



# OFFERTE CIS CONTROLS

Organisatie: Humankind  
T.a.v. de heer Keulen  
Postbus 591, 6400 AN Heerlen

Aangeboden via: E-mail

Datum: 9 oktober 2024

Dit document mag niet worden verspreid of gekopieerd zonder toestemming van NFIR B.V.

---



## Inhoudsopgave

CIS Center for Internet Security® .....	2
NFIR is SecureSuite member van CIS.....	2
De CIS Controls® .....	3
Opdrachtschrijving .....	3
Plan van aanpak.....	4
CIS Controls Self Assessment Tool (CIS CSAT PRO) en rapportage .....	4
Vereiste documenten voor de start .....	5
Tarieven en projectkosten .....	5



Geachte de heer Keulen,

Op dinsdag 9 oktober 2024 spraken wij tijdens de aangenane meeting met u Richard Kranendonk over de mogelijke beveiligingsmaatregelen die uw organisatie zou kunnen nemen om de kans op een IT-Security Incident en de impact daarvan te verkleinen. Dit kan door gebruik te maken van een security framework om de staat van de IT-security aantoonbaar op orde te krijgen. Door gebruik te maken van een erkend security framework zoals de CIS Controls maakt u voor uw eigen organisatie (en voor externe stakeholders zoals de accountant, toezichthouders en klanten) inzichtelijk wat de status van de beveiliging van uw IT-omgeving is. De Security consultants van NFIR helpen uw organisatie met het inrichten van deze CIS Controls die Humankind wil implementeren.

In deze offerte treft u een korte uitleg over de organisatie CIS (Center for Internet Security), de CIS Controls, de opdrachtomschrijving, het plan van aanpak en de vereisten voor de start van dit project. Tot slot treft u een urenrekening van dit CIS Controls adviesproject, de CSAT PRO tool die wij hierbij leveren en onze tarieven.

## CIS Center for Internet Security®

Het Center for Internet Security, Inc. (CIS) maakt de digitale wereld een veiligere plek voor mensen, bedrijven en overheden door middel van hun kerncompetenties samenwerking en innovatie. CIS is een door de gemeenschap gedreven non-profitorganisatie, verantwoordelijk voor de CIS Controls en CIS Benchmarks, wereldwijd erkende best practices voor het beveiligen van IT-systemen en gegevens. CIS leidt een wereldwijde gemeenschap van IT-professionals om deze normen voortdurend te ontwikkelen en producten en diensten te leveren om proactief te beschermen tegen opkomende bedreigingen. De CIS Hardened Images bieden veilige, on-demand, schaalbare computeromgevingen in de cloud.

## NFIR is SecureSuite member van CIS

NFIR B.V. is officieel secureSuite member van het CIS en maakt daarbij gebruik van de middelen die aan de SecureSuite members ter beschikking zijn gesteld om daarmee onze opdrachtgevers te kunnen voorzien van de beste gestandaardiseerde IT beveiligingsinformatie toegespitst op uw organisatie. De totstandkoming van deze standaarden uit de diverse middelen is volledig transparant en met medewerking van duizenden IT-security professionals wereldwijd ontwikkeld. Voor uw organisatie biedt dit een aantal voordelen waaronder:

- Gebruik van een open framework dat door een wereldwijde gemeenschap wordt onderhouden
- Geen vendor specifieke beveiligingsstandaarden
- Een toetsbare inrichting met op risico-analyse gebaseerde, vooraf gedefinieerde activiteiten
- Gebruik van diverse tools zoals de CIS WorkBench en CSAT PRO (Controls Self Assessment Tool)



## De CIS Controls®

De CIS Controls zijn een aanbevolen reeks acties voor cyberverdediging die specifieke en bruikbare manieren bieden om zich te verdedigen tegen de meest voorkomende aanvallen. De ondersteuning met CIS Controls is bedoeld om organisaties te helpen om snel het startpunt voor hun IT-security beleid te definiëren, de (schaarse) middelen te richten op acties die onmiddellijk waarde toevoegen aan de algehele IT-beveiliging en vervolgens hun aandacht en middelen te richten op aanvullende risico kwesties. De CIS-controls worden samengesteld door informatie uit daadwerkelijke aanvallen en effectieve verdedigingen. Ze weerspiegelen de gecombineerde kennis van experts uit elk deel van het ecosysteem (bedrijven, overheden, individuen); met elke rol (threat responders en analisten, technologen, ethisch hackers, toolmakers, solution providers, verdedigers, gebruikers, beleidsmakers, auditors, enz.); en binnen vele sectoren die de handen ineen hebben geslagen om de controls te creëren, toe te passen en te ondersteunen. CIS beveelt organisaties aan om prioriteit te geven aan de implementatie van de controles door gebruik te maken van de Implementation Groups (IG's):

- IG1 - Een organisatie met beperkte middelen en verantwoordelijk voor gegevens met een lage gevoeligheid valt doorgaans onder IG1.
- IG2 - Een organisatie met matige middelen en een beveiligingsteam om gevoelige klant- of bedrijfsinformatie te beheren valt onder IG2.
- IG3 - Een zeer volwassen organisatie met aanzienlijke middelen en ervaring op het gebied van cyberbeveiliging valt onder IG3.

Zie bijlage “CIS Critical Security Controls\_v8” voor meer informatie over de Critical Security Controls, de Implementation Groups en de daarbij behorende “Safeguards” (maatregelen).

## Opdrachtomschrijving

Humankind heeft ervoor gekozen om de hulp van Security Consultants van NFIR in te zetten voor de totstandkoming van een CIS Controls assessment. Het doel van deze opdracht is om middels de maatregelen verbonden aan CIS Controls niveau IG1 en of IG2 Humankind te helpen om op een pragmatische manier het startpunt en prioritering van het security beleid en alle bijbehorende maatregelen vorm te geven.

