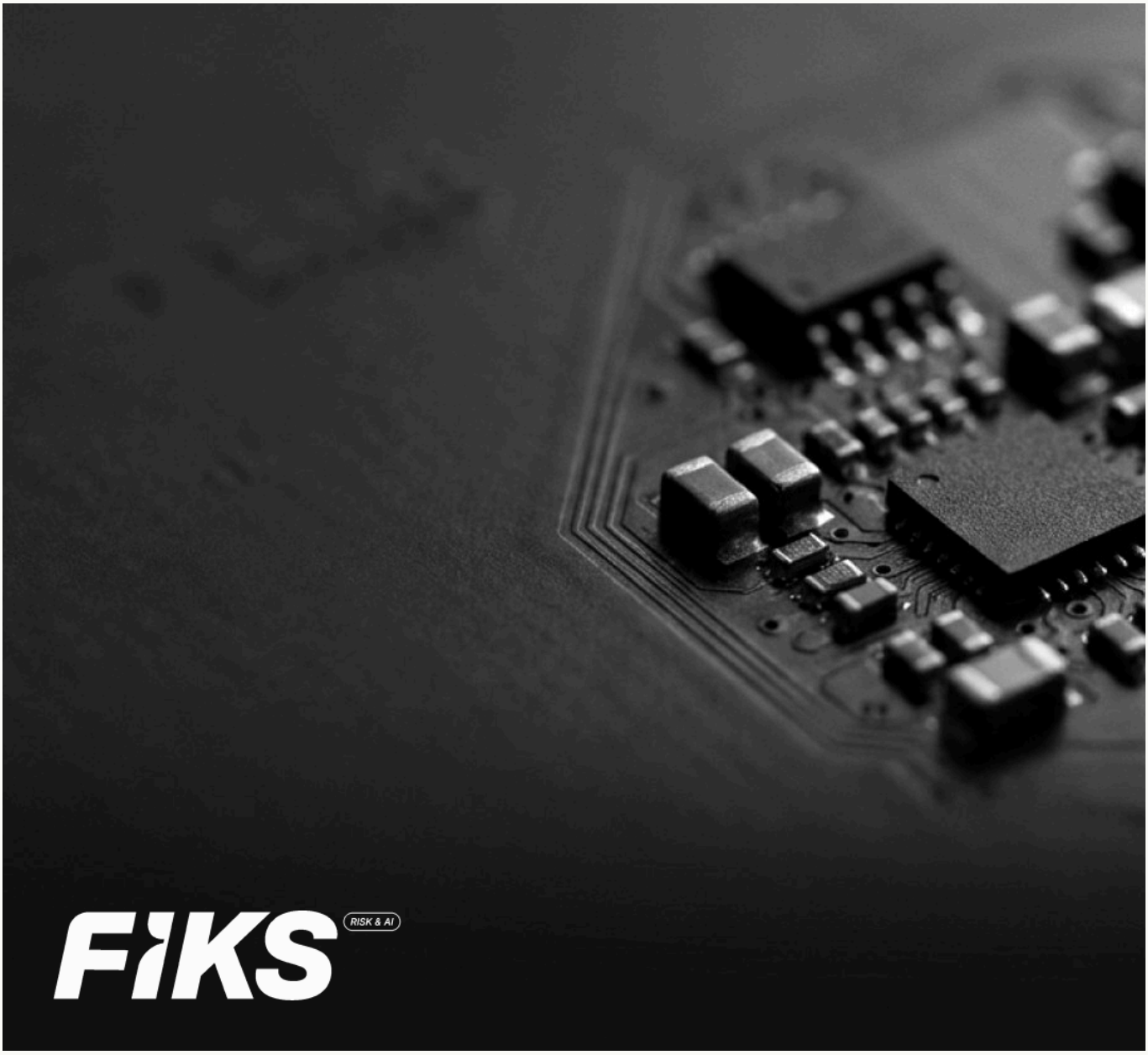
Uw klant vraagt om ISO 27001. Wie regelt het?



Steeds meer klanten en opdrachtgevers vragen om een ISO 27001-certificaat. Daarmee laat u zien dat uw informatiebeveiliging systematisch is geregeld: dat u uw risico's kent, passende maatregelen heeft genomen en die ook bijhoudt. Dat vraagt om een managementsysteem dat klopt met hoe u werkelijk werkt. Het opzetten en bijhouden daarvan komt vaak boven op het dagelijkse IT-werk.

In het kort

FIKS Risk & AI helpt u een managementsysteem voor informatiebeveiliging (ISMS) in te richten dat voldoet aan ISO 27001, met het **ISO 27001-certificaat** als resultaat. Onze specialisten doen het uitzoekwerk, stellen de documentatie op en bereiden u voor op de certificeringsaudit. De afgesproken beheersmaatregelen voeren we samen met uw team in.

