CYRA

hoe pak ik CYRA in de keten aan?

versie: 8 mei 2026

Evelien Bras

Inhoudsopgave

Inleiding

Dit document belicht wat CYRA is en geeft een overzicht van de positionering ten opzichte van de NIS-2 / cyberweerbaarheidswet. Aangezien CYRA is afgeleid van ISO27001 en niet van de wet (die op dit moment nog niet is aangenomen), is er een delta in compliancy.

CYRA is derhalve idealiter wel te gebruiken voor leveranciersmanagement. Dit document beschrijft stappen die je kunt nemen om meer grip te krijgen op de mate van cyberweerbaarheid van jouw toeleveranciers en partners met behulp van CYRA.

Het beschrijft:

- Wat is CYRA
- Een checklist voor toepassing
- Het beschrijft een aantal opties voor het bepalen van het wensniveau
    - Kraljic methode
    - Punten-methode
    - Op basis van classificatie van gedeelde informatie
- Naar welke organisaties kun je doorverwijzen voor support?
- Hoe toets ik het wensniveau?

In de bijlage aan deze memo is meer achtergrondinformatie over CYRA te vinden, waaronder het overzicht van de onderwerpen voor de controls en een voorbeeld van een certificaat.

Voor vragen kun je terecht bij de organisatie via welke je toegang tot CYRA hebt verkregen, zoals bijvoorbeeld Cyberweerbaarheidscentrum Brainport, FERM, MKB Cyber Campus, Z-CERT, FME, Metaalunie, CCV (Centrum voor Criminaliteitspreventie en Veiligheid) of natuurlijk “The Cyber Partners”.

Met ingang van medio augustus 2025 zal het CCV een nieuwe versie van de tooling lanceren. Zie ook bijgevoegde infosheet in bijlage voor informatie over de overgang.

Wat is CYRA?

Cyra staat voor Cyber Rating en is een uniforme aanpak te komen tot een certificeerbaar niveau voor informatiebeveiliging. CYRA definieert een aantal stappen die voor MKB bereikbaar zijn, in opmaat naar ISO 27001. ISO 27001 is een internationale standaard voor informatiebeveiliging. Niet voor ieder bedrijf is het haalbaar om meteen een volledig ISO 27001-certificaat te halen; dat hoeft ook niet. Met CYRA kun je een deelcertificaat halen, waarmee je aan je klanten kunt aantonen wat je doet op het vlak van cyberweerbaarheid.

Cyra is voor organisaties:

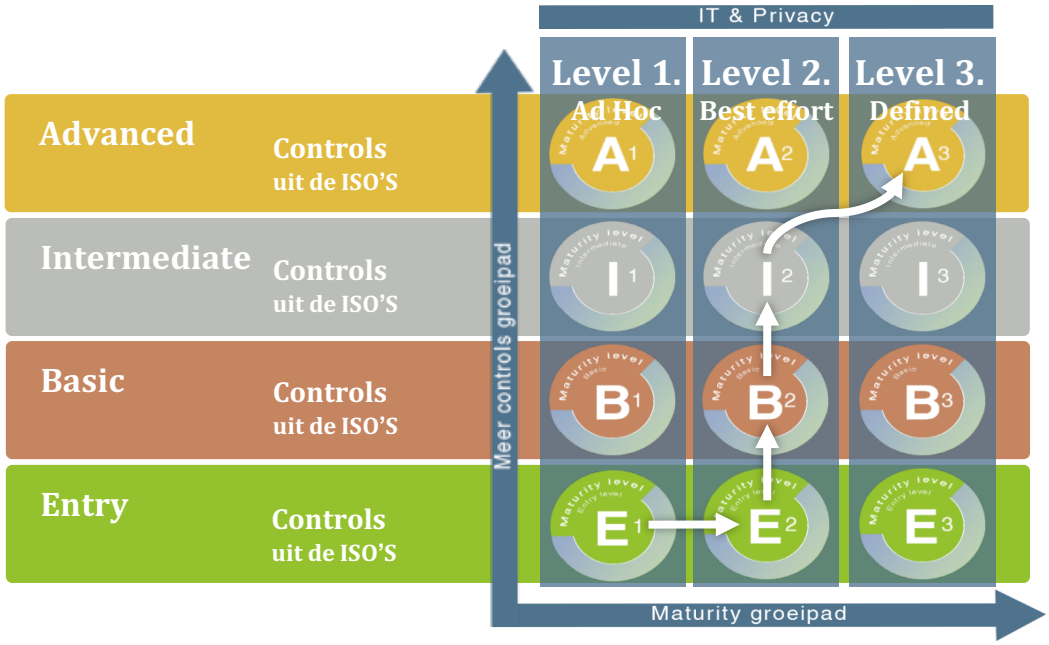
- aan de ene kant voor organisaties voor wie een ISO 27001-certificaat te veel gevraagd is, maar die toch op een manier met cyberbeveiliging aan de slag willen waarbij zij hun niveau onafhankelijk en betrouwbaar aantoonbaar willen maken.
- aan de andere kant voor organisaties, die het in willen zetten voor de keten.

Wil je garanties hebben van je leveranciers, maar is een volledig ISO 27001-certificaat momenteel nog wat te veel gevraagd van hen? Vraag dan een CYRA-certificaat, waarmee je in ieder geval over een aantal basiselementen garanties krijgt. Met het CYRA-certificaat heeft een organisatie een soort “rijbewijs” waarmee zij kan aantonen welke vaardigheden zij in welke mate beheerst.

Daarnaast zijn er organisaties zoals samenwerkingsverbanden en branches die organisaties zoals hierboven kunnen helpen om hun doelstellingen te halen. Ook zijn er toetsingsorganisaties die CYRA kunnen gebruiken om het niveau van hun achterban, branche of sector inzichtelijk te maken.

Twaalf tredes: CYRA kent twaalf tredes

In afbeelding 1 staat de matrix met twaalf CYRA tredes waarop gecertificeerd kan worden. De tredes variëren van instapniveau E1 tot en met het geavanceerde niveau A3. Als een organisatie het level A3 heeft gehaald, is het nog maar een kleine stap naar volledige ISO 27001 certificering.



Checklist voor gebruik CYRA in de keten.

Voor het gebruik van CYRA in de keten zijn er verschillende disciplines in een organisatie betrokken:

- business
- inkoop
- legal

We zien dat een CISO/office veelal coördinerend optreedt, bijvoorbeeld als gevolg van de vraag van het management op "NIS-2 compliancy[1]" na te streven. Hierbij nemen ze ook de rol van vertaling van de verschillende disciplines op zich.

De aansturing van de keten gaat in drie stappen.

1. Bepalen wensniveau

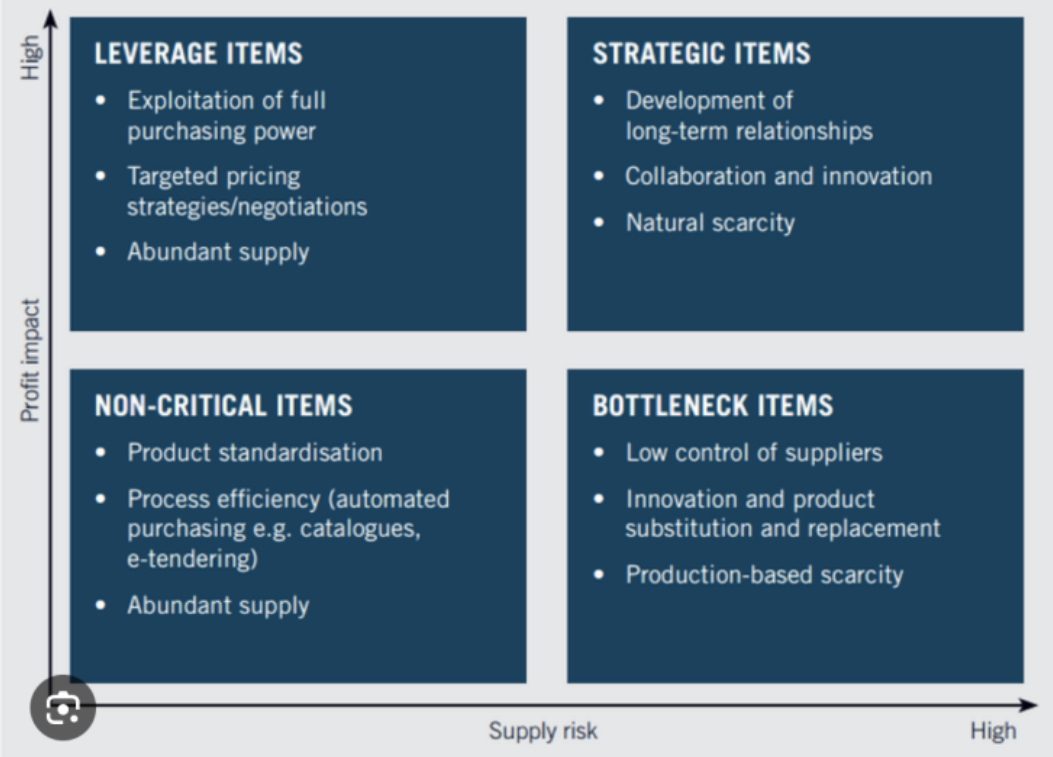
Ten eerste moet de gewenste trede van een leverancier/partner bepaald worden. Deze gewenste trede is natuurlijk sterk afhankelijk van je business afhankelijkheid en de relatie met de desbetreffende leverancier. Hieronder staan drie voorbeelden van een aanpak voor het bepalen van het wensniveau.

