ISO/IEC 27001:2022

Start your transition

New controls

Belangrijkste wijzigingen

In februari 2022 werd ISO 27002:2022 – de norm die de best practice-controles biedt die organisaties kunnen implementeren om de beveiliging te verbeteren – bijgewerkt. Als gevolg daarvan werd in het laatste kwartaal van 2022 ook een nieuwe versie van ISO 27001 gepubliceerd – de internationale norm die de vereisten van een information security management system (ISMS) beschrijft.

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

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

Er zijn nu
93
controles
in plaats van
114

In totaal zijn er
11
nieuwe controles

56
controles van ISO 27001:2013 zijn nu samengevoegd tot 24 controles in ISO 27001:2022

Het merendeel

van de controles is onderworpen aan een vorm van tekstwijziging die van invloed kan zijn op de interpretatie en de implementatie van de norm

De controles zijn nu verdeeld over vier ‘nieuwe’ thema’s

Organisatorisch	Mensen	Fysiek	Technisch
- 28 samengevoegd	- 2 samengevoegd	- 5 samengevoegd	- 21 samengevoegd
- 3 nieuw	- 0 nieuw	- 1 nieuw	- 7 nieuw

ISO 27001:2022-controles

De controles die in ISO 27002:2022 worden beschreven, worden opgenomen in ISO 27001:2022 Annex A – wat het meest significante wijzigingsgebied van de nieuwe norm vertegenwoordigt.

NIEUW **ISO 27001:2022**		
CONTROLE	**THEMA (NIEUW)**	**TITEL**
INFORMATIEBEVEILIGINGSBELEID		
A.5.1	Organisatorische controles	Beleid inzake informatiebeveiliging
A.5.1.2	**Samengevoegd in A.5.1**	
ORGANISATIE VAN INFORMATIE		
A.5.2	Organisatorische controles	Rollen en verantwoordelijkheden inzake informatiebeveiliging
A.5.3	Organisatorische controles	Scheiding van taken
A.5.5	Organisatorische controles	Contact met autoriteiten
A.6.6	Organisatorische controles	Contact met speciale belangengroepen
NIEUW A.5.7	Organisatorische controles	Informatie over bedreigingen
A.5.8	Organisatorische controles	Informatiebeveiliging in projectmanagement
A.8.1	Technisch	Eindpuntapparatuur voor gebruikers
A.6.7	Mensen	Telewerken

BEVEILIGING VAN HUMAN RESOURCES		
A.6.1	Mensen	Screening
A.6.2	Mensen	Algemene arbeidsvoorwaarden
A.5.4	Organisatorische controles	Managementverantwoordelijkheden
A.6.3	Mensen	Bewustzijn, opleiding en training inzake informatiebeveiliging
A.6.4	Mensen	Disciplinair proces
A.6.5	Mensen	Verantwoordelijkheden na beëindiging of wijziging van dienstverband
ASSETMANAGEMENT		
A.5.9	Organisatorische controles	Inventaris van informatie en andere bijbehorende assets
A.8.1.2	**Samengevoegd in A.5.9**	
A.5.10	Organisatorische controles	Aanvaardbaar gebruik van informatie en andere bijbehorende assets
A.5.11	Organisatorische controles	Teruggave van bedrijfsmiddelen
A.5.12	Organisatorische controles	Classificatie van informatie
A.5.13	Organisatorische controles	Labelen van informatie
A.8.2.3	**Samengevoegd in A.5.10**	
A.7.10	Fysiek	Opslagmedia
A.8.3.2	**Samengevoegd in A.7.10**	
A.8.3.3	**Samengevoegd in A.7.10**	

TOEGANGSCONTROLE		
A.5.15	Organisatorische controles	Toegangscontrole
A.9.1.2	**Samengevoegd in A.5.15**	
A.5.16	Organisatorische controles	Identiteitsbeheer
A.5.18	Organisatorische controles	Toegangsrechten
A.8.2	Technisch	Toegangsrechten van bevoegden
A.5.17	Organisatorische controles	Authenticatiegegevens
A.9.2.5	**Samengevoegd in A.5.18**	
A.9.2.6	**Samengevoegd in A.5.18**	
A.9.3.1	**Samengevoegd in A.5.17**	
A.8.3	Technisch	Beperking van toegang tot informatie
A.8.5	Technisch	Beveiligde authenticatie
A.9.4.3	**Samengevoegd in A.5.17**	
A.8.18	Technisch	Gebruik van nutsprogramma's door bevoegden
A.8.4	Technisch	Toegang tot broncode
CRYPTOGRAFIE		
A.8.24	Technisch	Gebruik van cryptografie
Samengevoegd in A.8.24 met A.10.1.1		