Het abonnement omvat de nulmeting, de inrichting van het ISMS, de auditvoorbereiding en het onderhoud na certificering. De audit zelf wordt uitgevoerd door een onafhankelijke certificerende instelling. U krijgt een **certificeringsgarantie**, onder de voorwaarden die we op pagina 6 beschrijven.

Duidelijke afspraken tussen IT en directie

Uw IT-manager kent de systemen. ISO 27001 vraagt daarnaast nadrukkelijk om betrokkenheid van de directie: die stelt het informatiebeveiligingsbeleid vast, wijst rollen en verantwoordelijkheden toe en beoordeelt periodiek of het ISMS werkt. Daarom betrekken we de directie vanaf de start. Samen bepalen we het toepassingsgebied en wie waarover beslist.

Uit de nulmeting en de risicoanalyse volgt een werkplan waarin staat wat er moet gebeuren, wie het oppakt en wanneer het klaar moet zijn.



Waarom ISO 27001?

ISO/IEC 27001 is de internationale norm voor informatiebeveiliging. Klanten en opdrachtgevers vragen er steeds vaker om, in contracten en in aanbestedingen, omdat het certificaat laat zien dat een onafhankelijke partij uw aanpak heeft getoetst.

De norm bestaat uit eisen aan het managementsysteem en een bijlage met **93 beheersmaatregelen**, ingedeeld in de thema's Organisatie, Mens, Fysiek en Technologie. Op basis van uw risicoanalyse bepaalt u welke maatregelen van toepassing zijn. Daarnaast adviseren we u in de nulmeting of uw organisatie onder de Cyberbeveiligingswet (Cbw) valt, de Nederlandse uitwerking van NIS2. Een ISMS volgens ISO 27001 vormt daarvoor een stevige basis.

Uw klanten en opdrachtgevers

Vragen om aantoonbare informatiebeveiliging

Uw organisatie zelf

Valt u onder de Cyberbeveiligingswet?

Specialisten die het werk uit handen nemen

De dienst is bedoeld voor organisaties die hun informatiebeveiliging met een ISO 27001-certificaat moeten aantonen en daarvoor onvoldoende capaciteit in huis hebben. Onze specialisten plannen het werk, voeren het uit en houden het bij. Uw team levert de benodigde informatie en beslist mee over de beheersmaatregelen.

Een eis van een klant, een tender of de komst van NIS2 kan de aanleiding zijn. De eisen en termijnen die daarbij horen, bepalen waar we beginnen.

De aanleiding

Klanteis
Tender
NIS2

Dit zit in het abonnement

Nulmeting	Inrichting ISMS	Auditvoorbereiding	Onderhoud

Nulmeting en risicoanalyse	We bepalen samen het toepassingsgebied, brengen de belangrijkste systemen, gegevens en leveranciers in kaart en toetsen de huidige situatie aan ISO 27001. In de risicoanalyse bepalen we welke risico's er zijn, hoe groot ze zijn en hoe u ze behandelt. Daaruit volgt een werkplan met prioriteiten.
ISMS inrichten en verklaring van toepasselijkheid	We stellen het informatiebeveiligingsbeleid op en leggen in de verklaring van toepasselijkheid vast welke van de 93 beheersmaatregelen voor u gelden, en waarom. Daarna helpen we uw team de gekozen maatregelen in te voeren. Ook maken we een incidentplan dat we samen oefenen. De taken en bewijsstukken houden we overzichtelijk bij. Nieuwe Vogels verzorgt de uitvoering op het gebied van informatiebeveiliging. Privacy- en juridische vragen binnen de opdracht leggen we voor aan FIKS Legal.
Interne audit en directiebeoordeling	Voor de certificeringsaudit begeleiden we de interne audit, die toetst of het ISMS werkt zoals beschreven. In de directiebeoordeling bespreekt uw directie de resultaten en besluit zij over verbeteringen. Beide zijn een eis van de norm.
Auditvoorbereiding	We stellen het bewijsdossier samen, bereiden uw team voor op beide fasen van de certificeringsaudit en zijn tijdens de audit beschikbaar voor toelichting.
Onderhoud en jaarlijkse surveillance-audit	Het certificaat is drie jaar geldig, met elk jaar een surveillance-audit. We houden de risicoanalyse, de verklaring van toepasselijkheid en de documentatie actueel, herhalen jaarlijks de interne audit en de directiebeoordeling en bereiden u voor op de surveillance-audits en de hercertificering.

Niet in het abonnement: de audit zelf	FIKS Risk & AI voert de certificeringsaudit nadrukkelijk **niet** zelf uit. De audit wordt uitgevoerd door een onafhankelijke, erkende certificerende instelling. Wij werken samen met een vaste auditpartner die wij u kunnen voorstellen. De kosten van de audit worden apart begroot en zijn voor uw rekening.