Bepaling gaat per organisatie waar een relatie mee is. Let op: CYRA is alleen bedoeld voor die organisaties in de keten voor wie ISO27001 (of: IEC62443) een stap te ver is. Voor organisaties waar je bijzonder van afhankelijk bent, raden we aan om geen CYRA trede te eisen, maar het ISO certificaat zelf.

[1] NIS-2 is weliswaar de naam van de Europese richtlijn en niet de wetgeving. Daarnaast is het in Nederland geïmplementeerd als open norm. "NIS-2 compliancy" is daarmee een niet helemaal juiste term, echter wordt het in veel organisaties wel zo genoemd, vandaar dat we dat in dit document zo volgen.

De Kraljic methode

Op basis van het risico en impact kan hier een analyse gemaakt worden. Zie voor een voorbeeld van de Kraljic matrix. Onderstaande matrix.



Op basis van punten voor diverse invalshoeken

Onderstaand model geeft op basis van een punten-score een advies voor entry, basic, intermediate of advanced. Deze punten worden gegeven voor gewenste integriteit, vertrouwelijkheid, beschikbaarheid in combinatie met de omvang van de organisatie.

Onderwerp	**Waardering**	**Score:**
Integriteit: Hoe schadelijk is het verlies van juistheid en/of de volledigheid van informatie, al dan niet ten gevolge van ongewenste aanpassingen?	Laag: 1 punt Middel: 2 punten Hoog: 3 punten	
Vertrouwelijkheid: Hoe schadelijk is het verlies van exclusiviteit van informatie ten gevolge van ongeautoriseerde toegang of inzage?	Laag: 1 punt Middel: 2 punten Hoog: 3 punten	
Beschikbaarheid: Hoe schadelijk is het verlies van controle over toegang tot informatie of het ongewenst kwijtraken van informatie?	Laag: 1 punt Middel: 2 punten Hoog: 3 punten	
Welk type gegevens wordt er door de organisatie verwerkt?	algemene persoonsgegevens, zoals namen, (e-mail)adressen etc: 1 punt algemene persoonsgegevens en geen bedrijfskritische gegevens : 2 punten bijzondere persoonsgegevens (gezondheid, religie etc.) en/of bedrijfskritische gegevens: 3 punten	
Uit hoeveel locaties bestaat de onderneming?	1: 1 punt 2-4: 2 punten >4: 3 punten	
Wordt er gebruik gemaakt van cloud services?	mail en sharepoint: 1 punt niet-kritische applicaties: 2 punten meer: 3 punten	
Hoeveel locaties zijn er buiten de EU?	Geen: 1 punt 1-2: 2 punten >2: 3 punten	
Hoeveel medewerkers heeft de organisatie?	1-4: 1 punt 5-99: 2 punten 100+: 3 punten	
Hoeveel systemen zijn publiek benaderbaar vanaf internet	1-3: 1 punt 4-6: 2 punten >6: 3 punten	

De totale score bepaalt het wensniveau:

9:	entry level
10 tot en met 15:	basic level
16 tot en met 20:	intermediate
21 of meer:	advanced

Op basis van classificatie van gedeelde informatie

Als de relatie met de toeleveranciers vooral gaat over de gedeelde data, kan het beste gekeken worden naar het wensniveau van de classificatie van de gedeelde informatie:

- Voor organisaties die met name publiek beschikbare informatie verwerken (dus geen vertrouwelijk intellectueel eigendom of privacygevoelige informatie van de klant) is niveau E (Entry) afdoende.

- Voor organisaties waarbij informatie bij voorkeur wel veilig moet worden opgeslagen, maar waarbij het geen ramp is als er af en toe eens iets in verkeerde handen komt, of wordt aangepast, is niveau B (Basic) afdoende.

- Organisaties die vertrouwelijke informatie verwerken, zoals vertrouwelijke ontwerpen of receptuur van een klant of persoonsgegevens, is niveau I (Intermediate) vereist.

- Voor een hoger wensniveau is niveau A (Advanced) vereist.

Maturity in de vier control-sets: Ad-hoc, best effort of defined?

Naast de hoeveelheid controls (Entry, Basic, Intermediate of Advanced) is er een 'maturity'as.

Deze maturity-as wordt veelal gebruikt voor organisaties om hun eigen groei te monitoren. Voor de aantoonbaarheid in de keten adviseren we per definitie "defined".
Immers zegt "ad hoc" of "best effort" niet zo heel veel en is de waarde van een onafhankelijke toetsing op die maturity niveau's niet erg groot.

2. Het wensniveau neerleggen

Ten tweede moet het wensniveau gesteld worden. Dit is een effort van inkoop en legal.

Het vastleggen kan door middel van inkoopcontracten of in de algemene voorwaarden. Hierbij adviseren we om de 'right to audit van een geldig CYRA certificaat – Level: Entry level, Maturity: Defined – in de algemene bepalingen van de algemene voorwaarden op te nemen. Een hoger wensniveau kan in specifieke contracten verwerkt worden.

Voorbeeld algemene voorwaarden:

> *Partijen zullen alle redelijke maatregelen treffen ter bescherming van elkaars belangen in het kader van integriteit, vertrouwelijkheid en beschikbaarheid van de informatie en diensten. , integriteit en beschikbaarheid van en zullen deze informatie niet aan derden bekend maken, behoudens voor zover dit noodzakelijk is voor de uitvoering van de overeenkomst of indien zij daartoe wettelijk verplicht zijn.*

Enkele aandachtspunten voor contracten:

- Definities en scope; omvat het certificaat de scope van het contract?
- Geldt het certificaat voor de specifieke locatie waarmee je zaken doet?
- Overleg of je eventueel de ingevulde gegevens wilt zien van je leverancier/partner. Deze gegevens zijn vertrouwelijk tussen organisatie en de certificerende instantie maar soms wil je in voorkomende gevallen hier toch meer inzage in. Dit gaat dan via de onderlinge bedrijfsrelatie en moet derhalve opgenomen worden in het contract.
- De 'risk appetite' van uw toeleverancier/partner – de risico's die voor hem wel of niet acceptabel zijn – hoeven niet dezelfde te zijn als voor jouw organisatie.
  Maak een link tussen de aansprakelijkheid voor jouw bedrijfsrisico's. Hoe ga je om met gevolgschade, indirecte schade?
  Dit zal de kosten/baten analyse van de te nemen maatregelen voor uw toeleverancier/partner beïnvloeden. Een certificeringsinstantie kan niet toetsen wat niet is afgesproken.
- Hoe lang geldt deze verplichting? Ook na oplevering/uitvoering van het contract of beëindiging van de overeenkomst?
- Maak in de contracten de maatregelen rondom beveiliging zo specifiek mogelijk, bijvoorbeeld over uptime of de snelheid van het installeren van patches. Of over het beschikbaar stellen van backups en snelheid in het opnieuw kunnen opbouwen van een capability. Het CYRA certificaat is een start, het beschrijven van specifieke casussen en duidelijke en meetbare KPI's is een logisch gevolg.

3. Informeren over toegang en support

Ten derde moeten toeleveranciers/partners weten waar ze terecht kunnen voor toegang en support. Immers wil je als afnemer niet per definitie de vragen van de keten beantwoorden. Daar zijn samenwerkingsorganisaties voor ingericht.

