ISO 27001-sjabloon voor de verklaring van toepasselijkheid

Alle 93 beheersmaatregelen uit bijlage A van ISO/IEC 27001:2022, vooraf geladen en klaar om in te vullen — met kolommen voor toepasselijkheid, rechtvaardiging, implementatiestatus en bewijs, precies zoals paragraaf 6.1.3, onder d), verlangt.

Dit PDF is de print- en reviewmetgezel. Het werkbestand is de XLSX (met keuzelijsten, een automatisch berekende samenvatting en een mappingwerkblad voor artikel 21 NIS2); een machine-leesbare Markdown-variant is er voor AI-agents. Alle drie zijn gratis op orbiqhq.com/templates/iso-27001-statement-of-applicability-template — geen e-mail vereist.

Normbasis: ISO/IEC 27001:2022 (incl. Amd 1:2024), paragraaf 6.1.3, onder d), en bijlage A. De namen van de beheersmaatregelen volgen de titels uit bijlage A; de tekst van de maatregelen en de richtlijnen blijven in de norm en in ISO/IEC 27002:2022 en worden hier niet weergegeven. Schaf de normen aan bij ISO of bij NEN. Dit sjabloon is een hulpmiddel, geen juridisch advies.

Wat paragraaf 6.1.3, onder d), verlangt

De verklaring van toepasselijkheid moet bevatten: (1) de noodzakelijke beheersmaatregelen die via het risicobehandelproces zijn bepaald; (2) de rechtvaardiging voor de opname van elke beheersmaatregel; (3) of elke noodzakelijke beheersmaatregel al dan niet is geïmplementeerd; (4) de rechtvaardiging voor de uitsluiting van een beheersmaatregel uit bijlage A. Het is een van de verplichte ISMS-documenten, en uw certificerende auditor gebruikt het als routekaart voor de hele audit.

Zo vult u het register in

1. Werk vanuit uw risicobeoordeling, niet vanuit de lijst met beheersmaatregelen. Beheersmaatregelen worden geselecteerd omdat zij geïdentificeerde risico's behandelen; de VvT legt de uitkomst van die beslissing vast.

2. Beslis over elke rij. Elk van de 93 beheersmaatregelen moet als van toepassing of uitgesloten worden gemarkeerd — lege rijen gelden als een onvolledige VvT.

3. Rechtvaardig de opnames. Benoem het risico of de wettelijke, contractuele of bedrijfsmatige eis die de maatregel behandelt, stel de implementatiestatus vast en verwijs naar het bewijs.

4. Rechtvaardig uitsluitingen inhoudelijk. 'Geen fysieke kantoren' volstaat; 'te duur' niet.

5. Wijs een eigenaar en een datum van laatste beoordeling toe per rij, en houd de VvT onder versiebeheer: werk haar bij zodra de risicobeoordeling, het risicobehandelplan of de set beheersmaatregelen wijzigt, en beoordeel haar ten minste eenmaal per ISMS-cyclus (directiebeoordeling, vóór controle- en hercertificeringsaudits).

Let op: 'Van toepassing? = Nee' en 'Implementatiestatus = Niet van toepassing' zijn verschillende uitspraken. De eerste zegt dat de beheersmaatregel niet nodig is; de tweede hoort niet voor te komen bij een maatregel die als van toepassing is gemarkeerd.

Documentbeheer

Veld	Waarde
Organisatie	_____
Referentie ISMS-scope	_____
Versie van de VvT	_____
Goedgekeurd door	_____
Goedkeuringsdatum	JJJJ-MM-DD
Volgende beoordeling uiterlijk	JJJJ-MM-DD
Referentie risicobeoordeling	_____
Referentie risicobehandelplan	_____

Register van de verklaring van toepasselijkheid

Alle 93 beheersmaatregelen uit bijlage A van ISO/IEC 27001:2022. Markeer elke rij als Ja of Nee bij 'Van toepassing?', noteer de rechtvaardiging, stel de implementatiestatus vast en verwijs naar het bewijs.

Organisatorisch (37 beheersmaatregelen)

ID	Naam van de beheersmaatregel	Nieuw in 2022	Van toepassing?	Rechtvaardiging	Status
A.5.1	Beleid voor informatiebeveiliging	Nee			
A.5.2	Rollen en verantwoordelijkheden voor informatiebeveiliging	Nee			
A.5.3	Functiescheiding	Nee			
A.5.4	Verantwoordelijkheden van de directie	Nee			
A.5.5	Contact met autoriteiten	Nee			
A.5.6	Contact met belangengroepen	Nee			
A.5.7	Dreigingsinformatie	Ja			
A.5.8	Informatiebeveiliging in projectmanagement	Nee			
A.5.9	Inventaris van informatie en andere bijbehorende bedrijfsmiddelen	Nee			
A.5.10	Aanvaardbaar gebruik van informatie en andere bijbehorende bedrijfsmiddelen	Nee			
A.5.11	Teruggave van bedrijfsmiddelen	Nee			
A.5.12	Classificatie van informatie	Nee			
A.5.13	Labelen van informatie	Nee			
A.5.14	Informatieoverdracht	Nee			
A.5.15	Toegangsbeveiliging	Nee			
A.5.16	Identiteitsbeheer	Nee			
A.5.17	Authenticatie-informatie	Nee			
A.5.18	Toegangsrechten	Nee			
A.5.19	Informatiebeveiliging in leveranciersrelaties	Nee			
A.5.20	Informatiebeveiliging opnemen in leveranciersovereenkomsten	Nee			
A.5.21	Beheer van informatiebeveiliging in de ICT-toeleveringsketen	Nee			
A.5.22	Monitoring, beoordeling en wijzigingsbeheer van leveranciersdiensten	Nee			
A.5.23	Informatiebeveiliging bij het gebruik van clouddiensten	Ja			
A.5.24	Planning en voorbereiding van het beheer van informatiebeveiligingsincidenten	Nee			
A.5.25	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Nee			
A.5.26	Reactie op informatiebeveiligingsincidenten	Nee			

ID	Naam van de beheersmaatregel	Nieuw in 2022	Van toepassing?	Rechtvaardiging	Status
A.5.27	Leren van informatiebeveiligingsincidenten	Nee			
A.5.28	Verzamelen van bewijsmateriaal	Nee			
A.5.29	Informatiebeveiliging tijdens verstoringen	Nee			
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	Ja			
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Nee			
A.5.32	Intellectuele-eigendomsrechten	Nee			
A.5.33	Bescherming van registraties	Nee			
A.5.34	Privacy en bescherming van PII	Nee			
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	Nee			
A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Nee			
A.5.37	Gedocumenteerde bedieningsprocedures	Nee			

Mensen (8 beheersmaatregelen)

ID	Naam van de beheersmaatregel	Nieuw in 2022	Van toepassing?	Rechtvaardiging	Status
A.6.1	Screening	Nee			
A.6.2	Arbeidsvoorwaarden	Nee			
A.6.3	Bewustzijn, opleiding en training op het gebied van informatiebeveiliging	Nee			
A.6.4	Disciplinaire procedure	Nee			
A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Nee			
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Nee			
A.6.7	Werken op afstand	Nee			
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	Nee			

Fysiek (14 beheersmaatregelen)

ID	Naam van de beheersmaatregel	Nieuw in 2022	Van toepassing?	Rechtvaardiging	Status
A.7.1	Fysieke beveiligingszones	Nee			
A.7.2	Fysieke toegang	Nee			
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Nee			
A.7.4	Fysieke beveiligingsmonitoring	Ja			
A.7.5	Bescherming tegen fysieke en omgevingsdreigingen	Nee			
A.7.6	Werken in beveiligde gebieden	Nee			
A.7.7	Clear desk en clear screen	Nee			
A.7.8	Plaatsing en bescherming van apparatuur	Nee			
A.7.9	Beveiliging van bedrijfsmiddelen buiten het terrein	Nee			
A.7.10	Opslagmedia	Nee			
A.7.11	Nutsvoorzieningen	Nee			
A.7.12	Beveiliging van bekabeling	Nee			
A.7.13	Onderhoud van apparatuur	Nee			
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Nee			

Technologisch (34 beheersmaatregelen)

ID	Naam van de beheersmaatregel	Nieuw in 2022	Van toepassing?	Rechtvaardiging	Status
A.8.1	Eindgebruikersapparatuur	Nee			
A.8.2	Geprivilegieerde toegangsrechten	Nee			
A.8.3	Beperking van toegang tot informatie	Nee			
A.8.4	Toegang tot broncode	Nee			
A.8.5	Veilige authenticatie	Nee			
A.8.6	Capaciteitsbeheer	Nee			
A.8.7	Bescherming tegen malware	Nee			
A.8.8	Beheer van technische kwetsbaarheden	Nee			
A.8.9	Configuratiebeheer	Ja			
A.8.10	Verwijderen van informatie	Ja			
A.8.11	Datamaskering	Ja			
A.8.12	Voorkomen van gegevenslekken	Ja			
A.8.13	Back-up van informatie	Nee			
A.8.14	Redundantie van informatieverwerkende faciliteiten	Nee			
A.8.15	Loggen	Nee			
A.8.16	Monitoringactiviteiten	Ja			
A.8.17	Kloksynchronisatie	Nee			
A.8.18	Gebruik van geprivilegieerde systeemhulpmiddelen	Nee			
A.8.19	Installatie van software op operationele systemen	Nee			
A.8.20	Netwerkbeveiliging	Nee			
A.8.21	Beveiliging van netwerkdiensten	Nee			
A.8.22	Scheiding van netwerken	Nee			
A.8.23	Webfiltering	Ja			
A.8.24	Gebruik van cryptografie	Nee			
A.8.25	Veilige ontwikkelcyclus	Nee			
A.8.26	Beveiligingseisen voor applicaties	Nee			
A.8.27	Principes voor veilige systeemarchitectuur en -engineering	Nee			
A.8.28	Veilig programmeren	Ja			
A.8.29	Beveiligingstesten bij ontwikkeling en acceptatie	Nee			
A.8.30	Uitbestede ontwikkeling	Nee			
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Nee			

ID	Naam van de beheersmaatregel	Nieuw in 2022	Van toepassing?	Rechtvaardiging	Status
A.8.32	Wijzigingsbeheer	Nee			
A.8.33	Testinformatie	Nee			
A.8.34	Bescherming van informatiesystemen tijdens audittests	Nee			

De VvT hergebruiken als NIS2-bewijs

Voor EU-entiteiten die onder NIS2 (Richtlijn (EU) 2022/2555) vallen, mappen de set van toepassing zijnde beheersmaatregelen en het bijbehorende bewijs op de risicobeheersmaatregelen van artikel 21, lid 2 — de XLSX bevat het volledige mappingwerkblad. Aansluiting op ISO 27001 ondersteunt de naleving van NIS2, maar toont die op zichzelf niet aan: NIS2 kent eigen verwachtingen op het gebied van governance, rapportage en handhaving onder de nationale omzettingswetgeving (in Nederland de Cyberbeveiligingswet).

Van spreadsheet naar levend bewijs

Een VvT in een spreadsheet veroudert de dag na de audit. Orbiq houdt hetzelfde register van beheersmaatregelen verbonden met levend bewijs en publiceert de kant richting kopers naar een Europees Trust Center: orbiqhq.com.

Versie 1.0 · gepubliceerd 2026-07-13 · Vrij te gebruiken; bronvermelding gewaardeerd. Bron: orbiqhq.com/templates/iso-27001-statement-of-applicability-template