ticketsysteem.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8.2-2 **De resultaten van de risicobeoordelingen worden bewaard als gedocumenteerde informatie.** Document

Waaraan je het vaststelt: Historische versies van het risicoregister met data, niet alleen de huidige stand. Overschrijven van het bestand maakt de ontwikkeling onbewijsbaar; versiebeheer in het bestandssysteem of in Git lost dit op.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8.3-1 **Het risicobehandelplan wordt uitgevoerd.**

Waaraan je het vaststelt: Vergelijk plan met werkelijkheid: afgeronde acties met een implementatiedatum en een concreet artefact (configuratie, beleid, contract). Openstaande acties vereisen een gedocumenteerde onderbouwing en een nieuwe streefdatum.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8.3-2 **De resultaten van de risicobehandeling worden bewaard als gedocumenteerde informatie.** Document

Waaraan je het vaststelt: Statusrapporten of afgesloten actiepunten met een verwijzing naar het bewijs. Het register alleen volstaat als elke regel een afrondingsdatum en een koppeling naar het bewijs bevat.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9 Prestatiebeoordeling 21

9.1-1 **Er wordt bepaald wat er bewaakt en gemeten moet worden, met inbegrip van de informatiebeveiligingsprocessen en beheersmaatregelen.**

Waaraan je het vaststelt: Een meetwaardenoverzicht met een beheersbaar aantal solide maatstaven: patchachterstand, MFA dekking, tijd om incidenten op te lossen, resultaat van de laatste restore test, openstaande bevindingen. Een paar meetwaarden die daadwerkelijk worden verzameld zijn beter dan een lange wensenlijst.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.1-2 **De methoden voor bewaking, meting, analyse en evaluatie zijn vastgesteld en leveren geldige resultaten op.**

Waaraan je het vaststelt: Documenteer voor elke meetwaarde de gegevensbron en de berekening, bijvoorbeeld een export uit de kwetsbaarhedenscanner of uit het identity provider rapport. Herleidbaarheid van de bron is de kern van geldigheid.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.1-3 **Er is vastgesteld wanneer en door wie bewaking en meting worden uitgevoerd en wanneer de resultaten worden geanalyseerd en geevalueerd.**

Waaraan je het vaststelt: Voeg kolommen voor frequentie en eigenaar toe aan het meetwaardenoverzicht. Een terugkerende agenda afspraak voor de evaluatie bewijst regelmaat beter dan welke beschrijving ook.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.1-4 **De resultaten van bewaking en meting worden bewaard als gedocumenteerde informatie.** Document

Waaraan je het vaststelt: Gearchiveerde evaluaties, geexporteerde dashboards of een meetwaardenoverzicht dat als tijdreeks wordt bijgehouden. Een live weergave zonder historie voldoet niet aan de eis.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.1-5 **De informatiebeveiligingsprestaties en de effectiviteit van het ISMS worden beoordeeld op basis van de meetresultaten.**

Waaraan je het vaststelt: Een geschreven evaluatie, niet alleen cijfers: trend, oorzaken, actiebehoefte. Deze evaluatietekst is tegelijk input voor de directiebeoordeling.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.2.1-1 **Interne audits worden uitgevoerd met geplande tussenpozen en leveren informatie op over de vraag of het ISMS voldoet aan de eigen eisen van de organisatie en aan de eisen van de norm en effectief is geimplementeerd.**

Waaraan je het vaststelt: Voor de certificatie audit moet ten minste een volledige interne auditcyclus die de gehele reikwijdte dekt zijn afgerond. Zonder dit is certificatie onbereikbaar; dit is een van de meest voorkomende struikelblokken bij eerste certificeringen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.2.2-1 **Een auditprogramma wordt gepland, vastgesteld en onderhouden; het definieert frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage, en het houdt rekening met het belang van de betrokken processen en de resultaten van eerdere audits.**

Waaraan je het vaststelt: Een meerjarig auditprogramma dat alle hoofdstukken en alle toepasselijke beheersmaatregelen over de certificatiecyclus dekt, met een hogere frequentie voor kritieke gebieden. Een eenvoudige tabel over drie jaar volstaat ruimschoots.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.2.2-2 **Auditcriteria en auditreikwijdte worden voor elke audit vastgesteld.**

Waaraan je het vaststelt: Een auditplan per datum met de criteria (de norm, interne beleidsdocumenten, contracten) en een duidelijke reikwijdte. Een auditplan van een pagina per audit volstaat en dient tevens als basis voor het rapport.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.2.2-3 **Auditors worden geselecteerd en audits worden uitgevoerd op een manier die objectiviteit en onpartijdigheid waarborgt. Niemand audit zijn eigen werk.**

Waaraan je het vaststelt: Onafhankelijkheid is hier de lastige horde: wie de beleidsdocumenten heeft geschreven en de systemen heeft geconfigureerd, mag ze niet auditen. In zeer kleine organisaties betekent dit vrijwel altijd een externe interne auditor, bijvoorbeeld een ingehuurde consultant of een collega van een partnerbedrijf; een auditovereenkomst plus de onafhankelijkheidsverklaring van de auditor vormen het bewijs. Alleen in voldoende grote teams kan de rol intern worden geroteerd naar iemand zonder verantwoordelijkheid voor het geauditeerde gebied, en dat moet dan blijken uit de rolmatrix.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.2.2-4 **De auditresultaten worden gerapporteerd aan de relevante directie.**

Waaraan je het vaststelt: Een auditrapport met bevindingen, afwijkingen, aanbevelingen en een verspreidingslijst, plus bewijs van overdracht aan de directie, bijvoorbeeld een genotuleerd agendapunt of een gedateerde e mail overdracht.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.2.2-5 **Gedocumenteerde informatie over het auditprogramma en de auditresultaten wordt bewaard.** Document

Waaraan je het vaststelt: Bewaar het auditprogramma, auditplannen, auditrapporten en de daaruit voortvloeiende acties op een plek. De koppeling van een bevinding naar een corrigerende actie (hoofdstuk 10.2) moet volledig zichtbaar zijn.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.1-1 **De directie beoordeelt het ISMS met geplande tussenpozen om de blijvende geschiktheid, toereikendheid en effectiviteit ervan te waarborgen.**

Waaraan je het vaststelt: Ten minste jaarlijks en ingepland voor de externe audit. Zelfs in zeer kleine organisaties moeten er gedateerde, ondertekende notulen zijn, ook als de directie en de ISMS eigenaar dezelfde persoon zijn.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.2-1 **De directiebeoordeling houdt rekening met de status van acties uit eerdere directiebeoordelingen.**

Waaraan je het vaststelt: De notulen beginnen met een opvolgtabel van de beslissingen van vorig jaar en hun huidige status. Zonder deze terugverwijzing telt de beoordeling als onvolledig.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.2-2 **De directiebeoordeling houdt rekening met veranderingen in de externe en interne kwesties die relevant zijn voor het ISMS, met inbegrip van relevante aspecten van klimaatverandering.**

Waaraan je het vaststelt: Een eigen agendapunt dat verwijst naar de bijgewerkte contextanalyse. Klimaatverandering wordt in de tekst van dit hoofdstuk niet expliciet genoemd (Amd 1:2024 wijzigt alleen 4.1 en 4.2), maar komt hier binnen via wijzigingen in de kwesties uit 4.1 en auditors verwachten het. Zelfs een uitkomst van niet relevant, ongewijzigd hoort in de notulen thuis.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.2-3 **De directiebeoordeling houdt rekening met veranderingen in de behoeften en verwachtingen van belanghebbenden die relevant zijn voor het ISMS.**

Waaraan je het vaststelt: Nieuwe klanteisen uit contracten en beveiligingsvragenlijsten, nieuwe wettelijke verplichtingen, eisen van de certificatie instelling. Leg ze vast als een lijst met bronnen in de notulen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.2-4 **De directiebeoordeling houdt rekening met feedback over informatiebeveiligingsprestaties, met inbegrip van afwijkingen en corrigerende acties, resultaten van bewaking en meting, auditresultaten en de mate waarin de informatiebeveiligingsdoelstellingen zijn behaald.**

Waaraan je het vaststelt: Behandel deze vier blokken als aparte agendapunten, anders ontbreekt er later een in de notulen. Voeg het meetwaardenoverzicht, het auditrapport en het doelstellingenoverzicht als bijlagen toe.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.2-5 **De directiebeoordeling houdt rekening met feedback van belanghebbenden.**

Waaraan je het vaststelt: Klantklachten met een beveiligingsaspect, resultaten van klantaudits, meldingen via het klokkenluiderskanaal, feedback van dienstverleners. Leg dit vast in de notulen, ook wanneer de bevinding is dat er geen zijn ontvangen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.2-6 **De directiebeoordeling houdt rekening met de resultaten van de risicobeoordeling en de status van het risicobehandelplan.**

Waaraan je het vaststelt: Voeg het actuele risicoregister en de implementatiestatus van het behandelplan toe, met expliciete bevestiging van restrisicoacceptatie door de risico eigenaren.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.2-7 **De directiebeoordeling houdt rekening met kansen voor voortdurende verbetering.**

Waaraan je het vaststelt: Een agendapunt met concrete verbeteridee en een besluit per idee. Geaccepteerde ideeen komen als vermeldingen met streefdata in het verbeterregister.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.3-1 **De resultaten van de directiebeoordeling omvatten besluiten over kansen voor voortdurende verbetering en over eventuele behoefte aan wijzigingen aan het ISMS.**

Waaraan je het vaststelt: De notulen eindigen met een besluitensectie: besluit, eigenaar, streefdatum. Notulen zonder besluiten zijn een bevinding in de audit, omdat het sturende effect dan ontbreekt.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9.3.3-2 **Gedocumenteerde informatie wordt bewaard als bewijs van de resultaten van de directiebeoordeling.** Document

Waaraan je het vaststelt: Ondertekende notulen met datum, deelnemers, input, evaluatie en besluiten. Het is een van de eerste documenten die een certificatie instelling in stage 1 opvraagt.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10 Verbetering 7

10.1-1 **De geschiktheid, toereikendheid en effectiviteit van het ISMS worden voortdurend verbeterd.**

Waaraan je het vaststelt: Een verbeterregister gevoed vanuit meerdere bronnen (audits, incidenten, ideeen, afwijkingen van meetwaarden) met zichtbare voortgang over de tijd. Continuiteit over meerdere maanden is het bewijs, niet het aantal vermeldingen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10.2-1 **Wanneer een afwijking optreedt, reageert de organisatie erop: zij beheerst en corrigeert deze en behandelt de gevolgen.**

Waaraan je het vaststelt: Een afwijkingsrapport met een directe actie en een datum. Bronnen zijn interne audits, externe audits, incidenten en waarnemingen uit de dagelijkse bedrijfsvoering; ze voeden allemaal hetzelfde register.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10.2-2 **Er wordt beoordeeld of actie nodig is om de oorzaken weg te nemen zodat de afwijking niet opnieuw of elders optreedt; dit omvat het controleren of soortgelijke afwijkingen bestaan of zouden kunnen optreden.**

Waaraan je het vaststelt: Documenteer de oorzaakanalyse, bijvoorbeeld met 5 keer waarom of Ishikawa, plus een expliciete uitspraak over overdraagbaarheid naar andere systemen of processen. De overdraagbaarheidsstap wordt het vaakst overgeslagen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10.2-3 **Eventuele noodzakelijke corrigerende acties worden uitgevoerd en de effectiviteit ervan wordt beoordeeld.**

Waaraan je het vaststelt: Leg per actie de implementatiedatum, het bewijsstuk en een latere effectiviteitsbeoordeling met eigen datum vast. Twee datumvelden per regel zijn de eenvoudigste manier om de effectiviteitsbeoordeling niet kwijt te raken.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10.2-4 **Waar nodig worden wijzigingen aan het ISMS aangebracht als gevolg van de afwijking.**

Waaraan je het vaststelt: Als een afwijking herleidbaar is tot een hiaat in een beleid, het risicoregister of de VvT, moet de wijziging daar zichtbaar worden. Een verwijzing van de afwijking naar de bijgewerkte documentversie sluit de keten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10.2-5 **Corrigerende acties zijn passend bij de gevolgen van de geconstateerde afwijkingen.**

Waaraan je het vaststelt: Een ernstclassificatie in het register waaruit de proportionaliteit van de actie blijkt. Geen bagatel behandeld als project en geen ernstige afwijking beantwoord met slechts een herinnerings e mail.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10.2-6 **Gedocumenteerde informatie wordt bewaard over de aard van de afwijkingen, de daarop genomen acties en de resultaten van de corrigerende acties.** Document

Waaraan je het vaststelt: Een register van afwijkingen en corrigerende acties met kolommen voor aard, oorzaak, actie, eigenaar, streefdatum en het resultaat van de effectiviteitsbeoordeling. Het is verplicht bewijs en wordt bij elke surveillance audit opgevraagd.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5 Bijlage A: Organisatorische beheersmaatregelen 37

A.5.1 **Beleid voor informatiebeveiliging: Een overkoepelend informatiebeveiligingsbeleid en onderwerpspecifieke beleidsdocumenten worden vastgesteld, door de directie goedgekeurd, gecommuniceerd en met geplande tussenpozen en bij significante wijzigingen beoordeeld.** Document

Waaraan je het vaststelt: Een beleidsset met versie, goedkeuringsdatum en volgende beoordelingsdatum, plus bewijs van kennisname. Voor kleine organisaties volstaan een kaderbeleid en een handvol onderwerpsbeleidsdocumenten (toegang, cryptografie, thuiswerken, incidenten).

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.2 **Rollen en verantwoordelijkheden voor informatiebeveiliging: Rollen en verantwoordelijkheden voor informatiebeveiliging worden vastgesteld en toegewezen naar de behoeften van de organisatie.**

Waaraan je het vaststelt: Een rolmatrix met namen, plaatsvervangers en taken. Vermeld in zeer kleine organisaties openlijk waar meerdere rollen bij een persoon samenkomen en koppel dit aan de compenserende maatregelen onder A.5.3.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.3 **Functiescheiding: Taken en verantwoordelijkheidsgebieden die elkaar zouden moeten controleren, liggen niet bij een enkele persoon. Het doel is dat niemand een wijziging alleen kan initieren, goedkeuren en verhullen.**

Waaraan je het vaststelt: In kleine organisaties is volledige functiescheiding structureel onmogelijk; een algemene bewering van conform stort in het auditinterview meteen in. Wat wel standhoudt is een eerlijke analyse: welke combinaties van taken kritiek zijn (ontwikkelen en uitrollen, rechten toekennen en gebruiken, betalingen initieren en goedkeuren), welke daarvan bij een persoon liggen, en welke compenserende maatregelen gelden. Beproefde aanpakken zijn onveranderlijke auditlogs die voor een derde toegankelijk zijn, MFA op geprivilegieerde accounts, geautomatiseerde CI gates en branch protection in plaats van vier ogen beoordeling, een periodieke logbeoordeling door een externe persoon, en aparte goedkeuring voor betalingen. Bewaar de analyse en de compenserende maatregelen als een eigen gedateerd document en koppel het vanuit de VvT.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.4 **Verantwoordelijkheden van de directie: De directie vereist van alle medewerkers dat zij informatiebeveiliging toepassen in lijn met het vastgestelde beleid en de procedures.**

Waaraan je het vaststelt: Een verplichting in arbeids en opdrachtovereenkomsten, kennisname van het beleid bij onboarding, en regelmatige herinneringen vanuit de directie. Bewijs: ondertekende verklaringen van verplichting en vergadernotulen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.5 **Contact met autoriteiten: Passende contacten met relevante autoriteiten worden onderhouden en zijn bereikbaar wanneer nodig.**

Waaraan je het vaststelt: Een contactlijst met de bevoegde toezichthouder gegevensbescherming, de politie of cybercrime eenheid, het nationale meldpunt cyberveiligheid en, waar van toepassing, NIS2 meldkanalen. Noteer de termijnen (zoals de 72 uur onder de AVG) direct in de lijst.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.6 **Contact met speciale belangengroepen: Contacten met speciale belangengroepen, beveiligingsforums en beroepsverenigingen worden onderhouden.**

Waaraan je het vaststelt: Lidmaatschappen, geabonneerde adviezen (nationaal CERT, leveranciersfeeds), deelname aan speciale belangengroepen. Eenvoudig bewijs: een lijst met abonnementen plus een voorbeeld waarbij een advies tot een actie heeft geleid.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.7 **Dreigingsinformatie: Informatie over informatiebeveiligingsdreigingen wordt verzameld en geanalyseerd om er passende acties uit af te leiden.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Werkbaar voor kleine organisaties: abonneer op nationale CERT adviezen en leveranciersadviezen, voer dan een korte maandelijkse beoordeling uit met een relevantiebesluit en daaruit voortvloeiende tickets. Het bewijs is de analyse, niet het abonnement.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.8 **Informatiebeveiliging in projectmanagement: Informatiebeveiliging wordt geintegreerd in projectmanagement, ongeacht het type project.**

Waaraan je het vaststelt: Beveiligingspunten in de projectchecklist: beschermingsbehoefte, risicobeoordeling, privacycheck, beveiligingsgoedkeuring voor go live. Veranker ze in agile teams als vaste punten in de definitie van gereed voor start en de definitie van klaar.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.9 **Inventaris van informatie en andere bijbehorende assets: Een inventaris van informatie en andere bijbehorende assets met met naam genoemde eigenaren wordt aangemaakt en onderhouden.**

Waaraan je het vaststelt: Een assetinventaris die hardware, software, clouddiensten, gegevensopslag, domeinen en accounts dekt, elk met een eigenaar en de beschermingsbehoefte ervan. In kleine organisaties kan deze automatisch worden samengesteld uit een MDM export, een licentielijst en de cloudconsole; een actuele datum is verplicht.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.10 **Aanvaardbaar gebruik van informatie en andere bijbehorende assets: Regels voor het aanvaardbaar gebruik en de omgang met informatie en andere bijbehorende assets worden vastgesteld, gedocumenteerd en geimplementeerd.** Document

Waaraan je het vaststelt: Een beleid voor aanvaardbaar gebruik voor apparaten, netwerken, cloudaccounts en AI tools, met kennisnamebevestiging. Persoonlijke apparaten en externe AI diensten moeten expliciet worden behandeld, want daar vindt het meeste datalek plaats.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.11 **Teruggave van assets: Wanneer een arbeidsrelatie eindigt of wijzigt, wordt geregeld en schriftelijk bevestigd dat alle uitgegeven apparaten, sleutels, accounts en documenten worden teruggegeven.**

Waaraan je het vaststelt: Een offboarding checklist met een ontvangstbevestiging voor laptop, tokens, sleutels, certificaten en opslagmedia, plus deactivering van accounts op dezelfde dag. Dit geldt evenzeer voor freelancers en stagiairs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.12 **Classificatie van informatie: Informatie wordt geclassificeerd naar beschermingsbehoefte op het gebied van vertrouwelijkheid, integriteit, beschikbaarheid en wettelijke eisen.**

Waaraan je het vaststelt: Een eenvoudig schema met drie of vier niveaus (openbaar, intern, vertrouwelijk, strikt vertrouwelijk) en concrete omgangsregels per niveau. Leg de toewijzing vast in de assetinventaris of in het verwerkingsregister.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.13 **Labelen van informatie: Het classificatieniveau is herkenbaar op het document, het bestand of het bericht zelf, zodat ontvangers weten hoe ermee om te gaan zonder te hoeven vragen.**

Waaraan je het vaststelt: Labeling in de documentkop, de bestandsnaam, het e mail onderwerp of via gevoeligheidslabels in de cloud kantoorsuite. Bewijs via steekproeven van daadwerkelijk gelabelde documenten, niet alleen via de regel.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.14 **Informatieoverdracht: Regels, procedures en overeenkomsten voor het overdragen van informatie binnen de organisatie en met externe partijen zijn aanwezig.**

Waaraan je het vaststelt: Een regel die vastlegt welk kanaal is toegestaan voor welk classificatieniveau: versleutelde e mail of een dataroom voor vertrouwelijke inhoud, geen verzending via privemessengers. Onderbouw vertrouwelijke overdrachten met geheimhoudingsovereenkomsten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.15 **Toegangsbeveiliging: Regels om fysieke en logische toegang tot informatie en andere bijbehorende assets te beheersen worden vastgesteld en geïmplementeerd op basis van bedrijfs en beveiligingseisen.**

Waaraan je het vaststelt: Een toegangsbeveiligingsbeleid volgens need to know en least privilege, met een koppeling van rol naar rechten. Bewijs via de daadwerkelijke rechtenconfiguratie in de identity provider, niet alleen via het beleid.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.16 **Identiteitsbeheer: De volledige levenscyclus van identiteiten wordt beheerd.**

Waaraan je het vaststelt: Een proces van aanmaak via wijziging tot deactivering, idealiter gecentraliseerd in een identity provider met single sign on. Geen gedeelde groepsaccounts; waar technisch onvermijdelijk, benoem het account, onderbouw het en log het gebruik ervan.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.17 **Authenticatie informatie: De toewijzing en het beheer van authenticatie informatie worden beheerst door een beheerproces dat mensen verplicht deze correct te behandelen.**

Waaraan je het vaststelt: Een wachtwoordbeheerder als verplicht hulpmiddel, een beleid voor wachtwoordkwaliteit en MFA, veilige initiele toegang en een resetprocedure met identiteitsverificatie. Bewijs via configuratieschermafbeeldingen en het rapport van de wachtwoordbeheerder.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.18 **Toegangsrechten: Toegangsrechten worden toegekend, beoordeeld, gewijzigd en ingetrokken in overeenstemming met het toegangsbeveiligingsbeleid.**

Waaraan je het vaststelt: Een periodieke toegangsbeoordeling, ten minste jaarlijks, met een gedocumenteerd resultaat per account en bewijs van ingetrokken rechten. Intrekking op de dag van vertrek is een punt dat auditors graag aan de hand van een concreet geval natrekken.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.19 **Informatiebeveiliging in leveranciersrelaties: Processen en procedures worden vastgesteld en geïmplementeerd om de beveiligingsrisico's te beheersen die voortvloeien uit het gebruik van producten en diensten van derden.**

Waaraan je het vaststelt: Een leverancierslijst met een kritikaliteitsniveau en de diepgang van de beoordeling. Verkrijg voor kritieke leveranciers bewijs (ISO 27001 certificaat, SOC 2 rapport) in plaats van zelf audits uit te voeren, wat voor kleine organisaties de enige realistische route is.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.20 **Informatiebeveiliging opnemen in leveranciersovereenkomsten: Relevante beveiligingseisen worden met elke leverancier overeengekomen en in de contracten vastgelegd.**

Waaraan je het vaststelt: Een contractbijlage informatiebeveiliging met meldplicht bij incidenten, regels voor subverwerkers, verwijderverplichtingen en auditrechten. Voor standaarddiensten volstaan de voorwaarden van de leverancier plus een verwerkersovereenkomst, mits de inhoud ervan is beoordeeld en gedocumenteerd.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.21 **Beheersen van informatiebeveiliging in de ICT toeleveringsketen: Processen om de beveiligingsrisico's in de toeleveringsketen voor informatie en communicatietechnologie te beheersen worden vastgesteld en geïmplementeerd.**

Waaraan je het vaststelt: Dit betreft softwareafhankelijkheden en de eigen subleveranciers van leveranciers. In de praktijk: een software bill of materials (SBOM) of afhankelijkheidslijst, geautomatiseerde controles op kwetsbare pakketten in CI, en software alleen betrekken via ondertekende of officiele kanalen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.22 **Bewaking, beoordeling en wijzigingsbeheer van leveranciersdiensten: Wijzigingen in leveranciersdiensten worden regelmatig bewaakt, beoordeeld en beheerd.**

Waaraan je het vaststelt: Een jaarlijkse leveranciersbeoordeling die incidenten, beschikbaarheidsrapporten en certificaatgeldigheid bekijkt, plus een kanaal voor wijzigingsaankondigingen van de leverancier. Leg het resultaat vast als een korte notitie per leverancier.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.23 **Informatiebeveiliging voor gebruik van clouddiensten: Processen voor het verwerven, gebruiken, beheren en beeindigen van clouddiensten worden vastgesteld in lijn met de beveiligingseisen.**

Waaraan je het vaststelt: Nieuw in de editie van 2022 en de centrale beheersmaatregel voor kleine cloudgebaseerde organisaties. Bewijs via een cloudbeleid met een goedkeuringsproces voor nieuwe diensten, een gedocumenteerd model van gedeelde verantwoordelijkheid per dienst, hardeningsinstellingen, en een exitstrategie inclusief teruggave van gegevens en bevestiging van verwijdering.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.24 **Planning en voorbereiding van informatiebeveiligingsincidentbeheer: Processen, rollen en verantwoordelijkheden voor incidentafhandeling worden gepland en vastgesteld.** Document

Waaraan je het vaststelt: Een incident response plan met het meldpad, rollen, escalatieniveaus, contacten buiten kantooruren en communicatiesjablonen. Realistisch voor kleine teams: een pagina, maar geoefend.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.25 **Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen: Beveiligingsgebeurtenissen worden beoordeeld en er wordt een besluit genomen of zij geclassificeerd moeten worden als informatiebeveiligingsincidenten.**

Waaraan je het vaststelt: Triagecriteria met een ernstmatrix en een gebeurtenisregister waarin ook afgewezen gebeurtenissen met een onderbouwing verschijnen. De scheiding tussen gebeurtenis en incident moet zichtbaar zijn in het register.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.26 **Reactie op informatiebeveiligingsincidenten: Incidenten worden afgehandeld in overeenstemming met de gedocumenteerde procedures.**

Waaraan je het vaststelt: Incidentdossiers met een tijdlijn, de genomen acties, de betrokken personen en het afsluitbesluit. Als er nog geen echt incident is geweest, is een gedocumenteerde tabletop oefening het beste beschikbare bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.27 **Leren van informatiebeveiligingsincidenten: Kennis opgedaan uit incidenten wordt gebruikt om de beveiligingsmaatregelen te versterken.**

Waaraan je het vaststelt: Een blaamvrije post incident review met oorzaakanalyse en daaruit voortvloeiende acties, gekoppeld aan het verbeterregister en, waar nodig, aan het risicoregister.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.28 **Verzamelen van bewijs: Er wordt geregeld hoe sporen die verband houden met een beveiligingsgebeurtenis worden geidentificeerd, veiliggesteld en bewaard zodat ze later nog bruikbaar zijn.**

Waaraan je het vaststelt: Een korte procedure voor bewijsbehoud: systemen niet voortijdig heropbouwen, images en logs veiligstellen, de bewaarketen documenteren. Voor kleine organisaties volstaat het om het ernstniveau te definieren waarvanaf een externe forensisch dienstverlener wordt ingeschakeld, samen met de contactgegevens.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.29 **Informatiebeveiliging tijdens verstoring: De organisatie plant hoe informatiebeveiliging op een passend niveau wordt gehandhaafd tijdens een verstoring.**

Waaraan je het vaststelt: Noodmaatregelen mogen beveiliging niet uitschakelen. Documenteer dat MFA, logging en toegangsbeperkingen ook gelden in noodbedrijf, en dat noodaccounts (break glass accounts) verzegeld, gedocumenteerd en achteraf beoordeeld zijn.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.30 **ICT gereedheid voor bedrijfscontinuiteit: ICT gereedheid wordt gepland, geimplementeerd, onderhouden en getest op basis van bedrijfscontinuiteitsdoelstellingen en ICT continuiteitseisen.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Bewijs via vastgestelde recovery time objectives (RTO) en recovery point objectives (RPO) per kritiek systeem, een herstelprocedure en ten minste een gedocumenteerde test per jaar. Een geslaagde restore test met datum en duur is hier het sterkste enkele bewijsstuk.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.31 **Wettelijke, statutaire, regelgevende en contractuele eisen: De relevante eisen en de aanpak om eraan te voldoen worden geidentificeerd, gedocumenteerd en actueel gehouden.** Document

Waaraan je het vaststelt: Een wettelijk register dat de AVG, telecommunicatierecht, handels en fiscaal recht, en waar van toepassing NIS2 of sectorspecifieke regels dekt, elk met de regel die eraan uitvoering geeft en de beoordelingsdatum. Een jaarlijkse beoordeling volstaat, maar moet gedateerd zijn.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.32 **Intellectuele eigendomsrechten: Passende procedures om intellectuele eigendomsrechten te beschermen worden geimplementeerd.**

Waaraan je het vaststelt: Een licentie inventaris voor de gebruikte software, een controle van open source licenties in het product (een licentiescanner in CI) en een regel voor de omgang met code van derden en gegenereerde code. Bewijs: het licentierapport uit de build.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.33 **Bescherming van registraties: Bedrijfs en bewijsregistraties worden zo opgeslagen dat ze niet verloren kunnen gaan, niet ongemerkt kunnen worden gewijzigd en niet in verkeerde handen kunnen vallen, en dit geldt voor de hele bewaartermijn.**

Waaraan je het vaststelt: Een bewaarschema met de wettelijke termijnen, manipulatiebestendige opslag, beperkte toegang en back up. Noem voor fiscaal relevante registraties de wettelijke bewaartermijnen expliciet, omdat auditors dat graag specifiek controleren.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.34 **Privacy en bescherming van persoonsgegevens: De eisen voor privacy en de bescherming van persoonlijk identificeerbare informatie (PII) worden geidentificeerd en nageleefd in lijn met de toepasselijke wetgeving.**

Waaraan je het vaststelt: Verwerkingsregister, verwerkersovereenkomsten, een verwijderconcept, een proces voor rechten van betrokkenen en, waar vereist, een gegevensbeschermingseffectbeoordeling. Koppeling hiervan aan het ISMS via een gedeelde assetlijst voorkomt dubbel onderhoud.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.35 **Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie voor het beheren van informatiebeveiliging wordt onafhankelijk beoordeeld met geplande tussenpozen en bij significante wijzigingen.**

Waaraan je het vaststelt: Aangetoond door de interne audit uitgevoerd door een onafhankelijke auditor, door externe penetratietests of door de certificatie audit zelf. Onafhankelijk betekent niet uitgevoerd door de persoon die verantwoordelijk is voor het beoordeelde gebied.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.36 **Naleving van beleid, regels en normen voor informatiebeveiliging: Naleving van het eigen beveiligingsbeleid van de organisatie en de toepasselijke regels wordt regelmatig beoordeeld.**

Waaraan je het vaststelt: Nalevingscontroles met datum en resultaat, bijvoorbeeld een configuratiecontrole tegen de eigen hardeningsbaseline, steekproeven van documentlabeling, geautomatiseerde beleidscontroles in de cloud. Afwijkingen voeden het register van corrigerende acties.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.5.37 **Gedocumenteerde bedrijfsprocedures: Bedrijfsprocedures voor informatieverwerkende voorzieningen worden gedocumenteerd en beschikbaar gesteld aan de mensen die ze nodig hebben.** Document

Waaraan je het vaststelt: Runbooks voor back up en herstel, deployment, gebruikersbeheer, patchen en incidentafhandeling. Kort en actueel is beter dan uitgebreid en verouderd; een laatst gewijzigd datum per runbook is verplicht.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6 Bijlage A: Beheersmaatregelen voor personeel 8

A.6.1 **Screening: Kandidaten die voor de organisatie gaan werken worden vooraf gescreend, binnen de grenzen van de wet en in verhouding tot de beschermingsbehoefte; voor gevoelige rollen wordt de screening tijdens het dienstverband herhaald.**

Waaraan je het vaststelt: Zonder werknemers kan deze maatregel worden onderbouwd als momenteel niet van toepassing, maar de procedure voor het geval van aanwerving moet toch worden vastgesteld en als gepland worden vastgelegd in de Verklaring van Toepasselijkheid. Een werkbare reikwijdte: verificatie van identiteit, cv en referenties, plus diploma's; een verklaring omtrent gedrag alleen waar de beschermingsbehoefte dat rechtvaardigt en de wet dit toestaat. Eis dezelfde standaard van freelancers en opdrachtnemers via hun contracten, anders ontstaat het gat precies daar.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6.2 **Arbeidsvoorwaarden: De contractuele afspraken vermelden de informatiebeveiligingsverantwoordelijkheden van het personeel en van de organisatie.**

Waaraan je het vaststelt: Een beveiligingsbepaling in de arbeids of opdrachtovereenkomst die verwijst naar het toepasselijke beleid. Voor freelancers dezelfde bepaling in de opdrachtovereenkomst, plus een geheimhoudingsovereenkomst.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6.3 **Bewustzijn, opleiding en training op het gebied van informatiebeveiliging: Personeel en relevante externe partijen ontvangen passend bewustzijn en training alsmede regelmatige updates over het beleid van de organisatie.**

Waaraan je het vaststelt: Jaarlijkse training met aanwezigheidsbewijs en een datum, aangevuld met phishingsimulaties met een geevalueerde click rate. Ook solozelfstandigen hebben bewijs van hun eigen bijscholing nodig, bijvoorbeeld cursusbevestigingen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6.4 **Disciplinair proces: Er bestaat een formeel en gecommuniceerd proces voor het optreden tegen mensen die het beveiligingsbeleid hebben overtreden.**

Waaraan je het vaststelt: Zonder werknemers kan dit worden onderbouwd als momenteel niet van toepassing, maar het proces moet toch worden vastgesteld voor het geval van aanwerving; alleen de toepassing vervalt, niet de regel. Vereist is een gefaseerde, gecommuniceerde reeks van reacties (gesprek, berisping, formele waarschuwing, ontslag) in lijn met arbeidsrecht en medezeggenschapsregels. Weerspiegel het sanctieniveau voor opdrachtnemers in het contract, bijvoorbeeld een contractuele boete of een opzegrecht.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6.5 **Verantwoordelijkheden na beeindiging of wijziging van het dienstverband: Beveiligingsverantwoordelijkheden en plichten die geldig blijven na beeindiging of een rolwijziging worden vastgesteld, gehandhaafd en gecommuniceerd aan de betrokken mensen.**

Waaraan je het vaststelt: Een offboarding checklist met intrekking van rechten, teruggave van assets, overdracht, en een expliciete herinnering aan de voortdurende geheimhoudingsverplichtingen. Een ondertekend exitgesprek verslag is het eenvoudigste bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6.6 **Geheimhoudingsovereenkomsten: Er wordt bepaald wie een geheimhoudingsovereenkomst moet ondertekenen. De inhoud sluit aan bij de beschermingsbehoefte van de informatie, de overeenkomsten worden ondertekend, gearchiveerd en regelmatig beoordeeld om ze actueel te houden.**

Waaraan je het vaststelt: Ondertekende geheimhoudingsovereenkomsten voor medewerkers, freelancers, dienstverleners en stagiairs, met een nawerkingsperiode. Een overzichtstabel met wederpartij, datum en geldigheid maakt de portefeuille auditeerbaar.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6.7 **Thuiswerken: Beveiligingsmaatregelen worden geimplementeerd waar mensen buiten de bedrijfslocaties werken en daarbij toegang hebben tot informatie van de organisatie.**

Waaraan je het vaststelt: Een thuiswerk en op afstand werken beleid met eisen aan schijfversleuteling, schermvergrendeling, veilig wifi, gebruik van VPN of zero trust toegang, privacyschermen en een verbod op het gebruik van persoonlijke apparaten zonder goedkeuring. Bewijs via het MDM nalevingsrapport voor de endpoints.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.6.8 **Melden van informatiebeveiligingsgebeurtenissen: Er bestaat een mechanisme waarmee mensen tijdig waargenomen of vermoede beveiligingsgebeurtenissen kunnen melden.**

Waaraan je het vaststelt: Een duidelijk gecommuniceerd meldkanaal (mailbox, chatkanaal, telefoonnummer) met de garantie van geen sancties voor te goeder trouw gedane meldingen. Bewijs: het aantal meldingen in het gebeurtenisregister; een permanent leeg register is een waarschuwingssignaal in de audit.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7 Bijlage A: Fysieke beheersmaatregelen 14

A.7.1 **Fysieke beveiligingszones: Beveiligingszones worden vastgesteld en gebruikt om gebieden te beschermen die informatie en informatieverwerkende voorzieningen bevatten.**

Waaraan je het vaststelt: Een beschrijving van de zones met een schets of foto's: gebouw, kantoor, serverkast. In een thuiskantoor is de zone de afsluitbare werkruimte of, bij gebrek daaraan, een afsluitbare kast; beschrijf dit in plaats van het weg te laten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.2 **Fysieke toegang: Beveiligde gebieden worden beschermd door passende toegangscontroles en toegangspunten.**

Waaraan je het vaststelt: Een sleutel of badge register met uitgifte en teruggave, en een bezoekersregel met begeleiding en een log. Bij gebruik van een coworking ruimte of een datacenter, neem de toegangscontroles van de exploitant als bewijs en leg ze contractueel vast.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.3 **Beveiligen van kantoren, ruimtes en faciliteiten: Fysieke beveiliging voor kantoren, ruimtes en faciliteiten wordt ontworpen en geimplementeerd.**

Waaraan je het vaststelt: Afsluitbare deuren, raambeveiliging op de begane grond, geen vertrouwelijke schermen van buitenaf zichtbaar, geen bedrijfsbord op gevoelige ruimtes. Een korte beschrijving plus een foto volstaat als bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.4 **Fysieke beveiligingsbewaking: Bedrijfsterreinen worden continu bewaakt op ongeautoriseerde fysieke toegang.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Opties zijn een alarmsysteem, bewegingsmelders, cameratoezicht of toegangslogs. Cameratoezicht moet op naleving van privacywetgeving worden gecontroleerd; in een thuiskantoor is het onderbouwde alternatief een combinatie van een alarmsysteem, een afgesloten ruimte en de bevinding dat daar geen gevoelige servers staan.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.5 **Bescherming tegen fysieke en omgevingsdreigingen: Bescherming is aanwezig tegen fysieke en omgevingsdreigingen zoals natuurrampen en opzettelijke of onopzettelijke schade.**

Waaraan je het vaststelt: Een beoordeling van brand, water, hitte, stroomuitval en inbraak, samen met de aanwezige maatregelen (rookmelders, brandblussers, geen apparatuur onder waterleidingen, back up op een andere locatie opgeslagen). Hier sluit de klimaatveranderingsvaststelling uit 4.1 op aan.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.6 **Werken in beveiligde gebieden: Maatregelen voor het werken in beveiligde gebieden worden ontworpen en geimplementeerd.**

Waaraan je het vaststelt: Regels voor de serverruimte of gebieden met hoge vertrouwelijkheid: geen onbegeleide toegang van derden, geen opnames met camera's of mobiele apparaten, logging van de uitgevoerde werkzaamheden. Zonder beveiligde gebieden kan dit worden onderbouwd door te verwijzen naar cloud only bedrijfsvoering.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.7 **Clean desk en clean screen: Regels voor een opgeruimd bureau met betrekking tot papieren en verwijderbare media en voor vergrendelde schermen worden vastgesteld en nageleefd.**

Waaraan je het vaststelt: Dit geldt volledig ook in het thuiskantoor en mag daarom niet als niet van toepassing worden verklaard. Aangetoond door een korte regel (documenten wegsluiten, schermvergrendeling na vijf minuten, geen plaknotities met inloggegevens) plus de technisch afgedwongen vergrendeling via apparaatbeleid, waarvan de configuratie geexporteerd kan worden.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.8 **Plaatsing en bescherming van apparatuur: Apparatuur wordt veilig geplaatst en beschermd.**

Waaraan je het vaststelt: Plaatsing weg van doorgangsroutes en publieke gebieden, geen zicht van buitenaf, bescherming tegen hitte en vocht, kabelsloten voor mobiele apparaten. Een korte beschrijving binnen het thuiskantoor of kantoorbeleid volstaat.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.9 **Beveiliging van assets buiten de bedrijfslocatie: Assets die zich buiten de bedrijfslocatie bevinden worden beschermd.**

Waaraan je het vaststelt: In kleine organisaties gaat het vooral om de laptop, de smartphone en externe media, en dit kan niet worden weggeredeneerd. Bewijs: afgedwongen schijfversleuteling, remote wipe ingeschakeld via MDM, een regel tegen het achterlaten van apparaten in voertuigen en tegen het gebruik van openbare netwerken zonder VPN, plus een meldpad voor verlies. Het MDM nalevingsrapport met de versleutelingsstatus per apparaat is het meest solide enkele bewijsstuk.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.7.10 **Opslagmedia: Opslagmedia worden over hun volledige levenscyclus beheerd in lijn met het classificatieschema en de omgangseisen, van aanschaf via gebruik en transport tot afvoer.**

Waaraan je het vaststelt: Dit geldt zelfs bij puur mobiel werken, omdat usb sticks, externe schijven en back upmedia bestaan. Bewijs: een mediaregister, versleutelde media, een technisch afgedwongen verbod op niet goedgekeurde verwijderbare media, veilige opslag op een afsluitbare plek, en overdracht naar A.7.14 aan het einde van de levensduur.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

A.7.11 **Ondersteunende voorzieningen: Informatieverwerkende voorzieningen worden beschermd tegen uitval van de ondersteunende voorzieningen, in het bijzonder de stroomvoorziening.**

Waaraan je het vaststelt: Waar servers in eigen beheer draaien, een noodstroomvoorziening met een gedocumenteerde test. In een cloud only opzet is het bewijs de verwijzing naar de toezeggingen van de leverancier plus een regel over het doorwerken tijdens een lokale stroom of internetstoring (mobiel tetheren, uitwijklocatie).

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

A.7.12 **Beveiliging van bekabeling: Stroom, data en communicatiebekabeling worden beschermd tegen afluisteren, storing en schade.**

Waaraan je het vaststelt: Waar u eigenaar bent van de bekabeling, bescherming tegen schade en tegen ongeautoriseerde toegang tot patchpanelen. In kleine kantoren en thuiskantoren is de onderbouwing beperkt, maar moet wel worden gegeven: router en netwerkaansluitingen zijn niet publiek toegankelijk, ongebruikte poorten zijn uitgeschakeld.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

A.7.13 **Onderhoud van apparatuur: Apparatuur wordt correct onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen.**

Waaraan je het vaststelt: Een onderhoudsplan of leveranciersondersteuningsstatus per apparaat, en een regel voor reparaties door derden (eerst de opslag verwijderen of de gegevens wissen, en een geheimhoudingsovereenkomst afsluiten met de dienstverlener). Volg einddatums van ondersteuning in de assetinventaris.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

A.7.14 **Veilige verwijdering of hergebruik van apparatuur: Voordat een apparaat met opslag wordt doorgegeven, verkocht of afgevoerd, wordt geverifieerd en vastgelegd dat er geen beschermde gegevens en geen gelicentieerde software meer op te reconstrueren zijn.**

Waaraan je het vaststelt: Dit geldt ook in het thuiskantoor en voor uitgefaseerde persoonlijke apparaten die voor werk werden gebruikt. Bewijs: een wisregistratie per apparaat met serienummer, datum en methode (crypto erase op versleutelde SSD's, overschrijven, fysieke vernietiging), of een vernietigingscertificaat van een dienstverlener. Voor versleutelde apparaten volstaat de gedocumenteerde vernietiging van de sleutel, mits de procedure is beschreven.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

A.8 Bijlage A: Technologische beheersmaatregelen 34

A.8.1 **Eindpuntapparaten van gebruikers: Informatie die is opgeslagen op, verwerkt door of toegankelijk via eindpuntapparaten van gebruikers wordt beschermd.**

Waaraan je het vaststelt: Een hardeningsbaseline per besturingssysteem, centraal beheer via MDM, schijfversleuteling, automatische updates en schermvergrendeling. Het MDM nalevingsrapport met een status per apparaat toont dit allemaal in een keer aan.

○ Open ○ In behandeling ○ Voldaan ○ Niet van toepassing

Bewijs / onderbouwing

A.8.2 **Geprivilegieerde toegangsrechten: De toewijzing en het gebruik van geprivilegieerde toegangsrechten worden beperkt en beheerd.**

Waaraan je het vaststelt: Een lijst van alle beheerdersaccounts met een onderbouwing, aparte beheerdersaccounts die niet voor dagelijks werk worden gebruikt, afgedwongen MFA, tijdelijk verhoogde rechten waar mogelijk, en periodieke beoordeling. In kleine organisaties is dit de belangrijkste compenserende maatregel voor A.5.3.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.3 **Beperking van toegang tot informatie: Toegang tot informatie en andere bijbehorende assets wordt beperkt in overeenstemming met het vastgestelde toegangsbeveiligingsbeleid.**

Waaraan je het vaststelt: Een autorisatieconcept op basis van rollen en groepen in plaats van individuele toekenningen, aangetoond door een export van groepslidmaatschappen. Beoordeel openbare deellinks in cloudopslag regelmatig en laat ze verlopen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.4 **Toegang tot broncode: Lees en schrijftoegang tot broncode, ontwikkeltools en softwarebibliotheken wordt passend beheerd.**

Waaraan je het vaststelt: Repository rechten per rol, beveiligde hoofdbranches, afgedwongen beoordelingen of afgedwongen statuscontroles, geen directe push naar main. Bewijs via de branch protection configuratie en de ledenlijst van de organisatie.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.5 **Veilige authenticatie: Veilige authenticatietechnologieen en procedures worden geimplementeerd op basis van de toegangsbeperkingen en het onderwerpspecifieke beleid.**

Waaraan je het vaststelt: MFA voor alle externe toegang en alle beheerdersaccounts, phishingbestendige methoden (passkeys, FIDO2) waar mogelijk, en uitsluiting na mislukte pogingen. Bewijs via het MFA dekkingsrapport van de identity provider.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.6 **Capaciteitsbeheer: Opslag, rekenkracht, bandbreedte en licenties worden bewaakt, en de vraag wordt tijdig bijgesteld zodat knelpunten de beschikbaarheid nooit bedreigen.**

Waaraan je het vaststelt: Bewaking van opslag, rekenbelasting, licentiequota en cloudbudgetten met drempelwaarschuwingen. In kleine organisaties volstaat een waarschuwing bij schijfgebruik en bij kostenlimieten plus een jaarlijkse capaciteitscheck.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.7 **Bescherming tegen malware: Technische verdedigingsmaatregelen tegen malware zijn actief en actueel, en de mensen die de apparaten gebruiken zijn goed genoeg getraind om die verdediging niet te ondermijnen.**

Waaraan je het vaststelt: Actieve endpointbeveiliging met een centraal statusoverzicht, een mailfilter dat bijlagen en links controleert, en een regel tegen het uitvoeren van niet goedgekeurde software. Het gedateerde statusrapport van de beveiligingsoplossing is het directe bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.8 **Beheer van technische kwetsbaarheden: De organisatie brengt actief kwetsbaarheden in de gebruikte technologie in kaart, bepaalt per bevinding hoezeer zij daaraan blootstaat, en dicht het gat binnen vastgestelde termijnen of onderbouwt een andere aanpak.**

Waaraan je het vaststelt: Kwetsbaarhedenbeheer met een bron (scanner, afhankelijkheidscontrole in CI, leveranciersadviezen), een ernstclassificatie en vastgestelde termijnen per niveau, bijvoorbeeld kritiek binnen 7 dagen. Bewijs: scanrapporten uit meerdere periodes die de afname van openstaande bevindingen tonen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.9 **Configuratiebeheer: Configuraties van hardware, software, diensten en netwerken, met inbegrip van beveiligingsconfiguraties, worden vastgesteld, gedocumenteerd, geimplementeerd, bewaakt en beoordeeld.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Bewijs via gedocumenteerde baseline configuraties (hardeningsbaselines) en de handhaving ervan, idealiter als infrastructure as code in versiebeheer of via MDM profielen. Drift detectie en een periodieke configuratievergelijking maken het compleet.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.10 **Verwijderen van informatie: Informatie die is opgeslagen in informatiesystemen, op apparaten en op opslagmedia wordt verwijderd zodra deze niet langer nodig is.**

Waaraan je het vaststelt: Nieuw in de editie van 2022 en nauw verbonden met de AVG. Bewijs via een verwijderconcept met bewaartermijnen per gegevenscategorie, technisch geimplementeerd bewaarbeleid in clouddiensten en databases, en verwijderlogs. Ook back ups en logarchieven hebben een bewaartermijn nodig.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.11 **Gegevensmaskering: Gegevensmaskering wordt toegepast in overeenstemming met het onderwerpspecifieke beleid voor toegangsbeveiliging en met de bedrijfs en wettelijke eisen.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. In de praktijk: geen productiegegevens in test en ontwikkelomgevingen, maar geanonimiseerde of synthetische gegevens in plaats daarvan; pseudonimisering in analytics; maskering van rekeningnummers en inloggegevens in logs en supportinterfaces. Bewijs via het script of de procedure die de testgegevens genereert.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.12 **Voorkomen van gegevenslekkage: Maatregelen ter voorkoming van gegevenslekkage worden toegepast op systemen, netwerken en apparaten die gevoelige informatie verwerken, opslaan of overdragen.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Realistisch in kleine organisaties: beheersing van deellinks in cloudopslag, blokkering van niet goedgekeurde verwijderbare media, regels tegen doorsturen naar privemailboxen, controle op het invoeren van vertrouwelijke gegevens in externe AI diensten, en secret scanning in broncode. Bewijs via de configuratie en via beoordelingen van de treffers.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.13 **Back up van informatie: Back ups van gegevens, software en systemen bestaan volgens een vastgestelde regel (omvang, frequentie, bewaartermijn, locatie), en het herstellen ervan wordt daadwerkelijk regelmatig getest.**

Waaraan je het vaststelt: Een back upbeleid met frequentie, bewaartermijn en een offsite kopie volgens het 3 2 1 principe, versleuteling van de back ups, en bescherming tegen overschrijving door ransomware (onveranderlijke back ups). Doorslaggevend is de gedocumenteerde restore test met datum en resultaat, want een ongeteste back up telt in de audit als niet bestaand.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.14 **Redundantie van informatieverwerkende voorzieningen: Informatieverwerkende voorzieningen worden geimplementeerd met voldoende redundantie om aan de beschikbaarheidseisen te voldoen.**

Waaraan je het vaststelt: Redundantie moet aansluiten bij de beschikbaarheidsdoelstellingen, niet bij het maximaal haalbare. Bewijs via een architectuurbeschrijving met redundante instanties of zones, reserveapparatuur, en een onderbouwd besluit over waar redundantie bewust ontbreekt.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.15 **Logging: Beveiligingsrelevante activiteiten laten een spoor achter. Logs worden aangemaakt, bewaard, beschermd tegen wijziging en daadwerkelijk geanalyseerd, niet alleen verzameld.**

Waaraan je het vaststelt: Log ten minste aanmeldingen en mislukte pogingen, rechtenwijzigingen, beheerhandelingen en toegang tot vertrouwelijke gegevens. De logs zijn beschermd tegen wijziging en hebben een vastgestelde bewaartermijn; in kleine organisaties vormen onveranderlijke logs tegelijk de compensatie voor de ontbrekende functiescheiding onder A.5.3.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.16 **Bewakingsactiviteiten: Netwerken, systemen en applicaties worden bewaakt op afwijkend gedrag en er worden passende maatregelen genomen om mogelijke beveiligingsincidenten te beoordelen.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Werkbaar zonder eigen beveiligingsteam: identity provider waarschuwingen bij onmogelijke reizen en bij reeksen mislukte pogingen, cloudplatform waarschuwingen bij ongebruikelijke uitgaven of rechtenwijzigingen, doorgestuurd naar een bewaakte mailbox met een vastgestelde reactietijd. Bewijs via de waarschuwingsregels plus voorbeelden van afgehandelde waarschuwingen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.17 **Kloksynchronisatie: Alle systemen die logs schrijven ontlenen hun tijd aan een vastgestelde, betrouwbare bron, zodat gebeurtenissen over systemen heen in de juiste volgorde kunnen worden gezet.**

Waaraan je het vaststelt: NTP configuratie op servers en endpoints, en een uniforme tijdzone in de logs (idealiter UTC). Zonder gesynchroniseerde tijd houdt de reconstructie van een incident onder A.5.28 geen stand; een configuratie export volstaat als bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.18 **Gebruik van geprivilegieerde hulpprogramma's: Het gebruik van hulpprogramma's die systeembeveiligingen kunnen omzeilen wordt beperkt en strikt beheerst.**

Waaraan je het vaststelt: Een lijst van goedgekeurde beheertools, beperking van lokale beheerdersrechten, applicatiecontrole (allowlisting) waar mogelijk, en logging van het gebruik. Bewijs: het beleid plus de configuratie van het rechtenbeheer.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.19 **Installatie van software op operationele systemen: Procedures en maatregelen voor het veilig beheren van softwareinstallatie op operationele systemen worden geimplementeerd.**

Waaraan je het vaststelt: Alleen goedgekeurde software uit vertrouwde bronnen, installatie via centrale distributie of een pakketbeheerder, een terugdraaipad en bewaring van de vorige versie. Bewijs via de goedkeuringslijst en deploymentlogs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.20 **Netwerkbeveiliging: Netwerken en actieve netwerkapparaten hebben een met naam genoemde eigenaar, een geharde configuratie en een traceerbare regelset die vastlegt welk verkeer uberhaupt is toegestaan.**

Waaraan je het vaststelt: Een firewallregelset volgens deny by default, gedocumenteerde open poorten met een onderbouwing, een veilige wifi configuratie, en gewijzigde standaardinloggegevens op netwerkapparaten. Bewijs via een export van de regelset en een externe poortscan.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.21 **Beveiliging van netwerkdiensten: Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen van netwerkdiensten worden geidentificeerd, geimplementeerd en bewaakt.**

Waaraan je het vaststelt: Documenteer voor elke gebruikte netwerkdienst (VPN, DNS, mail, CDN) de beveiligingstoezeggingen en de eigen configuratie, met inbegrip van versleuteling onderweg en de dienstverleningsniveautoezeggingen van de leverancier. Bewijs: een configuratieoverzicht plus het contract of de dienstbeschrijving.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.22 **Segmentering van netwerken: Het netwerk is verdeeld in zones zodat diensten, gebruikersgroepen en systemen met verschillende beschermingsbehoeften elkaar niet ongefilterd kunnen bereiken.**

Waaraan je het vaststelt: Aparte netwerksegmenten of VLAN's voor gasten, beheer en productie; in de cloud, aparte accounts of virtuele netwerken met security groups. In een thuiskantoor is de werkbare implementatie een apart netwerk of VLAN voor werkapparaten, gescheiden van persoonlijke apparaten en domotica.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.23 **Webfiltering: Toegang tot externe websites wordt beheerd om blootstelling aan schadelijke inhoud te verminderen.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Met weinig inspanning haalbaar via een filterende DNS dienst of de webfiltering die in de endpointbeveiliging is inbegrepen, met geblokkeerde categorieen en logging van geblokkeerde verzoeken. Bewijs via de filterconfiguratie en een rapportage export.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.24 **Gebruik van cryptografie: Er wordt bindend vastgesteld waar versleuteling wordt toegepast, met welke algoritmen, en hoe sleutels over hun volledige levenscyclus worden gegenereerd, opgeslagen, geroteerd en vernietigd.** Document

Waaraan je het vaststelt: Een cryptografiebeleid met goedgekeurde algoritmen en minimale sleutellengtes, versleuteling onderweg (TLS) en in rust, plus een sleutelbeheerprocedure voor generatie, opslag, rotatie en vernietiging. Bewijs via het beleid plus de configuratie van de sleuteldienst of vault.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.25 **Levenscyclus van veilige ontwikkeling: Regels voor de veilige ontwikkeling van software en systemen worden vastgesteld en toegepast.**

Waaraan je het vaststelt: Een beschrijving van het ontwikkelproces met beveiligingsrakingspunten per fase: eisen, ontwerp, implementatie, testen, release, exploitatie. Voor kleine teams volstaat een pagina die verwijst naar de concrete CI gates en de beoordelingsverplichting.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.26 **Beveiligingseisen voor applicaties: Beveiligingseisen voor applicaties worden geidentificeerd, gespecificeerd en goedgekeurd tijdens ontwikkeling en verwerving.**

Waaraan je het vaststelt: Beveiligingseisen als expliciete punten in de eisenlijst of als een herbruikbare checklist, bijvoorbeeld georienteerd op gangbare application security verification standaarden. Bewijs via tickets of eisendocumenten met een beveiligingsaspect.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.27 **Beginselen voor veilige systeemarchitectuur en engineering: Beginselen voor veilige systeemengineering worden vastgesteld, gedocumenteerd en toegepast op ontwikkelactiviteiten.**

Waaraan je het vaststelt: Gedocumenteerde beginselen zoals least privilege, defence in depth, veilige standaardinstellingen, dataminimalisatie en een zero trust benadering, samen met zichtbare toepassing ervan in architectuurschetsen of besluitdocumenten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.28 **Veilig coderen: Beginselen van veilig coderen worden toegepast in softwareontwikkeling.**

Waaraan je het vaststelt: Nieuw in de editie van 2022. Bewijs via bindende coderingsregels, statische codeanalyse en secret scanning als verplichte CI gates, gebruik van beoordeelde bibliotheken, en gedocumenteerde codebeoordelingen. Waar functiescheiding onmogelijk is, treden afgedwongen geautomatiseerde gates in de plaats van vier ogen beoordeling; onderbouw dit en toon het aan met de pipelineconfiguratie.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.29 **Beveiligingstests in ontwikkeling en acceptatie: Processen voor beveiligingstests worden vastgesteld en geïmplementeerd binnen de ontwikkelingslevenscyclus.**

Waaraan je het vaststelt: Geautomatiseerde beveiligingstests in de pipeline (afhankelijkheidscontroles, statische en dynamische analyse) plus een periodieke penetratietest waar de beschermingsbehoefte verhoogd is. Bewijs via gedateerde testrapporten en de opvolging van de bevindingen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.30 **Uitbestede ontwikkeling: Uitbestede ontwikkelactiviteiten worden aangestuurd, bewaakt en beoordeeld.**

Waaraan je het vaststelt: Leg bij uitbestede ontwikkeling de beveiligingseisen vast in het contract, borg het eigendom van de code en het recht op beoordeling, en voer codebeoordelingen en beveiligingstests uit voor acceptatie. Zonder uitbestede ontwikkeling moet niet van toepassing consistent worden onderbouwd in de VvT.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.31 **Scheiding van ontwikkel, test en productieomgevingen: Ontwikkel, test en productieomgevingen worden gescheiden en beschermd.**

Waaraan je het vaststelt: Aparte accounts, projecten of namespaces, aparte inloggegevens en aparte gegevenssets. Zorg in combinatie met A.8.11 dat geen productiegegevens in niet productieomgevingen terechtkomen. Bewijs via het omgevingsoverzicht en de rechtentoewijzing.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.32 **Wijzigingsbeheer: Wijzigingen aan informatieverwerkende voorzieningen en informatiesystemen zijn onderworpen aan wijzigingsbeheerprocedures.**

Waaraan je het vaststelt: Een wijzigingsproces met verzoek, impactbeoordeling, testen, goedkeuring, implementatie en een terugdraaipad. In ontwikkelteams voldoet een pull request pipeline met afgedwongen controles en gelogde deployments aan dit punt, mits de historie onveranderlijk is.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.33 **Testinformatie: Testinformatie wordt passend geselecteerd, beschermd en beheerd.**

Waaraan je het vaststelt: Het principe: geen echte persoonsgegevens in testsystemen. Waar dit onvermijdelijk is, documenteer de goedkeuring, de maskering, de toegangsbeperking en de verwijdering na de test. Bewijs via het testgegevensconcept en de verwijderlogs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

A.8.34 **Bescherming van informatiesystemen tijdens audittests: Audittests waarbij toegang tot operationele systemen is betrokken worden gepland en afgestemd met de directie om verstoring van de bedrijfsvoering te voorkomen.**

Waaraan je het vaststelt: Een auditovereenkomst met een tijdvenster, een reikwijdte, waar mogelijk alleen leestoegang, logging van de audittoegang en goedkeuring door de directie. Dit geldt ook voor penetratietests: een schriftelijke testautorisatie met een tijdvenster en een noodcontact is het bewijs.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing