

# Stappenplan

ISO/IEC 27001:2022 - De nieuwe norm



# Stappenplan

## ISO/IEC 27001:2022 - De nieuwe norm

Om je ISO 27001 certificering te behouden, moet je voor 1 november 2025 voldoen aan de nieuwe ISO/IEC 27001:2022 norm. Er is geen mogelijkheid meer om te certificeren voor de 'oude' ISO/IEC 27001:2013 norm. De overstap hoeft geen complex en tijdrovend proces te zijn. Met een goede voorbereiding en planning kun je de veranderingen vloeiend en efficiënt implementeren. Ons stappenplan helpt je hierbij.



**Rianne Nijhuis**

Lead auditor

T +316 30 38 94 12

E [rienne.nijhuis@vicoconnect.com](mailto:rienne.nijhuis@vicoconnect.com)



**Charlotte Adama**

Lead auditor

T +316 43 20 88 86

E [charlotte.adama@vicoconnect.com](mailto:charlotte.adama@vicoconnect.com)

### Overstap service van Vico

Liever hulp bij het overstappen naar de nieuwe norm? Maak gebruik van de overstap service van Vico. Wij geven onafhankelijk advies en benaderen de overstap pragmatisch. Met oog voor praktijk en resultaat en altijd in samenwerking met jou en je collega's.



# Stappenplan

Onderstaand stappenplan geeft je een leidraad in de stappen die jouw organisatie moet nemen om succesvol over te stappen naar de nieuwe ISO/IEC 27001:2022 norm. Wil je een helder overzicht van alle veranderingen? Download onze checklist met de verschillen op [www.vicoconnect.com/iso-27001-nieuw](http://www.vicoconnect.com/iso-27001-nieuw).

## 1. Voer een gap-analyse uit

Identificeer de verschillen tussen jullie huidige Information Security Management Systeem (ISMS) en de nieuwe ISO/IEC 27001:2022 norm. Leg de huidige processen/het huidige handboek, de risicoanalyse, het risicobehandelplan, de Verklaring van Toepasselijkheid (VVT) naast elkaar en maak een analyse van de oude en nieuwe maatregelen.

Je kunt hierbij gebruik maken van de volgende informatie:

- Verklaring van Toepasselijkheid (VVT)
- Gap-analyse oude en nieuwe maatregelen \*

*\* Of download onze checklist verschillen op [www.vicoconnect.com/iso-27001-nieuw](http://www.vicoconnect.com/iso-27001-nieuw).*

## 2. Stel een actieplan op

Op basis van de gap-analyse bepaal je welke acties noodzakelijk zijn om het ISMS aan te passen aan de nieuwe norm. Wijs hierbij verantwoordelijkheden toe en stel deadlines voor het voltooien van deze acties.

## 3. Update de risicoanalyse en het behandelplan

Vergelijk jullie huidige maatregelen met de nieuwe Annex A van ISO/IEC 27001:2022 om te controleren of er geen essentiële maatregelen ontbreken. Pas de risicoanalyse en het behandelplan aan op basis van deze vergelijking.

## 4. Implementeer de nieuwe, bijgewerkte en samengevoegde maatregelen

Implementeer de 11 nieuwe, 58 bijgewerkte en 24 samengevoegde beheersmaatregelen uit de nieuwe norm. Gebruik de nieuwe ISO 27002 als leidraad. Hier vind je een goede toelichting over wat er wordt verwacht van een organisatie.



## **5. Herzie de VVT**

Update jullie VVT om te voldoen aan de nieuwe Annex A.

## **6. Interne audit uitvoeren en updaten auditprogramma**

Voer een interne audit uit om te verifiëren of het bijgewerkte Information Security Management Systeem (ISMS) voldoet aan de eisen van de nieuwe ISO/IEC 27001:2022 norm. Identificeer eventuele tekortkomingen en stel een plan op om deze aan te pakken.

## **7. Opleiding en communicatie**

Informeer alle betrokkenen binnen jouw organisatie over de veranderingen en zorg voor passende opleiding en bewustwording. Zorg voor effectieve communicatie tussen alle betrokken afdelingen en teams.

## **8. Externe audit plannen en certificering**

Plan een externe audit door een certificerende instantie en bereid je goed voor. Zorg ervoor dat alle plannen, bewijsmateriaal en documentatie klaarliggen, zodat je kunt laten zien dat jouw organisatie voldoet aan de nieuwe norm.

## **9. Continu verbeteren**

Blijf werken aan verbetering, ook na de ISO/IEC 27001:2022 certificering van jouw organisatie. Gebruik de resultaten van de interne en externe audits om jullie Information Security Management Systeem (ISMS) verder te verbeteren en te optimaliseren.

## Over Vico Connect

Vico Connect helpt organisaties met het behalen en behouden van (ISO) certificeringen. Wij maken een vertaalslag van certificeringseisen en zorgen voor een werkbare toepassing. Dit doen wij met pragmatische adviseurs en eigen procesmanagement software.

Wij zijn ervaren Lead auditors met een bedrijfskundige achtergrond. Onze kennis over (ISO) certificeringen is altijd up-to-date. Wij ontwerpen de benodigde managementsystemen voor jouw organisatie en begeleiden je bij de implementatie.

Ons advies is pragmatisch. Wij zorgen ervoor dat onze oplossingen aansluiten op de huidige werkwijze van jouw organisatie, dus geen grote veranderingen. Met onze kennis en software maken we de bedrijfsvoering makkelijker en plezieriger binnen wetgeving en normen.

Wij laten ons inspireren door de Italiaanse filosoof Giambattista Vico. Hij pleitte voor het gebruik van metaforen om complexe zaken duidelijk te maken.

Wij gebruiken ons procesmodel als metafoor om de organisatie helder in kaart te brengen. Dit model geeft inzicht en overzicht voor iedereen. Ons geoptimaliseerde procesmodel fungeert als de verbindende schakel tussen medewerkers en de systemen die zij gebruiken.





Vico Connect B.V.

**T** +31 55 303 49 79

**E** [info@vicoconnect.com](mailto:info@vicoconnect.com)

[vicoconnect.com](http://vicoconnect.com)