Stappenplan

— ISO 27002 transitie —

In dit handige stappenplan nemen we je stap voor stap mee door de transitie naar de ISO 27002:2022 norm.

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

Maak de transitie naar ISO 27002:2022

Ben je ISO 27001:2013 gecertificeerd en wil je de overgang maken naar de nieuwe versie van de Annex A; ISO27002:2022? Dan dien je een aantal stappen te doorlopen om de transitie te maken naar de nieuwe versie van de Annex A. In onderstaand stappenplan nemen we je mee in de wijzigingen en welke stappen je moet zetten om te voldoen aan de nieuwe norm.

Heb je vragen? Onze adviseurs staan voor je klaar!

Inhoudsopgave

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Stap 1: Herindelen Beheersmaatregelen en risico's

Voorheen kende de ISO 27002 een lange lijst van 114 beheersmaatregelen. Met de komst van de nieuwe versie ISO 27002:2022 norm is deze lijst teruggebracht naar 93 maatregelen. Tevens zijn de maatregelen voortaan verdeeld in 4 categorieën;

• Organisational controls
In deze categorie vind je alle beheersmaatregelen terug rondom controles van systemen en procedures in je organisatie. Denk hierbij bijvoorbeeld aan toegangscontroles.

• Organization of information security
In deze categorie vind je alle maatregelen rondom informatiebeveiliging terug. Bijvoorbeeld de preventie van datalekken.

• Physical controls
In deze categorie vind je de beheersmaatregelen terug die te maken hebben met het uitvoeren van fysieke controles zoals clear desk en clear screen.

• Technological controls
In deze categorie vind je alle technologische beheersmaatregelen terug. Bijvoorbeeld Logging.

ACTIE

Zorg dat je op de hoogte bent van de 93 beheersmaatregelen en dat deze administratief worden aangepast en onderverdeeld in bovenstaande 4 categorieën. Door dit te doen is je managementsysteem weer up-to-date en breng je in kaart voor welke beheersmaatregelen nog eventuele acties nodig zijn.

Let op: Binnen deze 93 maatregelen zijn 11 nieuwe maatregelen terug te vinden, hierover lees je meer in stap 2.

Stap 2: Risico-inventarisatie nieuwe beheersmaatregelen

Binnen de 93 beheersmaatregelen in de ISO 27002:2022 norm zijn er 11 nieuwe beheersmaatregelen aanwezig. Doordat deze nog niet in de vorige norm zijn opgenomen zijn, zijn deze nog niet in verband gebracht met aanwezige risico's. Het gaat om onderstaande 11 maatregelen:

5.7 Threat intelligence
Threat Intelligence is erop gericht om bedreigingen voor het ISMS op tijd te detecteren en zo laag mogelijk te maken. Hiervoor dienen de bedreigingen op zowel operationeel als strategisch en tactisch niveau in kaart te worden gebracht.

5.23 Information security for use of cloud services
De beheersmaatregel information security for use of cloud services draait om het specificeren en beheren van informatiebeveiliging voor het gebruik van cloud services.

5.30 ICT readiness for business continuity
Deze beheersmaatregel draait om het garanderen van de beschikbaarheid van informatie binnen de organisatie. Het opstellen van een ICT Continuïteitsplan staat hierbij centraal.

7.4 Physical security monitoring
Bij Physical security monitoring gaat het om het monitoren van de omgeving. Denk hierbij aan de monitoring door middel van bewakers, inbraakalarmsystemen of bewaking doormiddel van camerasystemen.

8.9 Configuration management
Deze beheersmaatregel is gericht op het instellen van de juiste beveiligingsinstellingen van hardware, software, services en netwerken.

8.10 Information deletion
Deze beheersmaatregel heeft als doel om gevoelige informatie veilig te stellen en het onnodig openbaren hiervan te voorkomen. Het formuleren van beleid rondom het veilig verwijderen van gegevens staat hierbij centraal.

8.11 Data masking
Data masking is erop gericht om de blootstelling van gevoelige gegevens te voorkomen. Denk hierbij bijvoorbeeld aan persoonlijk identificeerbare informatie zoals bepaaldec persoonsgegevens.

8.12 Data leakage prevention
Deze beheersmaatregel is er specifiek op gericht om datalekken te voorkomen. Hiervoor wordt o.a. dataclassificatie uitgevoerd en worden data lekkende kanalen gemonitord. Je kunt hierbij denken aan e-mail, bestandsoverdrachten, en draagbare harde schijven.

8.16 Monitoring activities
Binnen deze beheersmaatregel wordt afwijkend gedrag en eventuele informatiebeveiligingsincidenten gedetecteerd. Het level van monitoring wordt vooraf door de organisatie zelf bepaald.

8.23 Web filtering
Met deze beheersmaatregel worden systemen beschermd die kwetsbaar zijn voor malware. Hierbij staat o.a. het voorkomen van toegang aan ongeautoriseerde internetbronnen centraal.

8.28 Secure coding
Bij Secure coding draait het om het veilig schrijven van software. Hiermee worden mogelijke kwetsbaarheden in de informatiebeveiliging van software vermindert.

ACTIE:

Binnen de ISO 27002 norm dienen alle risico's gekoppeld te zijn aan relevante beheersmaatregelen voor de organisatie. Bekijk daarom de 11 nieuwe beheersmaatregelen en koppel deze aan de risico's die van toepassing zijn op jouw organisatie. Plan vervolgens de benodigde acties in die nodig zijn om aan de beheersmaatregel te voldoen.

Stap 3: Verklaring van toepasselijkheid

In de verklaring van toepasselijkheid worden de uitkomsten beschreven van de beheersmaatregelen. Waarom is een beheersmaatregel wel- of niet van toepassing op jouw organisatie?

ACTIE:

Doorloop de 11 nieuwe beheersmaatregelen en beschrijf duidelijk waarom de beheersmaatregel wel- of juist niet op jouw organisatie van toepassing is.

Let op; wanneer de beheersmaatregel niet van toepassing is dien je dit uitgebreid te onderbouwen.

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Concreet aan de slag? Doe de transitiescan!

Wil of moet je aan de slag met de wijzigingen, maar weet je niet goed waar te beginnen? Dan helpen wij je graag op weg met deze transitie ISO 27002 door middel van onze Transitiescan ISO 27002.

Bij de Transitiescan voeren wij in 1 dagdeel (4 uur) een zogenaamde ‘document review’ uit op het gedocumenteerde ISMS van je organisatie. Deze Transitiescan bestaat uit een analyse van de huidige situatie en een advies/plan van aanpak. Hiermee weet je snel waar je staat als organisatie en wat je nog moet doen om te voldoen aan ISO 27002:2022.

MEER INFORMATIE

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

CERTIFICERINGSADVIES NEDERLAND

JOUW PARTNER IN CERTIFICEREN

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

Heb je te maken met de transitie naar ISO 27002:2022 en wil je hier meer informatie over? Neem dan gerust contact met ons op. Wij vertellen je graag meer!

CertificeringsAdvies Nederland is de partner in certificeren. Wij ondersteunen mensen en organisaties in hun ontwikkeling. Zo helpen wij jou met je organisatie slim in te richten en zijn we een inspiratiebron voor de mensen binnen je organisatie. Dat doen we door advies-, opleidings- en outsourcingsdiensten aan te bieden binnen de thema's Kwaliteit, Arbo & Veiligheid, Milieu & MVO, Voedselveiligheid en Informatiebeveiliging.

Meer weten?

Kijk op www.certificeringsadvies.nl
T 085 4879972
E info@certificeringsadvies.nl