FYSIEKE EN OMGEVINGSBEVEILIGING			
	A.7.1	Fysiek	Fysieke veiligheidsperimeters
	A.7.2	Fysiek	Fysieke toegang
	A.7.3	Fysiek	Beveiliging van kantoren, ruimten en faciliteiten
NIEUW	A.7.4	Fysiek	Fysieke beveiligingsmonitoring
	A.7.5	Fysiek	Bescherming tegen fysieke en omgevingsbedreigingen
	A.7.6	Fysiek	Werken in beveiligde zones
A.11.1.6	**Samengevoegd in A.7.2 met A.11.1.2**		
	A.7.8	Fysiek	Plaatsing en bescherming van apparatuur
	A.7.11	Fysiek	Ondersteunende nutsvoorzieningen
	A.7.12	Fysiek	Beveiliging van kabels
	A.7.13	Fysiek	Onderhoud van apparatuur
A.11.2.5	**Samengevoegd in A.7.10**		
	A.7.9	Fysiek	Beveiliging van bedrijfsmiddelen buiten het terrein
	A.7.14	Fysiek	Veilige afvoer of hergebruik van apparatuur
A.11.2.8	**Samengevoegd in A.8.1 met A.6.2.1**		
	A.7.7	Fysiek	Opgeruimde werkplek en monitor

BEVEILIGING VAN ACTIVITEITEN			
	A.5.37	Organisatorische controles	Gedocumenteerde bedrijfsprocedures
	A.8.32	Technisch	Change Management
	A.8.6	Technisch	Capaciteitsbeheer
	A.8.31	Technisch	Scheiding van ontwikkelings-, test- en productieomgevingen
	A.8.7	Technisch	Bescherming tegen malware
	A.8.13	Technisch	Back-up van informatie
	A.8.15	Technisch	Protocollering
A.12.4.2		**Samengevoegd in A.8.1.5**	
A.12.4.3		**Samengevoegd in A.8.1.5**	
NIEUW	A.8.16	Technisch	Monitoringactiviteiten
NIEUW	A.8.17	Technisch	Kloksynchronisatie
NIEUW	A.8.19	Technisch	Installatie van software op besturingssystemen
NIEUW	A.8.8	Technisch	Beheersing van technisch kwetsbare punten
NIEUW	A.8.9	Technisch	Configuratiebeheer
NIEUW	A.8.10	Technisch	Wissen van informatie
NIEUW	A.8.11	Technisch	Datamasking
NIEUW	A.8.12	Technisch	Preventie van gegevenslekken
A.12.6.2		**Samengevoegd in A.8.19 met A.12.5.1**	
	A.12.7.1 A.8.34	Technisch	Bescherming van informatiesystemen tijdens audittesten

COMMUNICATIEBEVEILIGING		
A.8.20	Technisch	Netwerkbeveiliging
A.8.21	Technisch	Beveiliging van netwerkdiensten
A.8.22	Technisch	Scheiding van netwerken
NIEUW A.8.23	Technisch	Webfiltering
A.5.14	Organisatorische controles	Informatieoverdracht
A.13.2.2	**Samengevoegd in A.5.14**	
A.13.2.3	**Samengevoegd in A.5.14**	
A.6.6	Mensen	Vertrouwelijkheids- of geheimhoudingsovereenkomsten
SYSTEEMAANKOOP, -ONTWIKKELING EN -ONDERHOUD		
A.14.1.1	**Samengevoegd in A.5.8 met A.6.1.5**	
A.8.26	Technisch	Beveiligingseisen van applicaties
A.14.1.3	**Samengevoegd met A.8.26**	
A.8.2.5	Technisch	Beveiliging van de ontwikkelingslevenscyclus
A.14.2.2	**Samengevoegd in A.8.32 met A.12.1.2**	
A.14.2.3	**Samengevoegd in A.8.32 met A.12.1.2, A.14.2.2 en A.14.2.4**	
A.14.2.4	**Samengevoegd in A.8.32 met A.12.1.2, A.14.2.2 en A.14.2.3**	
A.14.2.5 A.8.27	Technisch	Veilige systeemarchitectuur en technische principes
A.14.2.6	**Samengevoegd in A.8.31 met A.12.1.4**	
NIEUW A.8.28	Technisch	Veilige programmering
A.8.30	Technisch	Uitbestede ontwikkeling
A.8.29	Technisch	Beveiligingstesten in ontwikkeling en acceptatie
A.14.2.9	**Samengevoegd in A.8.29 met A.14.2.8**	
A.8.33	Technisch	Testinformatie

LEVERANCIERSRELATIES			
	A.5.19	Organisatorische controles	Informatiebeveiliging in leveranciersrelaties
	A.5.20	Organisatorische controles	Aanpakken van informatiebeveiliging binnen leveranciersovereenkomsten
	A.5.21	Organisatorische controles	Beheer van informatiebeveiliging in de supply chain van informatie- en communicatietechnologie (ICT)
	A.5.22	Organisatorische controles	Monitoring, beoordeling en change management van leveranciersdiensten
	A.15.2.2	**Samengevoegd in A.5.22 met A.15.2.1**	
NIEUW	A.5.23	Organisatorische controles	Informatiebeveiliging voor het gebruik van clouddiensten
INCIDENTBEHEER INFORMATIEBEVEILIGING			
	A.5.24	Organisatorische controles	Planning en voorbereiding van informatiebeveiligingsincidentbeheer
	A.6.8	Mensen	Rapportage van informatiebeveiligingsgebeurtenissen
	A.16.1.3	**Samengevoegd in A.6.8 met A.16.1.2**	
	A.16.1.4 A.5.25	Organisatiorische controles	Beoordeling en beslissing over informatiebeveiligingsgebeurtenissen
	A.16.1.5	A.5.26 Organisatorische controles	Reactie op informatiebeveiligingsincidenten
	A.16.1.6 A.5.27	Organisatorische controles	Leren van informatiebeveiligingsincidenten
	A.16.1.7 A.5.28	Organisatorische controles	Verzamelen van bewijsmateriaal
INFORMATIEBEVEILIGINGSASPECTEN VAN HET BEDRIJFSCONTINUÏTEITSMANAGEMENT			
	A.17.1.1 A.5.29	Organisatorische controles	Informatiebeveiliging tijdens verstoring
	A.17.1.2	**Samengevoegd in A.5.29 met A.17.1.1, A.17.1.3**	
	A.17.1.3	**Samengevoegd in A.5.29 met A.17.1.1, A.17.1.2**	
NIEUW	A.5.30	Organisatorische controles	ICT-gereedheid voor bedrijfscontinuïteit
	A.8.14	Technisch	Redundantie van informatieverwerkende faciliteiten

COMPLIANCE		
A.5.31	Organisatorische controles	Wettelijke, verplichte, regelgevende en contractuele vereisten
A.5.32	Organisatorische controles	Intellectuele eigendomsrechten
A.5.33	Organisatorische controles	Bescherming van registraties
A.5.34	Organisatorische controles	Privacy en bescherming van persoonlijk identificeerbare informatie (PII)
A.18.1.5	**Samengevoegd in A.5.31 met A.18.1.1**	
REVIEWS VAN INFORMATIEBEVEILIGING		
A.5.35	Organisatorische controles	Onafhankelijke beoordeling van informatiebeveiliging
A.5.36	Organisatorische controles	Compliance met beleidslijnen, regels en normen voor informatiebeveiliging
A.18.2.3	**Samengevoegd in A.5.36 met A.18.2.2**	

Onze ISO 27001:2022 trainings- en auditservices

Training

Vergroot uw kennis van ISO 27001:2022 met een reeks cursussen die zijn ontworpen voor verschillende ervaringsniveaus – geleverd via meerdere leerstijlen.

Gap-analyse

Een optionele service waarbij een van onze deskundige auditors u helpt bij het identificeren van kritieke, risicovolle of zwakke punten van uw systeem voorafgaand aan uw overgangsaudit.

Overgangsaudit

Wij beoordelen uw ISMS overeenkomstig de vereisten van ISO 27001:2022 – met speciale aandacht voor de controlemaatregelen in Annex A en hun impact op uw systeem.

Geïntegreerde audits

Als u meerdere management-systemen hebt geïmplementeerd, kunt u profiteren van een geïntegreerd audit- en surveillance-programma, dat efficiënter en kosteneffectief is.

Samenwerken met u om elk aspect van cybersecurity aan te pakken

Onze diepgaande ervaring in assurance, gecombineerd met bekroonde cybersecurityservices en op bedreigingen gebaseerde intelligentie, stelt ons in staat om specifieke inzichten te bieden in – en bescherming tegen – de unieke bedreigingen waarmee uw bedrijf te maken heeft. Zo blijft u cyberrisico's een stap voor, vandaag, morgen en in de toekomst.

Wij bieden audit-, trainings- en certificeringsservices volgens 's werelds toonaangevende internationale normen en standaarden, aangevuld met een breed scala aan geavanceerde cybersecurityservices geleverd door onze specialisten van Nettitude.

We werken samen met uw bedrijf om u te helpen bij het identificeren van de specifieke bedreigingen waarmee u te maken hebt en ontwikkelen strategieën om ze te beperken. Wij werken met u samen om uw systemen te certificeren, kwetsbaarheden te identificeren en aanvallen en incidenten te voorkomen die impact kunnen hebben op uw merk, financiën en activiteiten.

Informatie-beveiliging

Onze naleving- en certificeringsservices helpen u om bedrijfskritische informatie te beschermen en internationaal erkende best practices te demonstreren.

Ontdek hier meer over >

Operationele veerkracht

Bereidt u voor op het voorkomen, reageren en herstellen van verstoringen met onze certificerings-, trainings- en governance-, risico- en nalevingservices.

Ontdek hier meer over >

Bescherming tegen cyberdreigingen

Blijf cyberbedreigingen een stap voor met op maat gemaakte oplossingen die een eerste verdedigingslinie bieden en reageren op alle soorten cyberaanvallen.

Ontdek hier meer over >

Ontdek ThreatWatcher

De ThreatWatcher-service van LRQA Nettitude biedt een beheerde beoordeling met behulp van geavanceerde verkenning en analyse om voorheen onbekende bedreigingen te identificeren die kunnen worden toegepast in een cyberaanval. Beveiligingsinformatie van ThreatWatcher kan zwakke punten in de opleiding van de gebruiker(s) aan het licht brengen en helpen om digitale aanvalsvlakken beter dan ooit tevoren te identificeren. Threat Watcher van Nettitude wordt geleverd door ons team van uiterst bekwame en ervaren analisten op het gebied van Threat Intelligence en wordt aangedreven door het Recorded Future-platform.

ThreatWatcher en ISO 27001:2022

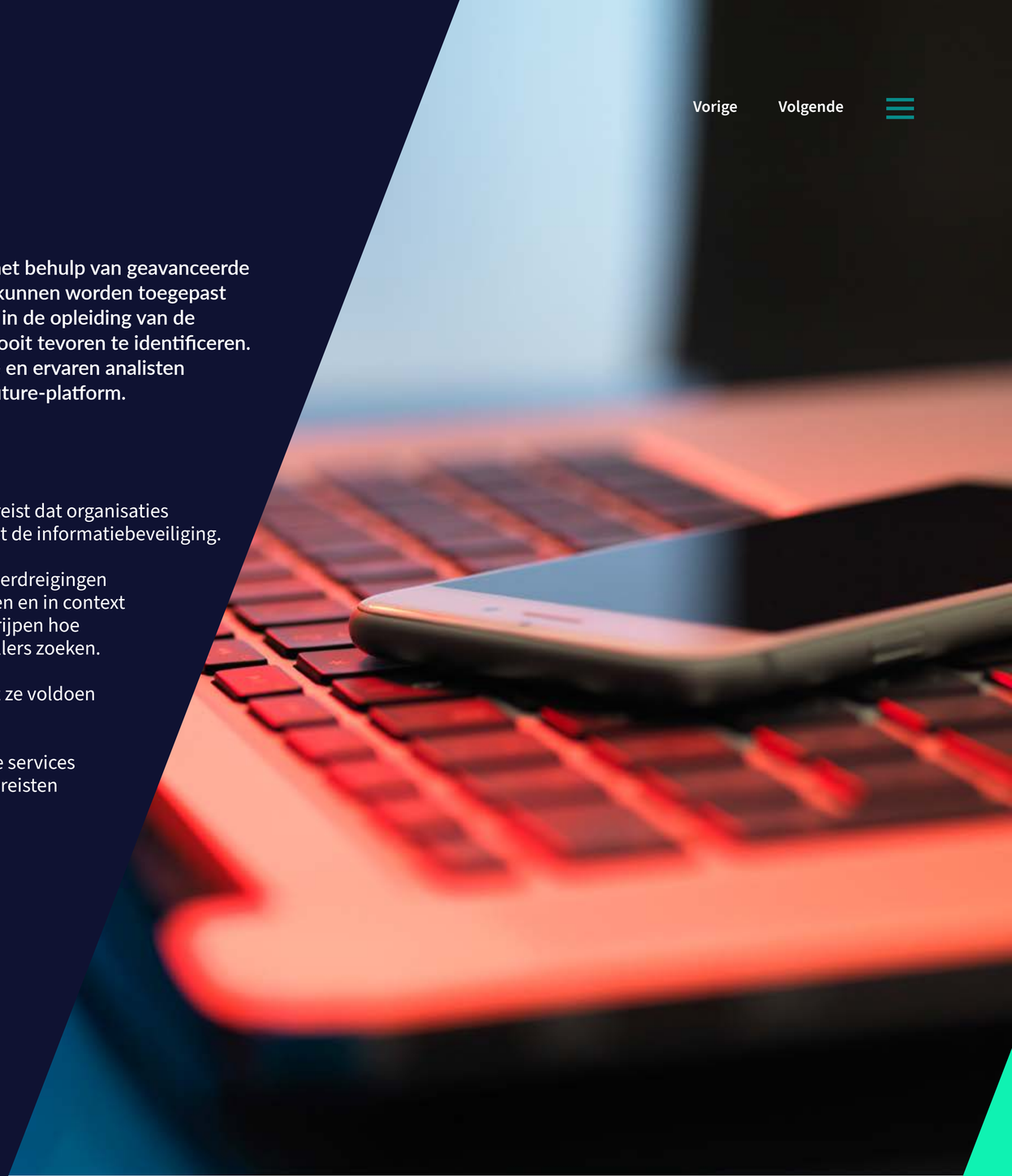
Eén van de nieuwe organisatorische controlemaatregelen, A.5.7 Threat Intelligence, vereist dat organisaties informatie over bedreigingen verzamelen, analyseren en produceren met betrekking tot de informatiebeveiliging.