Certificering met garantie

Wij garanderen dat uw organisatie de audit doorstaat en het **ISO 27001-certificaat** behaalt. Dat is een stevige toezegging, en daar staat een stevige inzet van uw organisatie tegenover. De garantie geldt alleen als u aan alle onderstaande voorwaarden voldoet:

- u voert alle maatregelen uit die wij adviseren, volledig en binnen de termijnen uit het werkplan;
- u levert de gevraagde informatie en bewijsstukken tijdig en volledig aan;
- u stelt een vaste contactpersoon beschikbaar en zorgt dat betrokken medewerkers meewerken;
- u wijkt niet zonder overleg met ons af van de afgesproken aanpak.

Kortom: wij bepalen wat er moet gebeuren, u zorgt dat het gebeurt.

Als de audit niet slaagt

Haalt u de audit onverhoopt niet terwijl aan de voorwaarden is voldaan, dan passen wij ons advies, de documentatie en het bewijsdossier aan op de bevindingen van de auditor en begeleiden we de heraudit **zonder extra advieskosten**.

Het doorvoeren van ontbrekende of onjuiste technische maatregelen blijft de verantwoordelijkheid van uw organisatie. De kosten van de certificerende instelling voor de heraudit zijn voor uw rekening.

Wat het certificaat aantoont

Het certificaat toont aan dat uw ISMS binnen het afgesproken toepassingsgebied voldoet aan ISO 27001. Of u ook aan alle toepasselijke wettelijke verplichtingen voldoet, vraagt een afzonderlijke beoordeling.

Uw inzet en de kosten

Uw inzet

Van uw organisatie vragen we een vaste contactpersoon en voldoende tijd om informatie aan te leveren en maatregelen door te voeren. Hoeveel tijd dat is, schatten we in tijdens de nulmeting en leggen we vast in het werkplan.

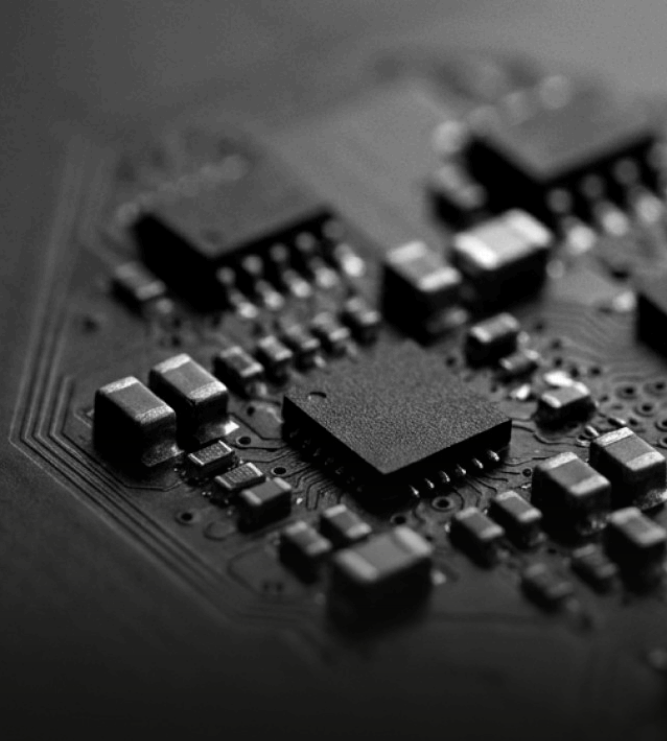
Wij verzorgen de planning en bewaken de voortgang. Besluiten over budget en verantwoordelijkheden blijven bij uw directie.

De kosten

Abonnement	ISO 27001-certificering (ISO/IEC 27001:2022)
Prijs	Op basis van uw omvang, het aantal locaties en het toepassingsgebied
Niet inbegrepen	De certificeringsaudit (via onze auditpartner, apart begroot), licenties, technisch beheer en de afhandeling van een daadwerkelijk incident

Offerte

De prijs hangt af van uw omvang, het aantal locaties en het toepassingsgebied van het ISMS. De exacte werkzaamheden, prijs, looptijd en opzegtermijn vindt u in de offerte.



Vragen over dit voorstel?

Wij lichten de offerte graag toe. Nodig daarvoor bij voorkeur uw IT-verantwoordelijke en de collega die over het budget beslist uit, zodat we ook de planning en haalbaarheid kunnen bespreken.

Wie wij zijn

FIKS Risk & AI is een samenwerking van RSafe, Nieuwe Vogels en FIKS Legal. Nieuwe Vogels voert de informatiebeveiliging uit, FIKS Legal adviseert over privacy en juridische vragen en RSafe is uw aanspreekpunt.



Rob Buddingh
FIKS Risk & AI

robb@rsafe.eu
+31 6 1208 5538