Toegang:

> Partners / leveranciers kunnen zich aanmelden op https://app.cyberrating.nl/ Deze site is ook in het Engels beschikbaar.Tegen administratieve kosten kan gebruik gemaakt worden van de tool.

Support:

> Support om op een bepaald niveau te komen kan bij een samenwerkingsorganisatie of partner (zoals The Cyber Partners).

Certificering:

> Als je als organisatie op basis van het self-beoordeling het idee heeft dat het gewenste niveau is bereikt (beschermingsniveau E-B-I-A en volwassenheidsniveau 1-2-3) kunt u een onafhankelijke en daartoe gemachtigde certificeringsinstantie[2] vragen om je organisatie te toetsen voor formele certificering op het gewenste niveau.
>
> Dit officiële certificaat is twee jaar geldig. Er bestaat de mogelijkheid om tussentijds een hercertificering te laten doen voor een hoger niveau (hoger in beschermingsniveau E-B-I-A of hoger in volwassenheidsniveau 1-2-3).

[2] Bijvoorbeeld TÜV Nord.

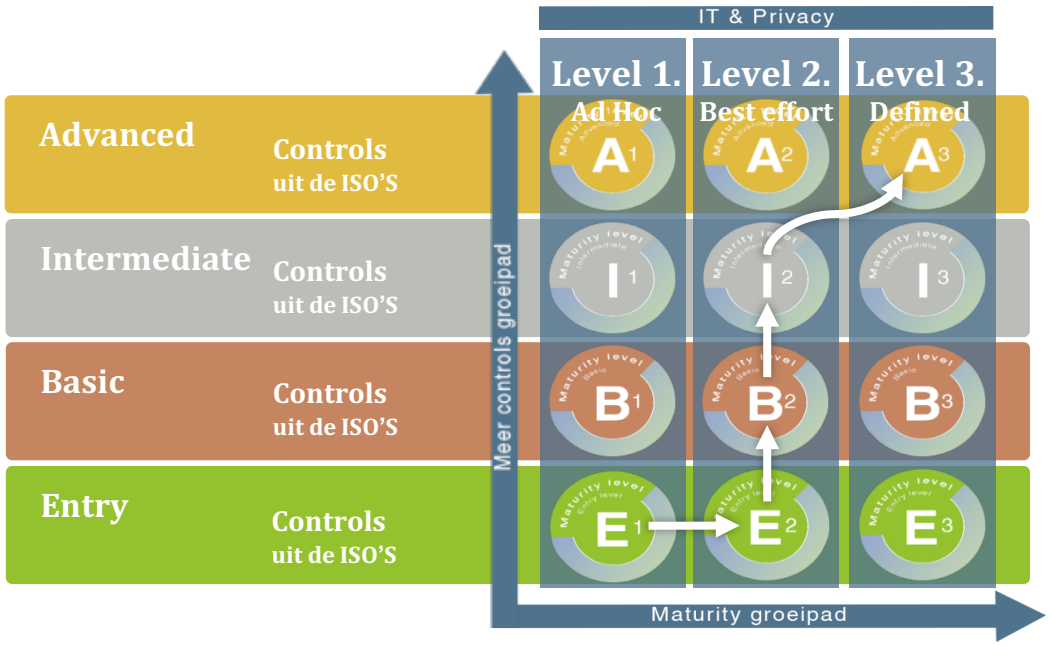
Hoe toets ik de status van de toeleveranciers/partners?

Door het certificaat of zelfverklaring op te vragen van de desbetreffende toeleverancier/partners. Let hierbij op de geldigheid van het certificaat.

Hier zit enorm veel tijdsbesparing. Je hoeft niet zelf een vragenlijsten bij te houden en te controleren, of vragen van je partners te beantwoorden. Daar zijn andere partijen voor, zoals CYRA, CCV, brancheorganisaties, samenwerkingsverbanden en certificeringsinstanties.

Jij bent 'regisseur' van de keten.

BIJLAGE: Achtergrondinformatie CYRA



De twaalf tredes bestaan uit vier beschermingsniveaus (verticaal afgebeeld in afbeelding 1): Entry, Basic, Intermediate en Advanced, en drie volwassenheidsniveaus: Ad hoc, Best effort en Defined.

Het volwassenheidsniveau wordt bepaald door de mate van zekerheid die je wilt hebben over hoe goed de organisatie de ISO-maatregelen naleeft (horizontaal afgebeeld in afbeelding 1).

- Niveau 1: Ad hoc. De ISO 27001 maatregelen die behoren bij het beschermingsniveau worden ad-hoc toegepast door de organisatie. Het is onvoorspelbaar; de prestatie is afhankelijk van de capaciteiten van individuen die de taken uitvoeren en varieert met de vaardigheden, kennis en motivatie die zij bezitten.
- Niveau 2: Best effort. De ISO 27001 maatregelen die behoren bij het beschermingsniveau zijn vastgesteld, geïmplementeerd en worden zo veel mogelijk nageleefd.
- Niveau 3: Defined. De ISO 27001 maatregelen die behoren bij het beschermingsniveau zijn vastgesteld, binnen de hele organisatie geïmplementeerd en onder controle.

Addendum I - Sectorale eisen

CYRA heeft zich volop doorontwikkeld. Zo is is samen met FERM Rotterdam een normenkader voor digitale ondermijning ontwikkeld. En samen met Z-CERT wordt een add-on op het standaard framework ontwikkeld die op maat is voor NEN7510, specifiek voor de zorg. Daarnaast heft het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) de ontwikkeling van een CYRA-model voor cyberweerbaarheid van Industrial Control Systems (ICS) of OT (Operationele Technologie) op basis van IEC62443/BIACS ontwikkeld.

Addendum II – Voorbeeld certificaat

Een certificaat is 2 jaar geldig. Er bestaat natuurlijk de mogelijkheid om tussentijds aan te passen: om voor een ander niveau gecertificeerd te worden.

Het CYRA-certificaat wordt gezien als een basis ‘rijbewijs’ om aan te tonen dat vaardigheden aanwezig zijn. Het is dus mogelijk om CYRA-certificaat aan te vullen met sectorspecifieke eisen.

Let op:

onderstaand voorbeeld is een TÜV NORD voorbeeld. Medio 2025 wordt dit format vervangen door een CCV voorbeeld, gebruikt door meerdere certificerende instanties.

TÜVNORD

Pagina 1 van 1

Certificaat

TÜVNORD
TÜV NORD Nederland B.V.
CYRA
tuv.nl

voor de cyberweerbaarheid volgens

CYRA 3 levels: Basic

Level: 1. Ad hoc

Branche / samenwerkingsverband: Cyberweerbaarheidscentrum Brainport

De certificatie instelling TÜV NORD Nederland bevestigt hiermee dat de evaluatie heeft plaatsgevonden volgens haar certificatiereglement voor de organisatie

<<naam bedrijf>>

De cyberweerbaarheid is onafhankelijk beoordeeld en voldoet aan de eisen van de norm.
De certificatie is onderworpen aan een driejaarlijkse evaluatie door TÜV NORD Nederland.

Toepassingsgebied

"De minimaal op volwassenheidsniveau Ad hoc implementatie van de van toepassing zijnde bij CYRA Basic behorende en beheersmaatregelen."

Registratienummer 17917-2

Certificaat geldig van 23-05-2023
Certificaat geldig tot 22-05-2026
Datum eerste certificatie 23-05-2023

Dhr. E.W.A.C. Franken
Managing Director

TÜV NORD Nederland B.V.
Ekkersrijt 4401, 5692 DL Son en Breugel
tuv.nl

TÜV®

CYRA CYBER RATING

TÜVNORDGROUP

(updaten iom Herman ?)

Addendum III – ISO 27001 Maatregelen per beschermingsniveau

CYRA bestaat uit de controls van ISO 27001 in combinatie met ISO 27701 (privacy). Op de volgende pagina staat een overzicht van de ISO 27001 maatregelen per beschermingsniveau.

De controls zijn volledig uitgeschreven beschikbaar op https://hetccv.nl//app/uploads/2024/12/20241230-CCV-CYRA-controls-2.2-DEF.pdf

Voor meer informatie over de controls, zie: https://hetccv.nl//app/uploads/2024/12/20241230-CCV-CYRA-controls-2.2-DEF.pdf

de controls