Het doel van deze nieuwe controle is om organisaties een dieper inzicht te geven in cyberdreigingen door gegevens over huidige en toekomstige cyberaanvallen te verzamelen, te analyseren en in context te brengen. Daarnaast is de nieuwe controle ontworpen om organisaties te helpen begrijpen hoe hackers ze kunnen aanvallen en om bedrijven te informeren over welk type data aanvallers zoeken.

ThreatWatcher biedt deze exacte oplossingen, zodat organisaties kunnen aantonen dat ze voldoen aan de nieuwe naleving van Threat Intelligence.

Neem contact op met onze experts voor meer informatie over ThreatWatcher en andere services van LRQA Nettitude die kunnen helpen bij het aantonen van naleving met de nieuwe vereisten en controlemaatregelen die zijn geïntroduceerd in ISO 27001:2022.

Ontdek hier meer over →



YOUR FUTURE. OUR FOCUS.

Over LRQA:

LRQA combineert ongeëvenaarde expertise op het gebied van certificering, merkgarantie en training en is een van ’s werelds toonaangevende leveranciers van oplossingen voor voedselveiligheid en assurance. In samenwerking met boerderijen, visserijbedrijven, voedselproducenten, restaurants, hotels en wereldwijde retailers helpen we voedselveiligheids- en duurzaamheidsrisico’s in de hele supply chain te beheren en zijn we uitgegroeid tot een toonaangevende wereldwijde assurance provider.

We kijken met trots terug op ons verleden, maar wie we vandaag zijn, bepaalt in belangrijke mate hoe we morgen samenwerken met onze klanten. Door sterke waarden, tientallen jaren ervaring in risicomanagement en het verminderen van risico’s te combineren met een scherpe focus op de toekomst, kunnen wij onze klanten specifiek ondersteunen bij het opbouwen van betrouwbare, beter beveiligde en duurzamere business.

Van onafhankelijke audits, certificatie en training tot technisch advies services, realtime assurancetechnologie en datagestuurde transformatie van de supply chain helpen onze innovatieve end-to-end-oplossingen onze klanten om hun weg te vinden door een snel veranderend risicolandschap – zodat ze hun eigen toekomst kunnen vormgeven.

Neem contact op

Ga naar **www.lrqa.com/nl-nl/** voor meer informatie. Of stuur een e-mail naar **info.nl@lrqa.com** of bel **+31 10 899 7300**

LRQA
George Hintzenweg 77
3068 AX
Rotterdam
Nederland
Nederland