

INFORMATIEBEVEILIGING: ISO 27001 IS GEÛPDATET

“ARE YOU READY?”

Uw gids voor een succesvolle overgang naar
ISO 27001:2022

LRQA





Introductie

In februari 2022 is ISO 27002:2022 geactualiseerd. De norm voorziet in de best practice controles die organisaties kunnen uitvoeren om de beveiliging te verbeteren. Als gevolg daarvan zal naar verwachting in het laatste kwartaal van 2022 ook een nieuwe versie van ISO 27001 - de internationale norm die de vereisten van een managementsysteem voor informatiebeveiliging (ISMS) schetst - worden gepubliceerd. Organisaties met een bestaande ISO 27001:2013-certificering krijgen drie jaar de tijd om over te stappen op de nieuwe norm.

De nieuwe versie van de norm zal de controles bevatten die in ISO 27002:2022 worden beschreven. Organisaties zullen hun risicobeoordeling opnieuw moeten bekijken om te bepalen of er updates of nieuwe risicobehandelingen moeten worden geïmplementeerd.

In deze gids schetsen we 10 belangrijke stappen die een ISO 27001-gecertificeerde organisatie kan nemen om succesvol over te stappen op de nieuwe norm.



Tien stappen voor een succesvolle overgang naar ISO 27001:2022

1

Begrijp de veranderingen



2

Evalueer uw trainingsbehoeften



3

Voer een Gap Analyse uit omtrend de bestaande controles



4

Herzie uw risicobeoordeling



5

Werk uw risicobehandelingsplan (RTP) bij



6

Werk uw verklaring van toepasbaarheid bij



7

Plan uw overgangsaudit



8

Voltooi uw audit en voer eventuele wijzigingen in



9

Promoot uw ISO 27001:2022 certificering



10

Focus op voortdurende verbetering





1. Begrijp de veranderingen

Inzicht verwerven in ISO 27002:2022, aangezien de nieuwe beveiligingsmaatregelen zullen voorkomen in Bijlage A van ISO 27001. Dit is de belangrijkste herziening van de nieuwe norm.

ISO 27002:2022 is geherstructureerd, met 93 controles in plaats van 114, opgesplitst verdeeld over 4 verschillende thema's:

- Organisatorisch
- Menselijk
- Fysiek
- Technologisch

53 controles uit de vorige versie zijn samengevoegd tot 24 in ISO 27002:2022, waarbij 11 nieuwe controles zijn toegevoegd. Wij wijzen u er graag op dat de meeste controles onderworpen zijn aan tekstwijzigingen die gevolgen kunnen hebben voor de wijze waarop de norm wordt geïnterpreteerd en toegepast.



2. Evalueer uw trainingsbehoeften

Maak een trainingsprogramma voor uw teamleden om hun kennis rond de norm op te bouwen en ervoor te zorgen dat ze de veranderingen effectief kunnen implementeren.

Na de publicatie van de herziene norm zullen bijgewerkte versies van LRQA's ISO 27001-trainingen beschikbaar komen met opties voor alle ervaringsniveaus, waaronder:

- Een inleiding tot ISO 27001:2022
- ISO 27001:2022 Implementatie
- ISO 27001:2022 Interne auditor
- ISO 27001:2022 Auditor Conversie
- ISO 27001:2022 Lead Auditor Conversie
- ISO 27001:2022: Management Briefing

Wij geven trainingen geven in verschillende online, persoonlijke of gemengde leerstijlen, afhankelijk van wat het beste werkt voor u en uw teamleden.



3. Voer een Gap-analyse uit omtrend de bestaande controles

Een Gap-analyse waarin uw bestaande controles en risicobehandelingen worden vergeleken met de controles en risicobehandelingen die zijn opgenomen in ISO 27002:2022.

Bijlage B van ISO 27002:2022 is een goed startpunt, omdat deze een nuttige vergelijking bevat van alle beschikbare controles en hoe deze overeenkomen met die in de vorige versie (ISO 27002:2013). De bijgewerkte norm verdeelt controles in vier hoofdthema's - organisatorisch, menselijk, fysiek en technologisch - en we raden aan een gespecialiseerd team te vormen dat zich deze gebieden eigen kan maken en inzicht kan verschaffen.

LRQA biedt optionele pre-assessment diensten die worden uitgevoerd door deskundige auditors in de vorm van een Gap-analyse of voorlopige audit. Wij kijken naar uw bestaande controles en bredere ISMS en stellen vast welke gebieden aandacht nodig hebben.



4. Herzie uw risicobeoordeling

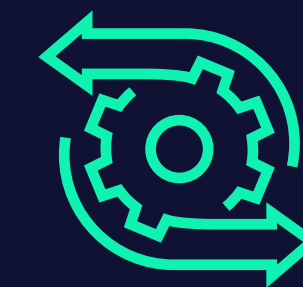
Het is noodzakelijk na te gaan of uw risicobeoordeling, samen met de doelstellingen en context, goed afgestemd blijft op uw bedrijf en risicobereidheid - als dat niet zo is, moeten er wijzigingen worden aangebracht. Misschien wilt u ISO 27005 raadplegen - de internationale norm die de procedures voor het uitvoeren van een risicobeoordeling van informatiebeveiliging.



5. Werk uw risicobehandelingsplan (RTP) bij

U moet het risicobehandelingsplan bijwerken om uw beslissingen over de reactie op bedreigingen weer te geven, door passende controles te selecteren uit de bijgewerkte versie van ISO 27002, die vindt u in bijlage A van ISO 27001:2022.

U kunt LRQA inschakelen om een aanvullende Gap-analyse uit te voeren om ervoor te zorgen dat de geselecteerde controles gerechtvaardigd en effectief zijn. Onze onafhankelijke inzichten geven u vertrouwen in de gereedheid van uw organisatie en onze specialisten op het gebied van cyberbeveiliging, kunnen advies en begeleiding geven over technische controles en diensten.



6. Werk uw verklaring van toepasbaarheid bij

Het is cruciaal dat u uw verklaring van toepasbaarheid bijwerkt om het bewijs en de rechtvaardiging voor het al dan niet opnemen van controles of beleid weer te geven. U moet ook aangeven of uw bedrijf controles heeft uitgevoerd in overeenstemming met het risicobehandelingsplan. Indien het antwoord ja is, moet er een degelijk intern auditprogramma worden uitgevoerd om de effectiviteit van uw activiteiten te kunnen de doeltreffendheid van uw activiteiten te beoordelen.



7. Plan uw overgangsaudit

Tegen die tijd hebben de veranderingen die u hebt doorgevoerd uw managementsysteem, informatiebeveiliging en bredere cyberweerbaarheid versterkt. Het is tijd om contact op te nemen met LRQA om uw speciale overgangsaudit te bespreken, die kan worden uitgevoerd als een op zichzelf staande activiteit of in lijn met een ander gepland bezoek.

Organisaties met een bestaande ISO 27001:2013-certificering hebben drie jaar de tijd om over te stappen naar de nieuwe norm.

[Neem contact op](#) →



8. Voltooi uw audit en voer eventuele wijzigingen in

Uw auditor beoordeelt uw ISMS en ondersteunende documentatie om te bepalen of het voldoet aan de eisen van ISO 27001:2022 - met speciale aandacht voor de wijzigingen in de controles in Bijlage A. Na afloop ontvangt u uw auditrapport, met daarin de feedback van uw auditor en eventuele bevindingen die die moeten worden aangepakt voordat de certificering wordt toegekend.



9. Promoot uw ISO 27001:2022 certificering

Uw certificering toont aan dat u zich inzet voor internationaal erkende beste praktijken en voortdurende verbetering - helpt u business zaken te winnen en te voldoen aan klanten. U kunt erop vertrouwen dat uw ISMS robuust en effectief is - met controles en risicobehandelingen die het veranderende dreigingslandschap weerspiegelen.



10. Focus op voortdurende verbetering

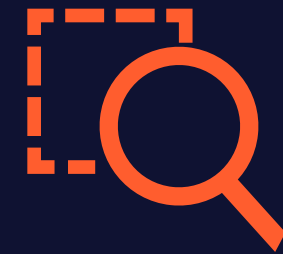
Na certificering is het belangrijk om de vaart erin te houden om ervoor te zorgen dat uw ISMS effectief en goed onderhouden blijft. We voeren jaarlijks controleaudits uit die gericht zijn op de status van uw systeem. We kijken ook of er voortdurend verbeteringen worden aangebracht.

Onze ISO 27001:2022-training en auditdiensten

[Previous](#)[Next](#)

Training

Bouw uw kennis op van ISO 27001:2022 met een reeks van trainingen ontworpen voor verschillende ervaringsniveaus - geleverd via meerdere leerstijlen.



Gap analysis

Een optionele dienst waarbij een van onze deskundige auditors u helpt bij het identificeren van kritieke, risicovolle of zwakke gebieden van uw managementsysteem voorafgaand aan uw overgangsaudit.



Transition audit

Wij beoordelen uw ISMS volgens de eisen van ISO 27001:2022 - met een bijzondere aandacht voor de Annex A controles en hoe deze van invloed zijn op uw managementsysteem.



Integrated audits

Als u meerdere managementsystemen hebt ingevoerd, kunt u profiteren van een geïntegreerd audit- en bewakingsprogramma dat efficiënter en kosteneffectiever is.

Samen met u werken aan elk aspect van cyberbeveiliging

[Previous](#)[Next](#)

Door onze ruime ervaring met assurance, gecombineerd met bekroonde cyberbeveiligingsdiensten en informatie over bedreigingen, kunnen wij inzichten op maat leveren in en bescherming tegen de unieke bedreigingen voor uw bedrijf. Zo blijft u cyberrisico's een stap voor, vandaag, morgen en daarna.

Wij bieden audit-, trainings- en certificeringsdiensten op basis van 's werelds toonaangevende internationale normen en programma's, aangevuld met een breed scala aan geavanceerde cyberbeveiligingsdiensten die door onze specialisten worden geleverd.

Wij helpen u om specifieke bedreigingen waarmee u wordt geconfronteerd te identificeren en strategieën op te stellen om deze te beperken. We werken met u samen om uw systemen te certificeren, kwetsbaarheden te identificeren en aanvallen en incidenten te voorkomen die gevolgen kunnen hebben voor uw merkintegriteit, financiën en activiteiten.



Informatie-beveiliging

Onze compliance- en certificeringsdiensten helpen u bij de bescherming van bedrijfskritische informatie en internationaal erkende best practices aan te tonen.

[Lees meer >](#)

Operationele weerbaarheid

Wees voorbereid om verstoringen te voorkomen, te reageren en snel te herstellen met onze certificering, training en governance, risico en nalevingsdiensten.

[Lees meer >](#)

Bescherming tegen cyberdreigingen

Blijf cyberbedreigingen een stap voor met oplossingen op maat die een eerste verdedigingslinie vormen en bereidt een reactie voor op alle soorten cyberaanvallen.

[Lees meer >](#)



YOUR FUTURE. OUR FOCUS.

Over LRQA:

Door het samenbrengen van ongeëvenaarde expertise op het gebied van certificering, assurance op maat, cyberbeveiliging, inspectie en training zijn wij een toonaangevende wereldwijde assurance provider geworden.

We zijn trots op ons erfgoed, maar het is wie we vandaag zijn dat er echt toe doet, want dat is wat vormgeeft aan hoe we met onze klanten zullen samenwerken. Door het combineren van sterke waarden, tientallen jaren ervaring in risico management, en een scherpe focus op de toekomst, zijn we er om onze klanten te ondersteunen bij het bouwen van veiligere, duurzamere organisaties.

Onze innovatieve end-to-end oplossingen - van onafhankelijke audits voor derden, certificering en training tot adviesdiensten, realtime assurance technologie en data gestuurde transformatie van de supply chain - helpen onze klanten bij het handelen in een snel veranderend risicolandschap. We zorgen ervoor dat zij hun eigen toekomst vormgeven, in plaats van die voor hen te laten bepalen.

Neem contact op

Bezoek www.lrqa.com/nl voor meer informatie, email info.nl@lrqa.com



LRQA Nederland BV
George Hintzenweg 77
Rotterdam
3068 AX
Nederland