INFORMATIEBEVEILIGING MANAGEMENT SYSTEMS

ISO 27001:2022 Checklist

Bent u er klaar voor?

Gebruik onze checklist en ontdek of u voldoende voorbereid bent voor certificering.

Deze ISO 27001:2022 checklist is een waardevol hulpmiddel om u te helpen uw informatiebeveiliging managementsysteem (ISMS) te beoordelen en eventuele aandachtspunten vast te stellen vóór uw certificerings- of overgangsaudit. De checklist is opgesteld in overeenstemming met de vereisten van ISO 27001:2022 en behandelt de volgende belangrijke gebieden:

- De context van uw organisatie
- Behoeften en verwachtingen van de belanghebbenden
- Leiderschap en inzet
- Risico's en kansen
- Risicobehandeling

Door deze checklist te gebruiken, kunt u gemakkelijk een antwoord selecteren en opmerkingen geven bij elke vereiste, wat u zal helpen een volledig inzicht te krijgen in alle aspecten van uw ISMS.

Hoofdstuk 1

De context van uw organisatie

ISO 27001:2022, die de Annex SL High Level Structure volgt, benadrukt het belang van een grondige analyse van de context van uw organisatie voordat u een ISMS ontwerpt en implementeert. Deze analyse is cruciaal om de specifieke behoeften en eisen van uw organisatie te bepalen en uiteindelijk de effectiviteit van uw ISMS te waarborgen. Door de tijd te nemen om de context waarin uw bedrijf opereert volledig te begrijpen, kunt u een beter toegesneden en effectiever ISMS creëren dat gericht is op uw unieke risico's en mogelijkheden.

U kunt deze interactieve checklist gebruiken om alle vereisten die u hebt vervuld te markeren en relevante opmerkingen toe te voegen.

- [ ] U hebt de externe factoren geïdentificeerd die uw ISMS en uw vermogen om de gewenste resultaten te bereiken, kunnen beïnvloeden.

- [ ] U hebt de interne factoren geïdentificeerd die uw ISMS en uw vermogen om de gewenste resultaten te bereiken, kunnen beïnvloeden.

- [ ] U hebt rekening gehouden met de contextuele factoren (intern en extern) bij het definiëren en documenteren van het toepassingsgebied en bij het plannen van uw ISMS.

- [ ] Wijzigingen in de contextuele factoren worden periodiek geëvalueerd tijdens de Management Review.

Hoofdstuk 2
Behoeften en verwachtingen van de belanghebbenden

Volgens ISO 27001:2022 moet een ISMS rekening houden met de behoeften en verwachtingen van de betrokken partijen en hoe zij de gewenste resultaten kunnen beïnvloeden. Dit is essentieel voor het bepalen van de reikwijdte van het systeem, van operationeel tot strategisch, en het afstemmen ervan op de bedrijfsdoelstellingen van de organisatie. De organisatie moet het begrip en de verwachtingen van alle partijen onder haar controle beoordelen en hen betrekken bij de effectieve werking van het systeem.

- [ ] U hebt de behoeften en verwachtingen vastgesteld van iedereen die onder toezicht van de organisatie staat, inclusief andere belanghebbenden, en u hebt vastgesteld welke daarvan als wettelijke vereisten kunnen worden beschouwd.

- [ ] U hebt rekening gehouden met de behoeften en verwachtingen van de betrokken partijen bij het plannen van uw ISMS en het definiëren en documenteren van het toepassingsgebied.

- [ ] Degenen die onder toezicht van de organisatie staan, zijn geraadpleegd toen u de behoeften en verwachtingen van de belanghebbenden vaststelde, en deze behoeften en verwachtingen worden periodiek herzien door het management.

- [ ] U hebt de belanghebbende partijen geïdentificeerd, naast de partijen die onder de controle van de organisatie vallen, die invloed kunnen uitoefenen op uw ISMS en uw vermogen om het gewenste resultaat te bereiken.

Hoofdstuk 3
Leiderschap en inzet

ISO 27001:2022 bevat specifieke eisen met betrekking tot de manier waarop het topmanagement leiderschap moet tonen en de rol van werknemers in het ISMS. Topmanagers kunnen bepaalde taken toewijzen, maar zijn toch uiteindelijk verantwoordelijk. Hun actieve en proactieve deelname helpt om het ISMS af te stemmen op de activiteiten van het bedrijf en zorgt voor consistentie tussen het informatiebeveiligingsbeleid, de bedrijfsdoelstellingen en de bedrijfsstrategie.

- [ ] Het top management is rechtstreeks betrokken bij het bevorderen van het ISMS door het belang van naleving van het systeem te communiceren, en de bedrijfsfuncties te ondersteunen, zodat zij bijdragen tot de doeltreffendheid van het systeem.

- [ ] Het informatiebeveiligingsbeleid omvat toezeggingen om aan de informatiebeveiligingseisen te voldoen en het ISMS voortdurend te verbeteren, alsmede informatiebeveiligingsdoelstellingen (of een kader voor de vaststelling daarvan).

- [ ] U hebt de bevoegdheden en verantwoordelijkheden van de relevante rollen binnen het ISMS gedefinieerd, gecommuniceerd en gedocumenteerd.

Hoofdstuk 4
Risico’s en kansen

ISO 27001:2022 schrijft voor dat het ISMS wordt ontworpen om zowel risico’s als kansen met betrekking tot de context van de organisatie en de betrokken partijen effectief aan te pakken, binnen het toepassingsgebied van het systeem. Dit betekent dat de organisatie risico’s en kansen moet beoordelen in termen van of het managementsysteem zijn doelen en doelstellingen kan bereiken. Deze beoordeling moet verder gaan dan alleen bedreigingen voor de informatiebeveiliging en naleving van de regelgeving inzake gegevensbescherming, en moet resulteren in een plan om onaanvaardbare risico’s te beheren en geïdentificeerde kansen te benutten. De doeltreffendheid van deze acties moet regelmatig worden geëvalueerd.

- [ ] U hebt de risico’s en kansen met betrekking tot de verwachte resultaten van het ISMS bepaald.

- [ ] Bij het identificeren van risico’s en kansen heeft u rekening gehouden met de algemene bedrijfsstrategie en -doelstellingen van de organisatie, interne en externe contextuele factoren, behoeften en verwachtingen van de betrokken partijen, de levenscyclus van informatie binnen de organisatie en de reikwijdte van het ISMS.

- [ ] Risico’s en kansen worden bekeken in het kader van de vaststelling van informatiebeveiligingsdoelstellingen, de planning van het managementsysteem, de vaststelling van de behoeften inzake toezicht en meting, en de managementsbeoordelingen.

Hoofdstuk 5
Risicobehandeling

ISO 27001:2022 vereist dat een organisatie een risicobehandelingsplan opstelt en uitvoert. Dit plan moet effectief zijn in het selecteren van de juiste behandelingsmethoden en het bewaken van de effectiviteit ervan. Om de juiste selectie van controles te waarborgen, moeten deze worden vergeleken met de in bijlage A van ISO 27001:2022 geschetste best practices. Het risicobehandelingsplan moet worden goedgekeurd en aanvaard door de geïdentificeerde risico-eigenaren.

- [ ] U hebt een proces ingevoerd om passende risicobehandelingsopties te selecteren.
- [ ] U hebt processen ingevoerd om de organisatorische, menselijke, fysieke en technische controles te bepalen die nodig zijn om de behandelingsopties te implementeren.
- [ ] U hebt de controles vergeleken met bijlage A en geverifieerd dat er geen controles ontbreken.
- [ ] U hebt een verklaring van toepasselijkheid opgesteld waarin u de opneming en uitsluiting van controles rechtvaardigt.
- [ ] U hebt de toestemming van de risico-eigenaren voor het risicobehandelingsplan.

Onze ISO 27001:2022 training en audit service

Training

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

Gap analyse

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

Geaccrediteerde certificering

Een onafhankelijk proces in twee fasen dat een duidelijk beeld geeft van uw capaciteiten - en u helpt nieuwe zaken te winnen en vertrouwen op te bouwen bij belanghebbenden.

Geïntegreerde audits

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

Bekijk Trainingen →

Waarom zou u LRQA kiezen?

Lokale & wereldwijde expertise

Wij zijn overal waar u bent. Met meer dan 300 hooggekwalificeerde auditors en 250 toegewijde cyberbeveiligingsspecialisten wereldwijd kunnen wij een lokale service bieden met een wereldwijd consistente toewijding aan excellentie. Onze mensen zijn technische experts met diepgaande kennis van informatie- en cyberbeveiligingsrisico's, uitdagingen, normen, voorschriften en kaders.

Flexibele levering

In de meeste gevallen kunnen al onze ISO 27001-trainingen en certificeringsdiensten ter plaatse of op afstand worden geleverd met behulp van veilige en beveiligde technologie. Als u kiest voor levering op afstand, ontvangt u dezelfde hoogwaardige service met verschillende extra voordelen, waaronder flexibiliteit, snelle levering en toegang tot wereldwijde expertise.

Geschiedenis van primeurs

Wij waren de eersten die UKAS-accreditatie ontvingen om certificeringsdiensten te leveren voor een reeks normen over de hele wereld. Wij blijven een rol spelen bij de ontwikkeling van een reeks specifieke normen en kaders in verschillende sectoren.

Verder dan compliance

Samen met ons bekroonde cyberbeveiligingsbedrijf Nettitude kunnen wij u helpen om geavanceerde cyberdreigingen een stap voor te blijven met geavanceerde diensten die een eerste verdedigingslinie vormen en reageren op alle dreigingen en kwetsbaarheden.

Samen met u werken aan elk aspect van cyberbeveiliging

Dankzij onze ruime ervaring met assurance, gecombineerd met bekroonde diensten op het gebied van cyberbeveiliging en informatie over bedreigingen, kunnen wij inzichten op maat leveren in - en bescherming bieden tegen - de unieke bedreigingen waarmee uw bedrijf wordt geconfronteerd. 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 worden geleverd door onze specialisten van Nettitude. Wij werken samen met uw bedrijf en helpen u de 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 helpen voorkomen die gevolgen kunnen hebben voor uw merkintegriteit, financiën en activiteiten.

Informatiebeveiliging management

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

ISO 27001, ISO 27701, ISO 27017, ISO 27018, CSA STAR

Meer weten >

Operationele weerbaarheid

Wees klaar om verstoringen te voorkomen, erop te reageren en ervan te herstellen met onze certificering, opleiding en diensten op het gebied van governance, risico en compliance.

ISO 22301, ISO 20000-1, Cyber Essentials

Meer weten >

Bescherming tegen cyberdreigingen

Blijf cyberdreigingen een stap voor, met op maat gemaakte oplossingen die een eerste verdedigingslinie vormen en reageren op alle soorten cyberaanvallen.

Security Assurance Testing, Managed Security Services, Threat Intelligence, Incident Response

Meer weten >

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 of stuur een email naar info.nl@lrqa.com

LRQA Nederland
George Hintzenweg 77
3068 AX Rotterdam
Nederland