Humankind kan met de uitkomst van dit assessment gerichte acties binnen de eigen organisatie uitzetten om daarmee het security beleid verder vorm te geven. NFIR zal gebruik maken van de CSAT PRO (Controls Self Assessment Tool) die voor Humankind 2 jaar beschikbaar blijft om te gebruiken. Indien uw organisatie na deze periode de CSAT tool wil blijven gebruiken dan kan dat.



## Plan van aanpak

Dit CIS Controls adviestraject wordt uitgevoerd door Security Consultants en bestaat uit 5 fases. Hieronder treft u de vijf fases met een korte beschrijving per fase:

- **Fase 1: Inventarisatie en assessment**  
Tijdens de inventarisatiefase wordt op basis van beschikbare informatie en interviews met uw organisatie inzicht verkregen in het huidige beleid en reeds genomen maatregelen in relatie tot de CIS Controls v8.
- **Fase 2: Vastleggen van het security beleid, alle genomen en nog te nemen maatregelen in CSAT tool**  
Tijdens deze fase wordt het huidige security beleid en alle genomen en nog te nemen maatregelen volgens het CIS Controls framework vastgelegd en beoordeeld.
- **Fase 3: Analyse en prioritering van nog te nemen maatregelen**  
Er zal aan de hand van een score een gewogen lijst worden opgesteld zodat duidelijk wordt welke sub-controls de hoogste prioriteiten hebben voor uw organisatie. Deze “roadmap” wordt geprioriteerd op basis van organisatie relevante eisen zoals tijd, budget, complexiteit, impact op de organisatie, eisen vanuit een certificering, etc.
- **Fase 4: Rapportage, overdracht en oplevering CSAT tool**  
Tijdens deze fase zullen de Security Consultants een pragmatische rapportage opstellen met de belangrijkste bevindingen van dit adviestraject. Dit rapport zal tijdens een toelichting worden doorgenomen. Daarna zal de CSAT tool overgedragen worden aan de betrokkenen zodat deze zelf in gebruik kunnen nemen.
- **Fase 5: Nazorg vanuit de Security Consultants**  
Na de oplevering van de rapportage en overdracht van de CSAT tool zullen onze Security Consultants binnen 12 maanden 2 maal contact opnemen om de voortgang te bespreken en vragen te beantwoorden om uw organisatie vooruit te helpen. Indien gewenst kunnen de Security Consultants additionele ondersteuning bieden.

## CIS Controls Self Assessment Tool (CIS CSAT PRO) en rapportage

De CIS Controls Self Assessment Tool (CIS CSAT) helpt NFIR en uw organisatie bij het vastleggen, beoordelen, volgen en prioriteren van de maatregelen van de CIS Controls v8. NFIR zal voor Humankind een eigen CSAT omgeving creëren zodat deze tool gebruikt kan worden gedurende het adviestraject en door uw organisatie gedurende minimaal 24 maanden (en langer indien gewenst). De belangrijkste bevindingen tijdens deze advies opdracht worden gedocumenteerd in een heldere en beknopte rapportage. Na oplevering van het rapport organiseert NFIR samen met Humankind een toelichtingsmoment. De rapportage zal op uw verzoek worden uitgebracht in de Nederlandse taal. De rapportage zal worden opgeleverd via de beveiligde SharePoint deelopgeving.



## Vereiste documenten voor de start

De volgende documenten en informatie zijn vereist voor het uitvoeren van deze opdracht:

- Een getekende versie van deze offerte
- Een getekende geheimhoudingsverklaring. Zie bijlage
- Gegevens van de personen die na afloop van de opdracht de rapportage dienen te ontvangen:

Naam	E-mailadres

## Tarieven en projectkosten

BESCHRIJVING VAN DE WERKZAAMHEDEN	TOTAAL
CIS controls	€ 18.250,-
Optioneel: fee per jaar voor gebruik CSAT tool na 24 maanden	€ 500,-

\* De werkzaamheden per fase kunnen verschillen per opdracht. Indien het geheel van de werkzaamheden meer dan 10% afwijkt van het totaal aantal uren dan worden deze uren op nacalculatie doorbelast. Mocht dit het geval zijn dan zullen de betrokken Security Consultants u hiervan tijdig op de hoogte stellen.

De geldigheidsduur van deze offerte bedraagt 30 dagen na offertedatum. Op deze aanbieding zijn de Algemene Verkoopvoorwaarden NFIR (v2.1 maart 2024) van toepassing. Deze zijn als bijlage bij deze offerte toegevoegd. Bij de start van het project zal 50% van deze offerte gefactureerd worden. De overige 50% wordt gefactureerd bij oplevering van de rapportage. Alle genoemde tarieven zijn excl. BTW. Deze offerte is 30 dagen geldig. De betalingstermijn is 14 dagen netto.



Mochten er naar aanleiding van deze offerte nog vragen zijn of heeft u de behoefte aan een toelichting, dan vernemen wij dat uiteraard graag. Indien u akkoord gaat met deze offerte, dan verzoeken wij u de getekende versies van deze offerte en de geheimhoudingsverklaring retour aan te bieden. Zodra wij uw officiële akkoord ontvangen, zullen wij de werkzaamheden van deze opdracht samen met u inplannen.

Nogmaals dank voor uw aanvraag en wij kijken er naar uit om deze opdracht te mogen uitvoeren.

Met vriendelijke groet,

Voor akkoord,

**NFIR B.V.**

S. van den Braak  
Accountmanager  
9 oktober 2024

**Humankind**

Naam:  
Functie:  
Datum: