



CCV centrum voor
criminaliteitspreventie en
veiligheid

CCV-certificatieschema Cyber Rating – CYRA

Versie 2.0

Publicatiedatum: 1 november 2025

Ingangsdatum: 1 januari 2026

Voorwoord

Dit certificatieschema volgt de relevante eisen conform ISO/IEC 17021-1 voor managementsystemen gericht op de beoordeling van digitale weerbaarheidsniveaus (Cyber Rating). Het heeft vier scopes:

- CYRA-IT – digitale weerbaarheid van organisaties;
- CYRA-NDO – weerbaarheid van organisaties tegen digitale ondermijning;
- CYRA-Zorg – digitale weerbaarheid van organisaties in de zorg;
- CYRA-OT – digitale weerbaarheid van organisaties die Operationele Technologie (OT) gebruiken.

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is beheerder van het certificatieschema. De Commissie van Belanghebbenden Cybersecurity heeft positief geadviseerd over vaststelling en publicatie van dit schema.

© 2025. Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B van de Auteurswet 1912 jo het besluit van 20 juni 1974, St.b. 351, zoals gewijzigd bij het besluit van 23 augustus 1985, St.b. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 882, 1180 AW Amstelveen). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

All rights reserved. No part of this book may be reproduced, stored in a database or retrieval system, or published, in any form or in any way, electronically, mechanically, by print, photo print, microfilm or any other means without prior written permission from the publisher.

Ondanks alle aan de samenstelling van deze uitgave bestede zorg, kan het Centrum voor Criminaliteitspreventie en Veiligheid geen aansprakelijkheid aanvaarden voor eventuele schade die zou kunnen voortvloeien uit enige fout die in deze uitgave zou kunnen voorkomen.

Inhoud

1	Inleiding	5
1.1	Algemeen	5
1.1.1	Introductie	5
1.1.2	Doel	5
1.1.3	Verantwoordelijkheden	6
1.1.4	Leeswijzer	6
1.2	Toepassingsgebied	7
1.3	Relatie met wet- en regelgeving	7
1.4	Relatieschema	8
1.5	Overgangsbepalingen	8
1.5.1	Voor certificaathouders voor deelgebieden A en B	8
1.5.2	Voor certificatie-instellingen	9
1.6	Wijzigingen ten opzichte van de vorige versie	9
2	Eisen aan weerbaarheidsniveaus	10
2.1	Algemeen	10
2.1.1	Toetsingskader CYRA	10
2.1.2	Eisen aan de digitale weerbaarheid van een organisatie (CYRA-IT)	10
2.1.3	Eisen aan de weerbaarheid van een organisatie tegen digitale ondermijning (CYRA-NDO)	10
2.1.4	Eisen aan de digitale weerbaarheid van een organisatie in de zorg (CYRA-Zorg)	10
2.1.5	Eisen aan de digitale weerbaarheid van OT (CYRA-OT)	10
2.2	Eigen beoordeling	10
3	Certificatievoorwaarden	12
3.1	Algemeen	12
3.2	Aanvraag van certificatie	12
3.2.1	Online beoordelingsinstrument	12
3.2.2	Gegevens bij aanvraag	12
3.2.3	Status gedurende de aanvraag	13
3.3	Instandhouding van het certificaat	13
3.3.1	Handhaven weerbaarheidsniveau	13
3.3.2	Wijzigingen	13
3.4	Wijziging van niveau	13
3.5	Voortzetting van certificatie	14
4	Eisen aan de uitvoering van certificatie	15
4.1	Algemeen	15
4.2	Eisen aan de certificatie-instelling	15
4.2.1	Algemeen	15
4.2.2	Relatie met – en gebruik van ISO/IEC 17021-1	15
4.2.3	Communicatie met de organisatie	16
4.3	Eisen aan de uitvoering	16
4.3.1	Kwalificaties	16
4.3.2	Behandeling aanvraag	18
4.3.3	Uitvoering beoordelingen	18
4.3.4	Klachten en beroep	21
4.3.5	Publicatie	21
4.4	Herstel van afwijkingen	21
4.4.1	Corrigerende maatregelen	21

4.4.2	Beoordeling van herstel door de certificatie-instelling	21
4.5	Schorsing	22
4.5.1	Schorsen	22
4.5.2	Gevolgen van schorsing	22
4.5.3	Opheffen van een schorsing	22
4.6	Intrekking	22
4.6.1	Intrekken	22
4.6.2	Gevolgen van intrekking	22
4.6.3	Nieuwe aanvraag	23
5	Certificatiemerken en certificaten	24
5.1	Certificatiemerken	24
5.1.1	Merken	24
5.1.2	Gebruik van het merken door de certificatie-instelling	25
5.1.3	Gebruik van het merken door de organisatie	25
5.2	Certificaat voor het weerbaarheidsniveau	25
5.2.1	Algemeen	25
5.2.2	Certificaat digitale weerbaarheidsniveau voor deelgebieden A (CYRA – IT) en C (CYRA- Zorg)	26
5.2.3	Aanvullende verklaring over de weerbaarheid tegen digitale ondermijning volgens deelgebied B (CYRA – NDO)	26
5.2.4	Certificaat digitale weerbaarheidsniveau voor deelgebied D (CYRA – OT)	27
6	Verwijzingen	29
6.1	Wet- en regelgeving	29
6.2	Begrippen en afkortingen	29
6.3	Normen en normatieve verwijzingen	30
Bijlage A	Overzicht CYRA beoordelingsniveaus en levels	32
A.1	Toetsingskader digitale weerbaarheid (deelgebied A)	32
A.2	Toetsingskader weerbaarheid tegen digitale ondermijning (deelgebied B)	33
Bijlage B	Inhoudsopgave Toetsingskader CYRA	36
B.1	Algemeen	36
B.2	Inhoudsopgave Toetsingskader CYRA-IT niveau Entry	36
B.3	Inhoudsopgave Toetsingskader CYRA-IT niveau Basic	37
B.4	Inhoudsopgave Toetsingskader CYRA-IT niveau Intermediate	38
B.5	Inhoudsopgave Toetsingskader CYRA-IT niveau Advanced	39
B.6	Inhoudsopgave Normkader Digitale Ondermijning	40
B.7	Inhoudsopgave Toetsingskader CYRA-Zorg niveau Entry	41
B.8	Inhoudsopgave Toetsingskader CYRA-Zorg niveau Basic	41
B.9	Inhoudsopgave Toetsingskader CYRA-Zorg niveau Intermediate	41
B.10	Inhoudsopgave Toetsingskader CYRA-Zorg niveau Advanced	41
B.11	Inhoudsopgave Toetsingskader CYRA-OT niveau Entry	42
B.12	Inhoudsopgave Toetsingskader CYRA-OT niveau Basic	43
B.13	Inhoudsopgave Toetsingskader CYRA-OT niveau Intermediate	45
B.14	Inhoudsopgave Toetsingskader CYRA-OT niveau Advanced	46
Bijlage C	Volwassenheidslevels	48

1 Inleiding

1.1 Algemeen

1.1.1 Introductie

De beveiliging van informatiesystemen, computers en geautomatiseerde systemen is complex. De schade als gevolg van digitale kwetsbaarheden kan voor het midden- en kleinbedrijf (mkb) zeer groot zijn. Financiële schade, verlies van bedrijfsgegevens of productiecapaciteit en imagoschade komen regelmatig voor.

Het is de eigen verantwoordelijkheid van de ondernemer om de risico's voor de bedrijfscontinuïteit te beheersen en zich zo goed mogelijk weerbaar te maken tegen cyberaanvallen of andere dreigingen. Als onderdeel van toeleveringsketens mag hij dat ook van ketenpartners verwachten, net zoals die rekenen op de digitale weerbaarheid van de ondernemer.

In veel gevallen kan de ondernemer niet volstaan met de implementatie van technische maatregelen ten behoeve van de digitale basisveiligheid. Ook op organisatieniveau zijn maatregelen nodig om de organisatie weerbaar te maken tegen digitale dreigingen. Weerbaarheid gaat niet alleen over het voorkomen, maar ook over het beheersen van de gevolgen van cyberincidenten.

Onderdeel van cybersecurity is periodieke risico-inventarisatie, evaluatie (assessment) van de digitale weerbaarheid, en het nemen van maatregelen om de digitale weerbaarheid van de organisatie te verhogen.

Goede methoden zijn opgenomen in de norm ISO/IEC 27001 voor informatiebeveiliging en de daarvan afgeleide normserie NEN 7510 (IT) en in de normserie IEC 62443 voor operationele technologie (OT). Deze zijn goed toepasbaar in grotere organisaties, ook in internationaal verband vanwege de brede acceptatie. Maar voor het midden- en kleinbedrijf kan de stap naar ISO 27001-, NEN 7510- of IEC 62443-niveau groot zijn, waardoor organisaties een drempel ervaren om hun digitale weerbaarheid op orde te brengen. Dit terwijl opdrachtgevers in de keten onder invloed van wet- en regelgeving steeds vaker bewijs vragen dat de toeleverancier voldoende aandacht heeft besteed aan zijn digitale weerbaarheid.

Om organisaties te helpen met versterking van hun digitale weerbaarheid is er een assessment- en certificatiemodel beschikbaar: Cyber Rating, afgekort CYRA. Dit model is gebaseerd op ISO/IEC 27001 en ISO/IEC 27701 voor IT-systemen, voor organisaties in de zorgsector op de van ISO 27001 afgeleide normserie NEN 7510, en voor organisaties met OT-systemen op deel 2-1 en deel 3-3 van de IEC 62443-serie. CYRA biedt organisaties een duidelijk omschreven pad om te groeien naar de breedte en de volwassenheid die nodig zijn om aan die normen te voldoen.

1.1.2 Doel

Het doel van cybersecurity is het weerbaar maken van een organisatie tegen cyberdreigingen en de mogelijke schadelijke effecten daarvan. Dit gebeurt door het nemen van organisatorische, mensgerichte, technische en fysieke informatiebeveiligingsmaatregelen. Voorbeelden van kaders hiervoor zijn de normen ISO/IEC 27001 en ISO/IEC 27701, de NEN 7510-serie en de IEC 62443-serie. Het doel van deze maatregelen is om schade te voorkomen en, als die toch optreedt, deze zoveel mogelijk te beperken. Daarmee wordt de bedrijfscontinuïteit gewaarborgd.

Het doel van het assessment- en certificatiemodel Cyber Rating (CYRA) is om organisaties te ondersteunen bij het bepalen van hun actuele niveau van digitale weerbaarheid. Criteria hiervoor zijn afgeleid van de eerdergenoemde normen. CYRA helpt organisaties desgewenst ook bij het bepalen van hun weerbaarheid tegen digitale ondermijning (NDO) of de digitale weerbaarheid van hun

operationele technologie. Daarnaast biedt het model inzicht in het groeipad naar het gewenste niveau van digitale weerbaarheid.

Het doel van het bepalen van het niveau van digitale weerbaarheid van organisaties (op het vlak van IT inclusief NDO, OT en Zorg) is om de organisatie inzicht te geven in de huidige staat van haar digitale weerbaarheid. Desgewenst kan dit ook inzicht bieden in de weerbaarheid tegen digitale ondermijning of de digitale weerbaarheid van OT. Daarnaast stelt dit proces de organisatie in staat om, waar nodig, in stappen kwetsbaarheden en risico's te verminderen, weg te nemen of te vermijden. Op die manier kan de organisatie haar digitale weerbaarheid versterken, evenals haar weerbaarheid tegen digitale ondermijning en de digitale weerbaarheid van OT.

Het doel van het onafhankelijk certificeren van het niveau van digitale weerbaarheid is het onderbouwen van het vertrouwen in de eigen beoordeling die de organisatie heeft gemaakt. Dit geldt voor de beoordeling van de digitale weerbaarheid, de weerbaarheid tegen digitale ondermijning en digitale weerbaarheid van OT. Onafhankelijke certificering helpt bovendien om de faal- en risicokosten voor derden te verminderen. Deze kosten kunnen namelijk optreden als de veronderstelde digitale weerbaarheid, weerbaarheid tegen digitale ondermijning of OT- weerbaarheid in werkelijkheid ontbreekt.

Een CYRA-certificaat stelt de organisatie in staat om – op basis van zowel de eigen ambities als de eisen van opdrachtgevers – het bereikte niveau van digitale weerbaarheid of weerbaarheid tegen digitale ondermijning of digitale weerbaarheid van OT inzichtelijk te maken en daarover te rapporteren.

Het vastleggen van de niveaus van digitale weerbaarheid afgeleid van de normen ISO/IEC 27001 en ISO/IEC 27701, NEN 7510-serie en de IEC62443-serie, de niveaus van weerbaarheid tegen digitale ondermijning en de digitale weerbaarheid van OT, en de werkwijzen gehanteerd door de certificatie-instelling voor de beoordeling daarvan, heeft als doel:

- het bieden van een herkenbare methode voor bepaling van digitale weerbaarheid, weerbaarheid tegen digitale ondermijning en digitale weerbaarheid van OT;
- het waarborgen van een geharmoniseerde en consistente uitvoering;
- het informeren van de markt over de wijze waarop certificatie van digitale weerbaarheidsniveaus en niveaus van weerbaarheid tegen digitale ondermijning en digitale weerbaarheid van OT is ingericht en wordt uitgevoerd.

1.1.3 Verantwoordelijkheden

De organisatie is verantwoordelijk voor het uitvoeren van het assessment van:

- haar digitale weerbaarheid, en/of
- haar weerbaarheid tegen digitale ondermijning, en/of
- haar digitale weerbaarheid van haar OT.

Daarnaast is de organisatie verantwoordelijk voor de definitie en implementatie van de beheersmaatregelen op het gewenste niveau.

1.1.4 Leeswijzer

De in dit certificatieschema opgenomen eisen en voorwaarden worden gehanteerd bij de behandeling van een aanvraag van een certificaat voor het digitale weerbaarheidsniveau, het niveau van weerbaarheid tegen digitale ondermijning en voor het digitale weerbaarheidsniveau van OT van een organisatie.

Het certificatieschema bevat:

- De eisen aan de digitale weerbaarheidsniveaus en de weerbaarheid tegen digitale ondermijning en de digitale weerbaarheidsniveaus van OT (hoofdstuk 2);
- De voorwaarden voor certificatie (hoofdstuk 3);

- Geharmoniseerde werkwijzen die de certificatie-instelling moet hanteren bij de behandeling van een certificatieaanvraag (hoofdstuk 4);
- Beschrijving van het certificaat dat de certificatie-instelling afgeeft aan de organisatie en het toe te passen certificatiemerk (hoofdstuk 5).

1.2 Toepassingsgebied

Het toepassingsgebied van dit certificatieschema betreft certificatie van de volgende deelgebieden:

- A. CYRA-IT: het digitale weerbaarheidsniveau van een organisatie, onderverdeeld in de niveaus Entry, Basic, Intermediate en Advanced, en per niveau naar volwassenheidslevel Ad Hoc (1), Best Effort (2) en Defined (3), bedoeld voor organisaties waarvoor de normen ISO/IEC 27001 en ISO/IEC 27701 nog geen praktische oplossing bieden, maar die inzicht willen of moeten hebben in hun digitale weerbaarheidsniveau.
- B. CYRA-NDO: de weerbaarheid van een organisatie tegen digitale ondermijning naar volwassenheidslevel Ad Hoc (1), Best Effort (2) en Defined (3), in combinatie met de digitale weerbaarheid van die organisatie volgens deelgebied A of C op minimaal niveau Entry in volwassenheidslevel Ad Hoc (1).
- C. CYRA-Zorg: het digitale weerbaarheidsniveau van een organisatie in de zorg, onderverdeeld in de niveaus Entry, Basic, Intermediate en Advanced, en per niveau naar volwassenheidslevel Ad Hoc (1), Best Effort (2) en Defined (3), bedoeld voor organisaties waarvoor de normserie NEN 7510 nog geen praktische oplossing biedt, maar die inzicht willen of moeten hebben in hun digitale weerbaarheidsniveau.
- D. CYRA-OT: het digitale weerbaarheidsniveau van OT, onderverdeeld in de niveaus Entry, Basic, Intermediate en Advanced, en per niveau naar volwassenheidslevel Ad Hoc (1), Best Effort (2) en Defined (3), bedoeld voor organisaties waarvoor de delen 2-1 en 3-3 van de normserie IEC 62443 nog geen praktische oplossing bieden, maar die inzicht willen of moeten hebben in het digitale weerbaarheidsniveau van hun operationele technologie.

Bijlage A bevat een overzicht van het toepassingsgebied.

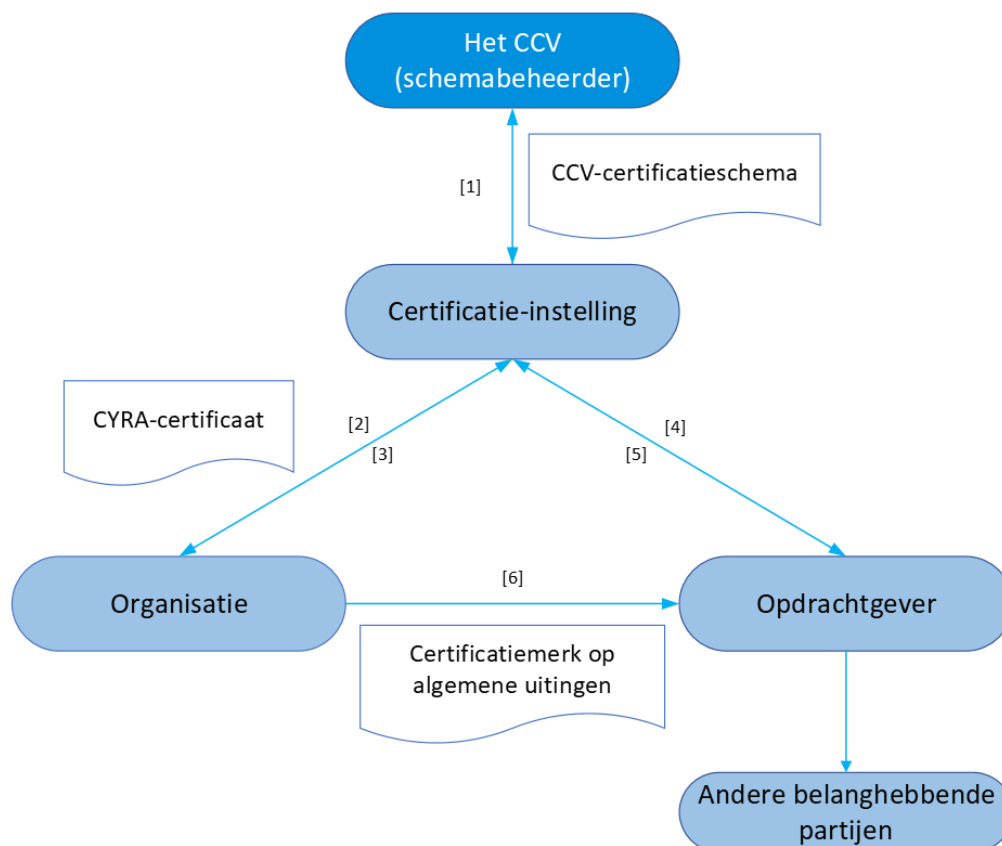
Organisaties kunnen zich voor een of meer deelgebieden laten certificeren. Certificatie voor deelgebied B is slechts mogelijk in combinatie met deelgebied A of C.

Certificatie-instellingen kunnen een licentie voor het certificatieschema afsluiten voor het gehele schema, of voor het deelgebied waarvoor zij certificatiecontracten willen afsluiten. Een licentie voor deelgebied A en/of deelgebied C is inclusief deelgebied B. De certificatie-instelling kan geen beoordelingen uitvoeren buiten de licentie.

1.3 Relatie met wet- en regelgeving

Het certificatieschema wordt niet aangestuurd vanuit wet- en regelgeving. Het certificatieschema is privaatrechtelijk en heeft geen wettelijke grondslag.

1.4 Relatieschema



Figuur 1 – Overzicht van partijen betrokken bij certificatie van digitale weerbaarheidsniveaus en niveaus van weerbaarheid tegen digitale ondermijning en voor digitale weerbaarheidsniveaus van OT

Legenda:

- [1] De certificatie-instelling heeft een licentieovereenkomst met het CCV (§ 4.1.1).
- [2] De organisatie bepaalt het niveau van digitale weerbaarheid en/of weerbaarheid tegen digitale ondermijning en/of het digitale weerbaarheidsniveau van OT (hoofdstuk 2) en vraagt certificatie aan (§ 3.2).
- [3] De certificatie-instelling beoordeelt het niveau van digitale weerbaarheid en/of weerbaarheid tegen digitale ondermijning en/of het digitale weerbaarheidsniveau van OT dat de organisatie heeft bepaald voor zijn organisatie (hoofdstuk 4).
- [4] Het CYRA-certificaat spreekt naar de markt onderbouwd vertrouwen uit.
- [5] Opdrachtgevers kunnen klachten die door de organisatie niet naar behoren behandeld worden bij de certificatie-instelling indienen.
- [6] De organisatie past het certificatiemerk op algemene uitingen toe als aan de gestelde eisen voldaan wordt. Gebruik van het certificatiemerk op producten en diensten is niet toegestaan.

1.5 Overgangsbepalingen

1.5.1 Voor certificaathouders voor deelgebieden A en B

Versie 2.0 van het certificatieschema gaat in op 1 januari 2026 en certificaathouders voor de deelgebieden A en B zijn verplicht vanaf die datum versie 2.0 te volgen. Deelgebieden C en D zijn nieuw; hiervoor geldt geen overgangsregeling.

Het certificatieschema mag worden toegepast vanaf de datum van publicatie.

1.5.2 Voor certificatie-instellingen

Een licentie voor versie 1.0 gaat op ingangsdatum over in een licentie voor deelgebieden A en B van versie 2.0. Versie 1.0 vervalt op 1 juli 2026 en de certificatie-instellingen nemen daarna geen certificatiebeslissingen meer volgens versie 1.0.

Versie 2.0 moet vanaf ingangsdatum worden toegepast voor nieuwe certificatie-aanvragen. Certificatie-instellingen die een licentie hebben voor versie 1.0 kunnen certificatie-aanvragen behandelen voor deelgebieden A en B. Certificatie-aanvragen voor de deelgebieden B en D kunnen behandeld worden als de certificatie-instelling met het CCV een uitbreiding van de licentie voor die deelgebieden is overeengekomen.

Een eventuele extra beoordeling moet vanaf 1 januari 2026 op alle eisen van versie 2.0 plaatsvinden. Hierbij gelden de bepalingen zoals weergegeven in paragraaf 4.3.3.4.

1.6 Wijzigingen ten opzichte van de vorige versie

De belangrijkste wijzigingen in versie 2.0 ten opzichte van versie 1.0 zijn:

- Het toepassingsgebied in 1.2 is uitgebreid met deelgebied C (CYRA-Zorg) en deelgebied D (CYRA-OT). De teksten in het Voorwoord en diverse paragrafen in Hoofdstuk 1 zijn hierop aangepast;
- Cyberweerbaarheid is als term vervangen door digitale weerbaarheid;
- In 1.5 is een overgangsregeling toegevoegd voor certificaathouders en certificatie-instellingen;
- In 2.1 zijn de eisen aan de deelgebieden C (CYRA-Zorg) en D (CYRA-OT) toegevoegd;
- In 2.2 is nader gespecificeerd dat het online CCV-zelfbeoordelingsinstrument CYRA moet worden gebruikt als basis voor certificatie;
- De strekking van hoofdstukken 3, 4 en 5 is aangepast in verband met de verbreding van het toepassingsgebied van het schema naar CYRA-Zorg en CYRA-OT;
- In 4.3.1.2 zijn kwalificatie-eisen toegevoegd voor certificatiepersoneel dat ingezet wordt voor CYRA-OT;
- De kwalificatie-eisen in 4.3.1.2 voor CYRA-IT zijn aangepast in lijn met wijzigingen in ISO 27006;
- In 4.3.3.1 is de tijdsbesteding voor beoordeling van CYRA-OT toegevoegd;
- In 5.1 zijn de certificatiemerken voor CYRA-Zorg en CYRA-OT toegevoegd, en in 5.2 de bepalingen voor gebruik daarvan. Daarnaast zijn de eisen aan de certificatieverklaring en de inhoud van de certificaten aangepast;
- In 6.2 zijn begrippen en afkortingen toegevoegd in verband met de verbreding van het toepassingsgebied van het schema naar CYRA-Zorg en CYRA-OT;
- In 6.3 zijn normatieve verwijzingen toegevoegd in verband met de verbreding van het toepassingsgebied van het schema naar CYRA-Zorg en CYRA-OT;
- Bijlage A is uitgebreid met overzichten van de beoordelingsniveaus voor CYRA-Zorg (onderdeel A.3) en CYRA-OT (onderdeel A.4);
- Bijlage B is uitgebreid met de inhoudsopgave van de toetsingskaders CYRA-Zorg (deelgebied C) en CYRA-OT (deelgebied D).

2 Eisen aan weerbaarheidsniveaus

2.1 Algemeen

2.1.1 Toetsingskader CYRA

De eisen voor certificatie zijn vastgelegd in het Toetsingskader CYRA.

Het Toetsingskader CYRA heeft betrekking op de digitale weerbaarheid van de organisatie (2.1.2), op de weerbaarheid van de organisatie tegen digitale ondermijning (2.1.3), op de digitale weerbaarheid van de organisatie in de zorg (2.1.4) en de digitale weerbaarheid van de organisatie met OT (2.1.5).

Het CCV publiceert de volledige tekst van de beheersmaatregelen en de te behalen volwassenheidslevels op de website www.hetccv.nl. Deze is opgenomen in het online CCV-zelfbeoordelingsinstrument op <https://cyberrating.nl/>. Ten behoeve van eenduidige koppeling met dit certificatieschema is in Bijlage B de inhoudsopgave van het online zelfbeoordelingsinstrument vermeld. De versie op <https://cyberrating.nl/> is maatgevend.

2.1.2 Eisen aan de digitale weerbaarheid van een organisatie (CYRA-IT)

De eisen aan de digitale weerbaarheid van de organisatie zijn afgeleid van de eisen uit de normen ISO/IEC 27001 en ISO/IEC 27701, en verbijzonderd naar vier niveaus: Entry, Basic, Intermediate en Advanced. Elk niveau is onderverdeeld in drie volwassenheidslevels. Bijlage C geeft een specificatie van de drie volwassenheidslevels 1. Ad Hoc, 2. Best effort en 3. Defined.

2.1.3 Eisen aan de weerbaarheid van een organisatie tegen digitale ondermijning (CYRA-NDO)

De eisen aan de weerbaarheid van de organisatie tegen digitale ondermijning zijn een specifieke invulling van eisen uit de norm ISO/IEC 27001, aangevuld met eisen aan bedrijfsprocessen die voor het versterken van de weerbaarheid tegen digitale ondermijning van belang zijn. De eisen aan de weerbaarheid van de organisatie tegen digitale ondermijning gelden in combinatie met minimaal niveau Entry van de eisen aan de digitale weerbaarheid van de organisatie. Het volwassenheidslevel van de weerbaarheid van de organisatie tegen digitale ondermijning moet ten minste gelijk zijn aan het volwassenheidslevel van de digitale weerbaarheid van de organisatie.

2.1.4 Eisen aan de digitale weerbaarheid van een organisatie in de zorg (CYRA-Zorg)

De eisen aan de digitale weerbaarheid van de organisatie in de zorg zijn afgeleid van de eisen uit de normserie NEN 7510, en verbijzonderd naar vier niveaus: Entry, Basic, Intermediate en Advanced. Elk niveau is onderverdeeld in drie volwassenheidslevels. Bijlage C geeft een specificatie van de drie volwassenheidslevels 1. Ad Hoc, 2. Best effort en 3. Defined.

2.1.5 Eisen aan de digitale weerbaarheid van OT (CYRA-OT)

De eisen aan de digitale weerbaarheid van de organisatie met OT zijn afgeleid van delen 2-1 en 3-3 van de normserie IEC 62443, en verbijzonderd naar vier niveaus: Entry, Basic, Intermediate en Advanced. Elk niveau is onderverdeeld in drie volwassenheidslevels. Bijlage C geeft een specificatie van de drie volwassenheidslevels 1. Ad Hoc, 2. Best effort en 3. Defined.

2.2 Eigen beoordeling

De organisatie moet een eigen beoordeling maken van het niveau van digitale weerbaarheid en/of de weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van OT.

Per niveau moet de organisatie voor elke beheersmaatregel het volwassenheidslevel bepalen.

De organisatie moet voor de eigen beoordeling gebruikmaken van het onlinezelfbeoordelingsinstrument dat het CCV voor dit certificatieschema beschikbaar stelt via <https://cyberrating.nl/>. Het bevat alle eisen uit het Toetsingskader CYRA dat het CCV heeft vastgesteld. Aan de hand van vragen per beheersmaatregel bepaalt de organisatie, op welk niveau beheersmaatregelen zijn ingevoerd (Entry, Basic, Intermediate of Advanced) en welk volwassenheidslevel (1. Ad hoc, 2. Best Effort, of 3. Defined) is behaald.

De eigen beoordeling leidt tot een eigen verklaring van de organisatie over het bereikte niveau van digitale weerbaarheid en/of de weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van OT. De eigen verklaring vormt het vertrekpunt voor certificatie.

3 Certificatievoorwaarden

3.1 Algemeen

De organisatie kan aan de certificatie-instelling een onafhankelijke beoordeling vragen van de eigen verklaring over zijn digitale weerbaarheid, eventueel in de zorg, en/of weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van OT. Dit hoofdstuk beschrijft hoe een aanvraag in zijn werk gaat, wat ervoor nodig is en welke voorwaarden er gelden gedurende de looptijd van het certificaat.

Zowel bij aanvraag (paragraaf 3.2) als tijdens de looptijd van het certificaat (paragraaf 3.3) moet de organisatie steeds aan de certificatie-instelling kunnen aantonen dat het niveau van digitale weerbaarheid en/of weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van de OT ten minste voldoet aan de eigen verklaring als bedoeld in hoofdstuk 2.

De organisatie voorziet de certificatie-instelling direct van alle opgevraagde informatie en gegevens. Het niet nakomen hiervan kan leiden tot de sancties beschreven in paragraaf 4.5 (schorsing) en 4.6 (intrekking).

3.2 Aanvraag van certificatie

3.2.1 Online beoordelingsinstrument

De organisatie doet de aanvraag met gebruikmaking van het online CCV-zelfbeoordelingsinstrument dat aan dit certificatieschema is verbonden. De organisatie maakt duidelijk of de aanvraag geldt voor de digitale weerbaarheid, eventueel in de zorg, de weerbaarheid tegen digitale ondermijning, voor de combinatie van deze twee en/of de digitale weerbaarheid van OT.

3.2.2 Gegevens bij aanvraag

De organisatie biedt bij aanvraag van certificatie de volgende gegevens aan de certificatie-instelling aan:

- Een eigen verklaring uit het CCV-zelfbeoordelingsinstrument als bedoeld in paragraaf 3.2.1 over de digitale weerbaarheid, eventueel in de zorg, met specificatie van het niveau Entry, Basic, Intermediate of Advanced en/of de weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van OT met specificatie van het niveau Entry, Basic, Intermediate of Advanced, en het volwassenheidslevel (1. Ad Hoc, 2. Best Effort of 3. Defined) waarop de beoordeling betrekking moet hebben;
- Een bewijs van wettelijke registratie waarbij de aard van de bedrijfsvoering en de bedrijfsactiviteiten zijn aangegeven;

In Nederland is dat inschrijving in het Handelsregister van de Kamer van Koophandel. Online raadpleging van het Handelsregister is toegestaan.

- Een verklaring van een hiertoe bevoegd persoon dat de organisatie zich zal houden aan de in het certificatieschema genoemde eisen, voorwaarden en verplichtingen;

Dit kan bijvoorbeeld de directeur, een lid van het managementteam of de kwaliteitsmanager zijn.

- De locatie, of in het geval van meerdere vestigingen: een overzicht van de locaties, of het organisatieonderdeel of de organisatieonderdelen waarvoor de eigen verklaring van toepassing is;
- De activiteiten van de organisatie waarop de eigen verklaring betrekking heeft.

De organisatie voorziet de certificatie-instelling verder op diens verzoek van alle nodige informatie en gegevens.

Om voor een certificaat in aanmerking te komen moet voor elke beheersmaatregel van het aangevraagde niveau tenminste voldaan zijn aan het aangevraagde volwassenheidslevel.

3.2.3 Status gedurende de aanvraag

Gedurende de beoordeling van de aanvraag is het de organisatie nog niet toegestaan enige verwijzing te publiceren naar de aanvraag voor certificatie. In individuele contacten en contracten mag hier wel naar worden verwezen.

3.3 Instandhouding van het certificaat

3.3.1 Handhaven weerbaarheidsniveau

De organisatie zorgt na certificatie dat haar digitale weerbaarheidsniveau en/of haar weerbaarheidsniveau tegen digitale ondermijning en/of het digitale weerbaarheidsniveau van OT gedurende de looptijd van het certificaat ten minste blijft voldoen aan het bij beoordeling vastgestelde niveau.

3.3.2 Wijzigingen

De organisatie meldt relevante ontwikkelingen en veranderingen in de organisatie tijdig bij de certificatie-instelling, zoals (niet limitatief):

- Contractueel en wettelijk meld-plichtige cyberveiligheidsincidenten;
- Fusies en overnames;
- Wijzigingen in de vestiging of de bedrijfsactiviteiten die van invloed zijn op het digitale weerbaarheidsniveau en/of de weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van OT of op toepassing van het certificatieschema;
- Wijzigingen in de inhoud en de status van andere certificaten (voor zover van invloed op uitvoering van het certificatieschema).

3.4 Wijziging van niveau

Indien de organisatie binnen 1 jaar na certificatie het niveau van haar eigen verklaring wil veranderen, kan zij vragen om de certificatiebeoordeling opnieuw te doen voor het dan gewenste niveau. De aanvraag verloopt volgens de bepalingen in 3.2.

Indien het certificaat langer dan 1 jaar geleden is afgegeven moet de organisatie die zich wil laten certificeren voor een ander niveau of voor een ander volwassenheidslevel, een nieuwe aanvraag doen volgens paragraaf 3.2.

3.5 Voortzetting van certificatie

Bij afloop van de geldigheid van het certificaat kan de organisatie een nieuwe aanvraag voor certificatie indienen op voet van paragraaf 3.2.

OPMERKING ter toelichting

Bij afloop van het certificaat verliest de organisatie het recht om het certificatiemerk te gebruiken.
Zie 5.1.3.

4 Eisen aan de uitvoering van certificatie

4.1 Algemeen

In dit hoofdstuk zijn geharmoniseerde werkwijzen over de uitvoering van het certificatieschema door certificatie-instellingen vastgelegd. Deze zijn bindend voor de betrokken certificatie-instellingen.

4.2 Eisen aan de certificatie-instelling

4.2.1 Algemeen

Certificatie-instellingen kunnen certificatiecontracten voor CYRA-certificatie sluiten met organisaties als zij een geldige accreditatie hebben voor beoordelingen tegen ISO/IEC 27006-1 of ISO/IEC 27001, en voor het certificatieschema een geldige licentieovereenkomst hebben met het CCV.

De modelovereenkomst voor certificatie-instellingen is gepubliceerd op de website van het CCV: www.hetccv.nl.

TOELICHTING

Dit certificatieschema wordt nog niet onder accreditatie uitgevoerd.

4.2.2 Relatie met – en gebruik van ISO/IEC 17021-1

Dit certificatieschema gaat uit van uitvoering op basis van ISO/IEC 17021-1.

Waar het certificatieschema geen detaillering geeft, moet de certificatie-instelling zelf de noodzakelijke invulling en detaillering aan brengen, en dit inbrengen in het harmonisatieoverleg met het CCV.

Certificatie-instellingen kunnen, voor zover niet strijdig met het certificatieschema, hun eigen reglementen en procedures toepassen. Indien hierbij strijdigheid optreedt met de bepalingen uit het certificatieschema, is het certificatieschema bindend.

Vanuit de accreditatieorganisatie hieraan verbonden documenten en interpretaties op nationaal en internationaal niveau zijn van toepassing.

TOELICHTING

ISO/IEC 17021-1 en de hieraan verbonden documenten, zoals de IAF MD documenten, geven al in hoge mate richting aan het kwaliteitsniveau en de harmonisatie in de uitvoering van certificatie onder ISO/IEC 17021-1.

Het certificatieschema beperkt zich tot die onderwerpen die vanuit ISO/IEC 17021-1 en de hieraan verbonden documenten niet geharmoniseerd zijn en waarvoor harmonisatie gewenst is.

Klanten van de certificatie-instelling kunnen uit het schema niet afleiden wat de procedurele aspecten van certificatie zijn, daarvoor is paragraaf 4.2.3 sturend.

4.2.3 Communicatie met de organisatie

4.2.3.1 Informatievoorziening over het schema

De certificatie-instelling is in staat, bij voorlichting aan de organisatie en/of op diens verzoek gedetailleerde informatie te verschaffen over:

- de inhoud, context en bedoeling van het certificatieschema;
- de inhoud, context en bedoeling van ISO/IEC 17021-1, en hieraan vanuit nationale en internationale uitvoering verbonden documenten;
- de te volgen procedures, werkwijzen, reglementen etc., zoals (niet limitatief):
 - Aanvraag;
 - Begroting van uren en kosten voor het uitvoeren van de certificatiebeoordeling;
 - Planning;
 - Auditplan;
 - Gebruik van certificatiemerken;
 - Afwijkingen en corrigerende maatregelen;
 - Schorsing, intrekking;
 - Beroepen en geschillen;
 - Beëindiging van het certificatiecontract.

Deze informatie kan algemeen zijn of betrekking hebben op specifieke delen van het certificatieschema.

4.2.3.2 Online beoordelingsinstrument

De certificatie-instelling moet voor de beoordeling van de eigen verklaring van de organisatie gebruik maken van het online CCV-beoordelingsinstrument dat via <https://cyberrating.nl/> voor dit certificatieschema beschikbaar is, en waarin de organisatie haar gegevens heeft geregistreerd en haar niveau van digitale weerbaarheid en/of weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van OT heeft bepaald.

4.2.3.3 Benchmarking

De certificatie-instelling verzamelt met inzet van het online beoordelingsinstrument uit 4.2.3.2 geanonimiseerde gegevens over beoordelingen van organisaties ten behoeve van benchmarking. De te verzamelen gegevens en de wijze van verwerken worden tussen schemabeheerder en certificatie-instelling nader overeengekomen. De certificatie-instelling regelt in het certificatiecontract de toestemming van de organisatie voor het verzamelen en verwerken van geanonimiseerde gegevens.

4.3 Eisen aan de uitvoering

4.3.1 Kwalificaties

4.3.1.1 Algemeen

De certificatie-instelling legt de kwalificaties van het betrokken certificatiepersoneel aantoonbaar vast. De certificatie-instelling onderbouwt dat het certificatiepersoneel voldoet aan de in dit certificatieschema genoemde kwalificatiecriteria. De kwalificatiecriteria zijn verwoord als competentie-eisen (kennis en vaardigheden).

De certificatie-instelling stelt voor nieuw te kwalificeren certificatiepersoneel een opleidingsprogramma vast, gericht op het voldoen aan de gestelde competentie-eisen.

De certificatie-instelling stelt voor gekwalificeerd certificatiepersoneel een programma vast voor het monitoren en evalueren van hun prestaties.

Maatgevend voor het kwalificeren zijn de competenties van het kwalificatiepersoneel. Opleiding, ervaring en andere vaardigheden kunnen bijdragen in het aantoonbaar maken van de gevraagde competenties.

De certificatie-instelling moet de competenties in voldoende mate detailleren om aan de eisen van ISO/IEC 17021-1 te voldoen. Dit geldt niet alleen voor de betrokken auditoren, maar voor al het certificatiepersoneel betrokken bij het certificatieproces, zoals (niet limitatief):

- Behandelen van de aanvraag, offerte;
- Kwalificeren van het certificatiepersoneel;
- Monitoren van het certificatiepersoneel;
- Review van audit rapporten;
- Beslissing;
- Administratieve verwerking van certificaten;
- Behandelen van klachten.

4.3.1.2 Specifieke eisen voor auditoren

Voor het certificatieschema geldt als minimum:

Deelgebied A	Informatiebeveiliging	Gekwalificeerd ISO 27001-auditor of:		
		Kennis	HBO- werk- en denkniveau.	
			Kennis van de inhoud, betekenis en context van de beheersmaatregelen uit de norm	
			Relevante IT-beveiligings- of ICT-opleiding + een relevante training voor ISMS-audit + audit management.	
Ervaring	Minimaal twee jaar fulltime praktijkervaring op de werkvloer in een rol of functie op het gebied van informatiebeveiliging.			
	Ervaring verworven in het volledige proces van het evalueren van informatiebeveiliging door deelname aan ten minste vier ISMS-audits, waaronder minimaal één initiële en één tussentijdse audit. Deze deelname omvat het beoordelen van documentatie, risicobeoordelingen, implementatie-evaluaties en het opstellen van auditrapporten.			
	Privacy	Aantoonbare privacy-kennis/ervaring m.b.t. verwerkers (bijvoorbeeld een training waar ISO 27701 Annex B onderdeel van uitmaakt, certificering als bijvoorbeeld CIPP/E of ECPC-B, of praktijkervaring als Functionaris Gegevensbescherming)		
Deelgebied B	Digitale ondermijning	Aanvullend op de kwalificatie-eisen voor Informatiebeveiliging en Privacy volgens deelgebied A en/of C: kennis van het Normkader Digitale Ondermijning (NDO).		
Deelgebied C	Informatiebeveiliging in de zorg	Gekwalificeerd NEN 7510-auditor voor Beheerders (B) of voor Zorginstellingen (Z), of:		
		Kennis	HBO- werk- en denkniveau.	
			Kennis van de inhoud, betekenis en context van de beheersmaatregelen uit de norm.	

			Relevante IT-beveiligings- of ICT-opleiding + een relevante training voor ISMS-audit + audit management.
		Ervaring	Minimaal twee jaar fulltime praktijkervaring op de werkvloer in een rol of functie op het gebied van informatiebeveiliging.
			Werkervaring in of aantoonbare kennis van de zorgsector.
			Ervaring verworven in het volledige proces van het evalueren van informatiebeveiliging door deelname aan ten minste vier ISMS-audits, waaronder minimaal één initiële en één tussentijdse audit. Deze deelname omvat het beoordelen van documentatie, risicobeoordelingen, implementatie-evaluaties en het opstellen van auditrapporten.
	Privacy		Aantoonbare privacy-kennis/ervaring m.b.t. verwerkers (bijvoorbeeld een training waar ISO 27701 Annex B onderdeel van uitmaakt, certificering als bijvoorbeeld CIPP/E of ECPC-B, of praktijkervaring als Functionaris Gegevensbescherming).
Deelgebied D	De kwalificatie-eisen voor Informatiebeveiliging volgens deelgebied A; ISA-certificering als Risk Assessment Specialist (https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program) of certificaat op minimaal de delen 2-1 en 3-3 van IEC 62443 of aantoonbare training op het vlak van OT zoals bijvoorbeeld (niet limitatief) een IC-32 trainingscertificaat vanuit ISA (https://www.isa.org/training/course-description/ic32).		

4.3.2 Behandeling aanvraag

De certificatie-instelling neemt elke aanvraag in behandeling en controleert of alle gegevens bij aanvraag compleet en juist zijn. De certificatie-instelling vraagt aanvullende gegevens op die nodig zijn voor het behandelen van de aanvraag en het opstellen van een begroting en planning.

De certificatie-instelling behandelt de aanvraag van een certificaathouder met een certificatieovereenkomst met een andere certificatie-instelling volgens het CCV-reglement Beoordelen overstappende certificaathouder.

4.3.3 Uitvoering beoordelingen

4.3.3.1 Minimum tijdsbesteding

De minimaal te besteden audittijd is gespecificeerd in tabel 1 en is gebaseerd op één organisatie met één locatie. De audittijd is inclusief voorbereidingstijd maar exclusief reistijd.

Uitgangspunt is verder: gebruik van het online CCV-zelfbeoordelingsinstrument waarin de organisatie zijn gegevens heeft ingevuld en zijn eigen verklaring heeft vastgelegd. De auditor baseert zich bij zijn beoordeling op die gegevens. De auditor legt zijn bevindingen vast in het online CCV-zelfbeoordelingsinstrument. Een afzonderlijke rapportage wordt niet verstrekt. De organisatie vindt eventuele afwijkingen terug in het online CCV-zelfbeoordelingsinstrument zelf.

TABEL 1 - TIJDSBESTEDING

	Aantal dagen voor deelgebied A en C ten minste	Aantal dagen voor deelgebied D ten minste
Toetsing niveau Entry	0,75*	1
Toetsing niveau Basic	1,5	2
Toetsing niveau Intermediate	2	3
Toetsing niveau Advanced	2,5	3,5
Toetsing weerbaarheid tegen digitale ondermijning volgens deelgebied B (in aanvulling op deelgebied A of C)	0,5**	

* Beoordeling van niveau Entry vindt in principe op afstand ('remote') plaats, zie 4.3.3.2.

** aanvullend op de beoordelingstijd voor Entry, Basic, Intermediate of Advanced. Beoordeling van weerbaarheid tegen digitale ondermijning in combinatie met niveau Entry kan *niet* op afstand ('remote') plaatsvinden.

Indien de organisatie binnen 1 jaar na certificatie het niveau van haar eigen verklaring wil veranderen, kan zij vragen om de certificatiebeoordeling opnieuw te doen voor het dan gewenste niveau. In dat geval geldt de tijdsbesteding volgens tabel 2:

TABEL 2 - TIJDSBESTEDING BIJ VERANDERING VAN NIVEAU

	Van Entry naar	Van Basic naar	Van Intermediate naar	Aanpassing Volwassenheidslevel
Naar Entry				1 dag
Naar Basic	0,5 dag			1 dag
Naar Intermediate	1,5 dag	1 dag		1 dag
Naar Advanced	2 dagen	1,5 dag	0,5 dag	1 dag

4.3.3.2 Beoordeling

Beoordeling vindt plaats op de locatie waarop de eigen verklaring betrekking heeft. Uitgezonderd is beoordeling van niveau Entry in deelgebieden A en C, die in principe plaatsvindt op afstand ('remote', online), tenzij de beoordeling wordt gecombineerd met beoordeling van de weerbaarheid tegen digitale ondermijning in deelgebied B, of naar het oordeel van de certificatie-instelling beoordeling op de locatie waarop de eigen verklaring betrekking heeft noodzakelijk is.

De auditor beoordeelt in hoeverre de eigen beoordeling van de organisatie overeenkomt met de eisen van het niveau en het volwassenheidslevel dat de organisatie bij aanvraag heeft gespecificeerd. Daartoe valideert de auditor de beheersmaatregelen van het gekozen niveau (Entry, Basic, Intermediate of Advanced) op het vooraf aangegeven volwassenheidslevel (Ad hoc, Best Effort of Defined) en desgewenst de beheersmaatregelen voor weerbaarheid tegen digitale ondermijning. Om tot een positief oordeel te komen moeten alle beheersmaatregelen minimaal op het gekozen niveau

en aangegeven volwassenheidslevel zijn geïmplementeerd. Ingeval deelgebied B onderdeel van de beoordeling uitmaakt moet het bereikte volwassenheidslevel van de weerbaarheid tegen digitale ondermijning op ten minste hetzelfde level liggen als het volwassenheidslevel van de digitale weerbaarheid van de organisatie.

Indien een auditor een afwijking vaststelt kan hij niet tot een positief oordeel komen. Elke afwijking moet eerst worden hersteld. Indien het aantal niet-conforme beheersmaatregelen minder is dan 15% (afgerond naar boven) en de organisatie de geconstateerde afwijking(en) binnen 8 weken herstelt, kan een herbeoordeling plaatsvinden. In het andere geval moet de organisatie een nieuwe aanvraag doen. Een herbeoordeling kan op afstand ('remote') plaatsvinden indien de correcties dat naar het oordeel van de auditor toestaan.

Indien de organisatie een (deel van een) beheersmaatregel niet heeft geïmplementeerd kan de auditor niet tot een positief oordeel komen, tenzij de organisatie onderbouwt dat (het betreffende deel van) de beheersmaatregel niet van toepassing is. Als de beheersmaatregelen die zijn geïmplementeerd en waarvan de implementatie is aangetoond gezamenlijk voldoen aan een niveau dat direct onder het bij aanvraag verklaarde niveau of volwassenheidslevel ligt, kan de auditor onder de volgende voorwaarden tot een positief oordeel komen over dat lagere niveau of volwassenheidslevel:

- de bevoegde persoon die de aanvraag tot certificatie heeft gedaan, is tijdens de audit beschikbaar voor consultatie;
- de bevoegde persoon stemt voordat de audit is afgerond in met certificatie op het naast-lagere niveau of naast-lagere volwassenheidslevel.

Indien aan alle eisen voor het aangevraagde niveau is voldaan kan de auditor tot een positief oordeel komen.

De certificatie-instelling verstrekt de organisatie in dat geval het certificaat als bedoeld in hoofdstuk 5. Het certificaat is twee jaar geldig.

4.3.3.3 Toezicht

De certificatie-instelling is verantwoordelijk voor toezicht op de certificaathouder gedurende de looptijd van het certificaat.

4.3.3.4 Extra beoordeling

De certificatie-instelling kan extra audits uitvoeren als hiertoe aanleiding is. Aanleidingen kunnen zijn:

- Cyberveiligheidsincidenten die de organisatie op grond van 3.2.2 heeft gemeld;
- Klachten dat de digitale weerbaarheid en/of de weerbaarheid tegen digitale ondermijning en/of de digitale weerbaarheid van OT niet aan het vastgestelde niveau of volwassenheidslevel voldoet;
- Klachten over misleidend of foutief gebruik van het certificatiemerk;
- Publicaties over cyberveiligheidsincidenten;
- Eigen waarnemingen door de certificatie-instelling;
- Informatie van belanghebbende partijen, zoals de overheid en/of verzekeraars.

Indien de auditor bij de extra beoordeling een situatie constateert die niet in overeenstemming is met de eisen stelt hij een afwijking vast. Afwijkingen kunnen zijn:

- Het niet in stand hebben gehouden van één van de eisen uit het certificatieschema, of
- Het niet in voldoen of voldaan hebben van één of meerdere voorwaarden uit dit certificatieschema (waaronder financiële verplichtingen en het reglement voor het gebruik van het certificatiemerk).

De certificatie-instelling communiceert de afwijking(en) aan de organisatie bij het afsluiten van de extra beoordeling. Voor herstel van (de) afwijking(en) geldt paragraaf 4.4. Voor de uitvoering, rapportage, review, besluitvorming van de extra beoordeling en eventuele sancties gelden de bepalingen genoemd in dit certificatieschema.

4.3.4 Klachten en beroep

De certificatie-instelling hanteert bij klachten en beroepen het eigen reglement dat onder accreditatie wordt toegepast.

4.3.5 Publicatie

De certificatie-instelling publiceert geen informatie over organisaties die certificatie hebben aangevraagd of waarvan hij het digitale weerbaarheidsniveau en/of het weerbaarheidsniveau tegen digitale ondermijning en/of het digitale weerbaarheidsniveau van OT heeft gecertificeerd.

4.4 Herstel van afwijkingen

4.4.1 Corrigerende maatregelen

In het geval de auditor tijdens de extra beoordeling (een) afwijking(en) heeft vastgesteld krijgt de organisatie 8 weken de tijd om corrigerende maatregelen te nemen. De corrigerende maatregelen moeten ten minste bestaan uit:

- Een analyse gericht op de grondoorzaak en/of grondoorzaken van de afwijking. In deze analyse komen in elk geval omvang en de mogelijke oorzaken naar voren;
- Acties nodig voor het opheffen van de afwijking (correctie);
- Oplossingen gericht op het voorkomen van herhaling en het borgen hiervan (corrigerende maatregel);
- Verantwoordelijke voor de verbeteracties en corrigerende maatregelen;
- Uiterlijke datum voor het afronden van de verbeteracties (correctie en corrigerende maatregelen);
- De beoordeling van de doeltreffendheid van de implementatie van deze oplossingen.

De organisatie documenteert de volgens het plan van aanpak uit te voeren correcties en corrigerende maatregelen volledig, zodat de certificatie-instelling deze kan verifiëren.

4.4.2 Beoordeling van herstel door de certificatie-instelling

De certificatie-instelling beoordeelt de uitvoering van de correcties en de implementatie van de corrigerende maatregelen om vast te stellen dat de afwijking is opgeheven. De wijze van beoordelen is afhankelijk van de aard van de afwijking. Zo nodig wordt een extra beoordeling uitgevoerd ter verificatie.

De certificatie-instelling hanteert hierbij de termijnen en procedures conform het reglement van de certificatie-instelling.

4.5 Schorsing

4.5.1 Schorsen

Het certificaat wordt geschorst:

- Bij een plan van aanpak dat onvoldoende borgt dat correcties uitgevoerd worden en/of dat onvoldoende borging biedt voor de uitvoering van de oorzakaanalyse en implementatie van corrigerende maatregelen (zie paragraaf 4.4.1), of
- Als de corrigerende maatregelen voor afwijkingen niet binnen de gestelde termijn hebben geleid tot herstel van de afwijking(en) (zie paragraaf 4.4.1), of
- Als de organisatie niet voldoet aan de voorwaarden voor certificatie (waaronder de financiële verplichtingen en verplichtingen inzake het gebruik van het certificatiemerk) (zie paragraaf 3.1).

De certificatie-instelling documenteert het advies van de beoordelaar, de review en besluitvorming en de beslissing volledig, inclusief onderbouwing.

De certificatie-instelling informeert de organisatie per email over de schorsing.

4.5.2 Gevolgen van schorsing

Vanaf het moment van schorsing is het de organisatie niet toegestaan om het certificatiemerk te gebruiken, of te verwijzen naar de het certificaat voor het digitale weerbaarheidsniveau en/of het certificaat voor weerbaarheid tegen digitale ondermijning en/of het certificaat voor het digitale weerbaarheidsniveau van OT.

4.5.3 Opheffen van een schorsing

Als de certificatie-instelling vaststelt dat alle geconstateerde afwijkingen opgeheven zijn, wordt de schorsing opgeheven. De certificatie-instelling stelt de organisatie hiervan schriftelijk op de hoogte.

Vanaf de datum die door de certificatie-instelling schriftelijk is vermeld, is het gebruik van het certificatiemerk en verwijzing naar het certificaat voor het digitale weerbaarheidsniveau en/of het certificaat voor weerbaarheid tegen digitale ondermijning en/of het certificaat voor het digitale weerbaarheidsniveau van OT weer toegestaan.

Een schorsing duurt maximaal zes maanden.

4.6 Intrekking

4.6.1 Intrekken

Het certificaat wordt ingetrokken indien de organisatie niet in staat is de geconstateerde afwijkingen binnen de periode van schorsing op te heffen.

De certificatie-instelling informeert de organisatie per email over de intrekking.

4.6.2 Gevolgen van intrekking

Vanaf het moment van intrekking is het de organisatie niet toegestaan om het certificatiemerk te gebruiken, of te verwijzen naar het certificaat voor het digitale weerbaarheidsniveau en/of het certificaat voor weerbaarheid tegen digitale ondermijning en/of het certificaat voor het digitale weerbaarheidsniveau van OT.

4.6.3 Nieuwe aanvraag

Een organisatie waarvan het certificaat voor het digitale weerbaarheidsniveau en/of het certificaat voor weerbaarheid tegen digitale ondermijning en/of het certificaat voor het digitale weerbaarheidsniveau van OT is ingetrokken, kan een nieuwe aanvraag doen voor certificatie volgens dit certificatieschema.

5 Certificatiemerken en certificaten

5.1 Certificatiemerken

Het certificatiemerk, verder te noemen 'het merk', is het bewijs voor opdrachtgever dat door beoordeling van de certificatie-instelling onderbouwd vertrouwen aanwezig is dat de digitale weerbaarheid van de organisatie en/of de weerbaarheid van de organisatie tegen digitale ondermijning en/of de digitale weerbaarheid van OT voldoet aan de gestelde eisen in het certificatieschema (zoals beschreven in hoofdstuk 2) en waarbij tevens aan de contractuele en reglementaire voorwaarden is voldaan.

Het merk is uitgevoerd als combinatie van een beeld- en woordmerk, zie paragraaf 5.1.1.

Uitsluitend het gebruik van het merk beschreven in het certificatieschema is toegestaan.

5.1.1 Merk

Aan dit certificatieschema is het aan de linkerzijde afgebeelde woordbeeldmerk verbonden. Dit woordbeeldmerk is gedeponeerde.



Voor digitale weerbaarheid volgens deelgebied A wordt het woordbeeldmerk aangevuld met het woordmerk Cyber Security en CYRA - IT, zoals aan de rechterzijde afgebeeld.



Voor weerbaarheid tegen digitale ondermijning volgens deelgebied B wordt het woordbeeldmerk aangevuld met het woordmerk Cyber Security en CYRA - NDO, zoals aan de rechterzijde afgebeeld. Dit merk mag alleen worden gebruikt in combinatie met het merk voor deelgebied A of C.



Voor digitale weerbaarheid volgens deelgebied C wordt het woordbeeldmerk aangevuld met het woordmerk Cyber Security en CYRA - Zorg, zoals aan de rechterzijde afgebeeld.



Voor digitale weerbaarheid van OT volgens deelgebied D wordt het woordbeeldmerk aangevuld met het woordmerk Cyber Security en CYRA - OT, zoals aan de rechterzijde afgebeeld.



De aanvullingen op het woordbeeldmerk geven de koppeling van het gedeponeerde woordbeeldmerk met dit certificatieschema aan. Separate woordmerken worden niet toegepast.

5.1.2 Gebruik van het merk door de certificatie-instelling

De certificatie-instelling moet het merk gebruiken in overeenstemming met het CCV-reglement Kwaliteitslogo. Eisen voor het gebruik van het merk zijn in algemene zin:

- De certificatie-instelling heeft een geldige licentie bij het CCV;
- Het merk wordt in rechtstreeks verband met het certificatieschema en bij wijze van illustratie gebruikt op briefpapier, in email, op de website, in folders en andere publiciteitsuitingen.

5.1.3 Gebruik van het merk door de organisatie

De organisatie moet het merk gebruiken in overeenstemming met het CCV-reglement Kwaliteitslogo. Eisen voor het gebruik van het merk zijn in algemene zin:

- De organisatie heeft een geldig certificatiecontract met een certificatie-instelling die voor uitvoering van het CCV-certificatieschema een geldige licentie heeft bij het CCV;
- De organisatie is niet geschorst;
- Het merk wordt in rechtstreeks verband met de locatie en de processen, diensten, activiteiten binnen scope en bij wijze van illustratie gebruikt op briefpapier, in email, op de website, in folders en andere publiciteitsuitingen.

5.2 Certificaat voor het weerbaarheidsniveau

5.2.1 Algemeen

Na positief besluit op de beoordeling verstrekt de certificatie-instelling aan de organisatie een certificaat voor het weerbaarheidsniveau. Het certificaat wordt opgesteld in de huisstijl van de certificatie-instelling en moet ten minste voldoen aan de eisen uit 5.2.2 of 5.2.4. Een gecombineerd certificaat is niet toegestaan.

Voor het weerbaarheidsniveau tegen digitale ondermijning is een certificaat niet mogelijk, de verklaring over dat weerbaarheidsniveau moet in voorkomend geval worden toegevoegd aan het certificaat voor de deelgebieden A en C als bedoeld in 5.2.2.

Aanvullende informatie mag op het certificaat worden toegevoegd, zolang die niet strijdig is met het certificatieschema en (of) wet- en regelgeving of betrekking heeft op zaken die buiten de beoordeling of de verantwoordelijkheid van de organisatie valt.

TOELICHTING

In afwijking van ISO/IEC 17021-1 is het certificaat twee jaar geldig

5.2.2 Certificaat digitale weerbaarheidsniveau voor deelgebieden A (CYRA – IT) en C (CYRA-Zorg)

Het certificaat voor het digitale weerbaarheidsniveau bevat minimaal de volgende gegevens:

- Koptekst: < CYRA-IT / CYRA-Zorg > - <Entry / Basic / Intermediate / Advanced> - <Ad Hoc (1) / Best Effort (2) / Defined (3)>;

Bijvoorbeeld: CYRA-Zorg Basic – Best Effort (2)

- NAW-gegevens van de certificatie-instelling;
- NAW-gegevens van de organisatie (correspondentieadres);
- De tekst:

<Certificatie-instelling> verklaart dat het digitale weerbaarheidsniveau van <naam van de organisatie> voor de locatie <aanduiding locatie> en de bedrijfsactiviteiten <processen, diensten, activiteiten binnen scope> voldoet aan de eisen van het CCV-certificatieschema CYRA op het digitale weerbaarheidsniveau <Entry – Basic – Intermediate – Advanced> (volwassenheidslevel <Ad Hoc (1) / Best Effort (2) / Defined (3)>).

<Certificatie-instelling> geeft <organisatie> onderstaand certificatiemerk in licentie voor gebruik volgens het CCV-reglement Kwaliteitslogo.

- Een uniek certificatenummer;
- De datum van uitgifte/vanaf wanneer het certificaat geldig is;
- De datum tot wanneer het certificaat geldig is [uitgiftedatum + 24 maanden];
- Handtekening, eventueel digitaal (met naam en functie);
- Het bedrijfslogo van de certificatie-instelling;
- Het certificatiemerk:

Ingeval van deelgebied A – CYRA – IT



Ingeval van deelgebied C – CYRA – Zorg



- De teksten:
 - De status van dit certificaat kan nagegaan worden bij <certificatie-instelling>
 - Dit certificaat blijft eigendom van <certificatie-instelling>.

5.2.3 Aanvullende verklaring over de weerbaarheid tegen digitale ondermijning volgens deelgebied B (CYRA – NDO)

Als in aanvulling op de beoordeling volgens deelgebied A of C ook beoordeling volgens deelgebied B heeft plaatsgevonden en positief is afgerond, wordt het certificaat als bedoeld in 5.2.2 aangevuld met de volgende gegevens:

- Koptekst: CYRA-NDO - <Entry / Basic / Intermediate / Advanced> - <Ad Hoc (1) / Best Effort (2) / Defined (3)>

- Het onderstreepte deel in de tekst van de verklaring van de certificatie-instelling:

<Certificatie-instelling> verklaart dat het digitale weerbaarheidsniveau en het weerbaarheidsniveau tegen digitale ondermijning van <naam van de organisatie> voor de locatie <aanduiding locatie> en de bedrijfsactiviteiten <processen, diensten, activiteiten binnen scope> voldoen aan de eisen van het CCV-certificatieschema CYRA (volwassenheidslevel <Ad Hoc (1) / Best Effort (2) / Defined (3)>).

<Certificatie-instelling> geeft <organisatie> onderstaande certificatiemerken in licentie voor gebruik volgens het CCV-reglement Kwaliteitslogo.

- Het certificatiemerk:



Opmerking ter toelichting: een gecombineerd certificaat CYRA-IT & CYRA-NDO of CYRA-Zorg & CYRA-NDO bevat dus twee certificatiemerken.

5.2.4 Certificaat digitale weerbaarheidsniveau voor deelgebied D (CYRA – OT)

Het certificaat voor het digitale weerbaarheidsniveau van operationele technologie bevat minimaal de volgende gegevens:

- Koptekst: CYRA-OT - <Entry / Basic / Intermediate / Advanced> - <Ad Hoc (1) / Best Effort (2) / Defined (3)>;

Bijvoorbeeld: CYRA-OT Intermediate – Defined (3)

- NAW-gegevens van de certificatie-instelling;
- NAW-gegevens van de organisatie (correspondentieadres);
- De tekst:

<Certificatie-instelling> verklaart dat de digitale weerbaarheid van operationele technologie van <naam van de organisatie> voor de locatie <aanduiding locatie> en de bedrijfsactiviteiten <processen, diensten, activiteiten binnen scope> voldoet aan de eisen van het CCV-certificatieschema CYRA op het digitale weerbaarheidsniveau <Entry – Basic – Intermediate – Advanced> (volwassenheidslevel <Ad Hoc (1) / best Effort (2) / Defined (3)>).

<Certificatie-instelling> geeft <organisatie> onderstaand certificatiemerk in licentie voor gebruik volgens het CCV-reglement Kwaliteitslogo.

- Een uniek certificatenummer;
- De datum van uitgifte;
- De datum tot wanneer het certificaat geldig is [uitgiftedatum + 24 maanden];
- Handtekening, eventueel digitaal (met naam en functie);
- Het bedrijfslogo van de certificatie-instelling;

- Het certificatiemerk:



- De teksten:
 - De status van dit certificaat kan nagegaan worden bij <certificatie-instelling>
 - Dit certificaat blijft eigendom van <certificatie-instelling>.

6 Verwijzingen

6.1 Wet- en regelgeving

Deze paragraaf is voor dit certificatieschema niet van toepassing.

6.2 Begrippen en afkortingen

Afwijking	Een situatie die niet in overeenstemming is met de eisen uit het certificatieschema.
Audit	Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijs en het objectief beoordelen daarvan om vast te stellen in welke mate aan overeengekomen auditcriteria is voldaan.
Beoordeling	Uitvoering van dit certificatieschema door de certificatie-instelling bij de organisatie.
CCV	Centrum voor Criminaliteitspreventie en Veiligheid.
CYRA	Cyber Rating
Certificaat	Document dat de certificatie-instelling verstrekt aan de organisatie met een verklaring over het digitale weerbaarheidsniveau of het niveau van weerbaarheid tegen digitale ondermijning of het digitale weerbaarheidsniveau van operationele technologie.
Certificatiemerk	Woord- of beeldmerk dat wordt gebruikt om conformiteit met de gestelde eisen aan te geven.
Certificatieschema	Stelsel van regels, procedures en beheeraspecten voor het uitvoeren van certificatiebeoordelingen.
Commissie van Belanghebbenden	De commissie binnen het CCV waar het draagvlak voor het schema wordt bepaald en die het CCV adviseert over (wijzigingen in) het certificatieschema. In deze commissie zijn belanghebbenden en betrokken partijen vertegenwoordigd.
EN	Europese Norm, uitgegeven door CEN of CENELEC (European Committee for (Electrotechnical) Standardization).
IACS	Industrial Automation and Control Systems. Verzamelnaam voor systemen en technologieën die industriële processen automatisch regelen, aansturen en monitoren, zoals PLC's (Programmable Logic Controller), SCADA-systemen (Supervisory Control and Data Acquisition), DCS'en (Distributed Control System). In dit schema aangeduid met Operationele Technologie (OT).
IEC	International Electrotechnical Commission. Een IEC-norm is een internationale norm die wordt uitgegeven door IEC.
ISMS	Information Security Management System.
ISO	International Organisation for Standardization. Een ISO-norm is een Internationale norm die wordt uitgegeven door ISO.
IT	Informatie Technologie
NAW-gegevens	Gegevens die betrekking hebben op naam, adres en woonplaats.
NDO	Normkader Digitale Ondermijning
NEN	Stichting Koninklijk Nederlands Normalisatie Instituut. Het NEN geeft de Nederlandse normen uit.
Norm	Document waarin door betrokken partijen afspraken zijn vastgelegd met het doel zich daaraan te houden.
Opdrachtgever	De rechtspersoon waarvoor of in opdracht waarvan de organisatie werkzaamheden uitvoert.

Organisatie	De organisatie die zijn digitale weerbaarheid of weerbaarheid tegen digitale ondermijning of de digitale weerbaarheid van zijn operationele technologie wil vaststellen, heeft vastgesteld of door een certificatie-instelling onafhankelijk wil laten beoordelen.
OT	Operationele Technologie. Verzamelnaam voor systemen en technologieën die industriële processen automatisch regelen, aansturen en monitoren, zoals PLC's (Programmable Logic Controller), SCADA-systemen (Supervisory Control and Data Acquisition), DCS'en (Distributed Control System). Internationale term: IACS, zie aldaar.

6.3 Normen en normatieve verwijzingen

De normen en documenten genoemd in onderstaande tabel zijn van toepassing voor dit certificatieschema, inclusief interpretaties die het CCV heeft gepubliceerd. Indien een versienummer is gegeven is die versie bindend (statische verwijzing). Deze normen en documenten zijn normatief, tenzij in dit schema aangegeven is dat het indicatieve verwijzing betreft. Er kan ook normatief of indicatief naar delen van een norm of document worden verwezen, waarbij dan de overige delen van deze norm of dit document voor dit schema geen betekenis hebben.

In deze normen en documenten genoemde andere normen of documenten zijn van toepassing, zoals hierin aangegeven.

Een certificatie-instelling moet beschikken over alle normatieve normen en documenten.

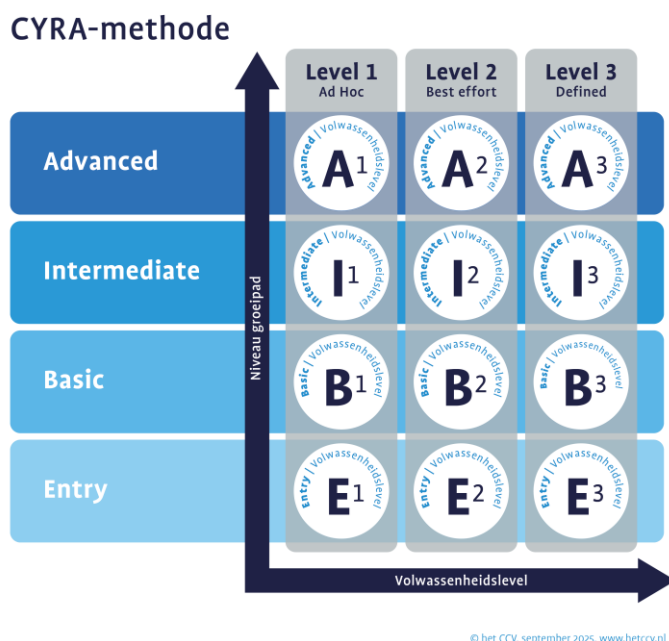
NORM	ONDERWERP	VERKRIJGBAAR BIJ
NEN-EN-IEC 62443-2-1	Beveiliging van industriële automatiserings- en besturingssystemen - Deel 2-1: Eisen voor beveiligingsprogramma's voor eigenaren van IACS-activa	NEN Delft
NEN-EN-IEC 62443-3-3	Industriële communicatie netwerken - Netwerk- en systeembeveiliging - Deel 3-3: Eisen voor systeembeveiliging en beveiligingsniveaus	NEN, Delft
ISO/IEC 17021-1	Conformiteitsbeoordeling – Eisen voor instellingen die audits en certificatie van managementsystemen leveren – Deel 1: Eisen	NEN, Delft
ISO/IEC 27001	Informatiebeveiliging, cybersecurity en bescherming van de privacy – Managementsysteem voor informatiebeveiliging – Eisen	NEN, Delft
ISO/IEC 27002	Informatiebeveiliging, cybersecurity en bescherming van de privacy – Beheersmaatregelen voor informatiebeveiliging	NEN, Delft
ISO/IEC 27006-1	Informatiebeveiliging, cybersecurity en privacybescherming – Eisen voor instanties die audits uitvoeren en certificering verzorgen van informatiebeveiligingsmanagementsystemen – Deel 1: Algemeen	NEN, Delft
ISO/IEC 27701	Veiligheidstechnieken – Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiesystemen – Eisen en richtlijnen	NEN, Delft
NEN 7510-1	Medische informatica - Informatiebeveiliging in de zorg - Deel 1: Managementsysteem	NEN, Delft
NEN 7510-2	Medische informatica - Informatiebeveiliging in de zorg - Deel 2: Beheersmaatregelen	NEN, Delft

	CCV-reglement Kwaliteitslogo	CCV, Utrecht
	CCV-reglement Beoordelen overstappende certificaathouder	CCV, Utrecht

Bijlage A - Overzicht CYRA beoordelingsniveaus en levels

A.1 Toetsingskader digitale weerbaarheid (deelgebied A)

Het toetsingskader voor digitale weerbaarheid in deelgebied A is afgeleid van de eisen uit de normen ISO/IEC 27001 en ISO/IEC 27701. Het bestaat uit 12 onderdelen: de niveaus Entry, Basic, Intermediate en Advanced en op elk niveau de volwassenheidslevels 1 t/m 3. De onderlinge samenhang is zichtbaar gemaakt in figuur 2.



Figuur 2: overzicht van niveaus en volwassenheidslevels in het CYRA-toetsingskader.

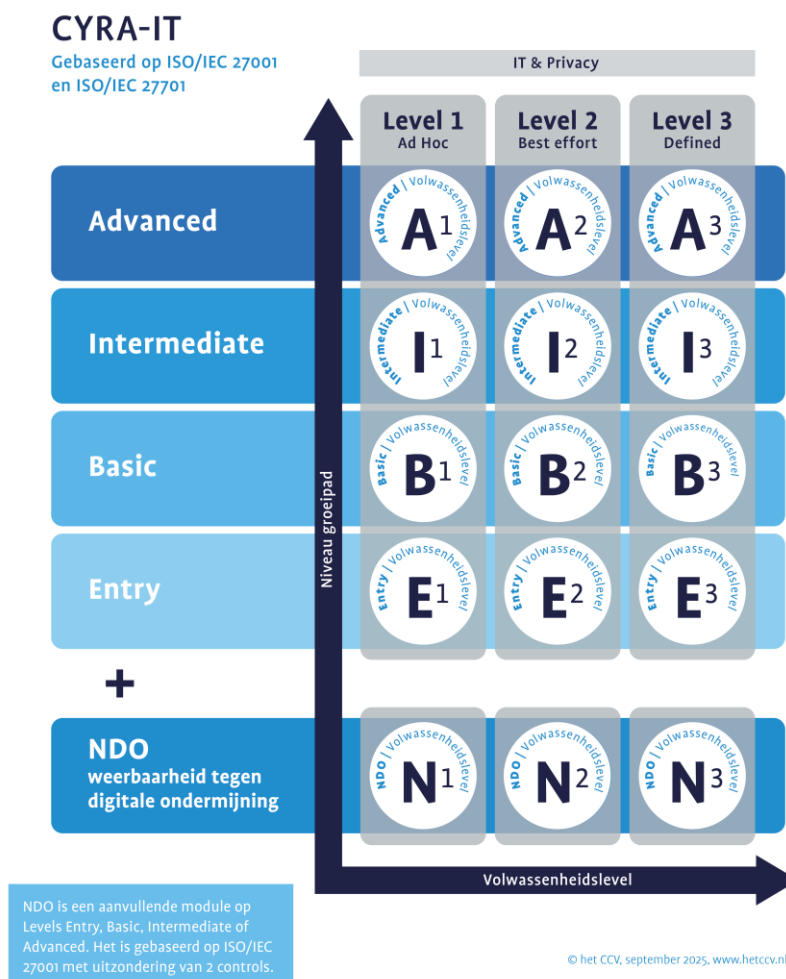
Een organisatie moet ten minste voldoen aan de beoordelingsaspecten van niveau Entry, Level 1 (Ad Hoc) om voor een certificaat CYRA-IT in aanmerking te komen.

Het groeppad ten opzichte van de uit ISO/IEC 27001 en ISO/IEC 27701 geselecteerde totale set beheersmaatregelen is als volgt:

- Entry = 25%
- Basic = 55%
- Intermediate = 80%
- Advanced = 100%

A.2 Toetsingskader weerbaarheid tegen digitale ondermijning (deelgebied B)

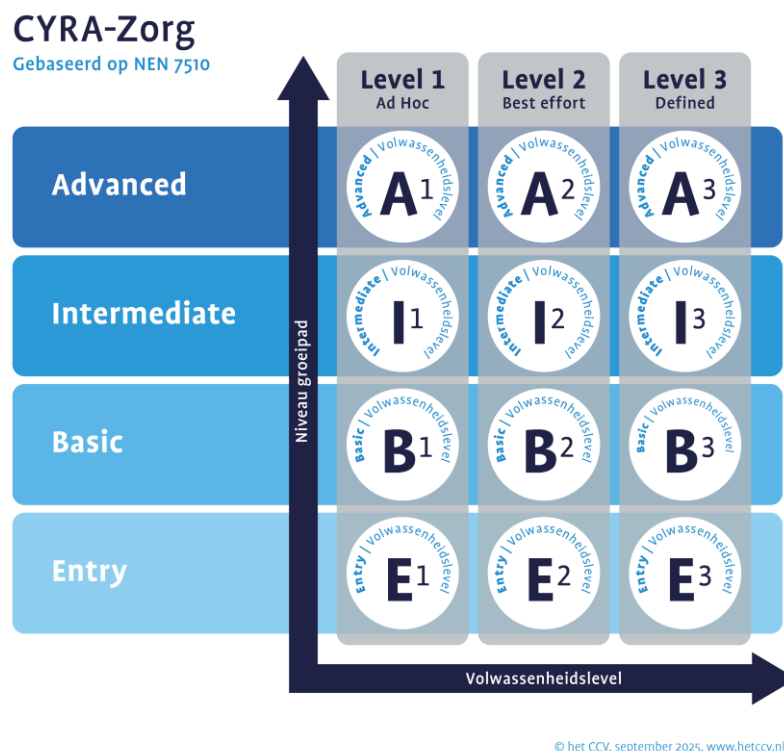
Het normkader Digitale Ondermijning (NDO) voor deelgebied B is een specifieke invulling van eisen uit de norm ISO/IEC 27001, aangevuld met eisen aan bedrijfsprocessen die voor het versterken van de weerbaarheid tegen digitale ondermijning van belang zijn. Het bestaat uit 9 beoordelingsaspecten. Deze worden in hun geheel beoordeeld in samenhang met de beoordelingsaspecten voor het van toepassing zijnde niveau uit het toetsingskader voor digitale weerbaarheid uit deelgebied A of C, tenminste Entry (volwassenheidslevel Ad Hoc (1)). De onderlinge samenhang is zichtbaar gemaakt in figuur 3.



Figuur 3: overzicht van samenhangende beoordelingsaspecten en volwassenheidslevels in het toetsingskader voor weerbaarheid tegen digitale ondermijning.

A.3 Toetsingskader digitale weerbaarheid organisatie in de zorg (deelgebied C)

Het toetsingskader voor digitale weerbaarheid van organisaties in de zorg in deelgebied C is afgeleid van de eisen uit de normserie NEN 7510. Het bestaat uit 12 onderdelen: de niveaus Entry, Basic, Intermediate en Advanced en op elk niveau de volwassenheidslevels 1 t/m 3. De onderlinge samenhang is zichtbaar gemaakt in figuur 4.



Figuur 4: overzicht van niveaus en volwassenheidslevels in het CYRA-toetsingskader digitale weerbaarheid van organisaties in de zorg.

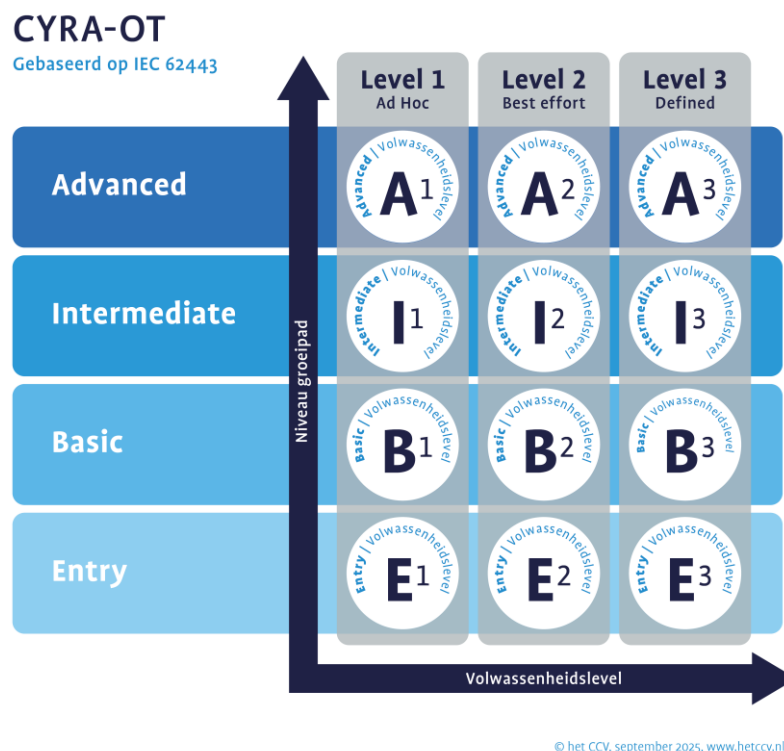
Een organisatie in de zorg moet ten minste voldoen aan de beoordelingsaspecten van niveau Entry, Level 1 (Ad Hoc) om voor een certificaat CYRA-Zorg in aanmerking te komen.

Het groeppad ten opzichte van de uit de NEN 7510-serie geselecteerde totale set beheersmaatregelen is als volgt:

- Entry = 25%
- Basic = 55%
- Intermediate = 80%
- Advanced = 100%

A.4 Toetsingskader digitale weerbaarheid van operationele technologie (deelgebied D)

Het toetsingskader voor digitale weerbaarheid van OT in deelgebied D is afgeleid van de delen 2-1 en 3-3 van de normserie IEC 62443. Het bestaat uit 12 onderdelen: de niveaus Entry, Basic, Intermediate en Advanced en op elk niveau de volwassenheidslevels 1 t/m 3. De onderlinge samenhang is zichtbaar gemaakt in figuur 5.



Figuur 5: overzicht van niveaus en volwassenheidslevels in het CYRA-toetsingskader digitale weerbaarheid van operationele technologie.

De digitale weerbaarheid van de operationele technologie moet ten minste voldoen aan de beoordelingsaspecten van niveau Entry, Level 1 (Ad Hoc) om voor een certificaat CYRA-OT in aanmerking te komen.

Het groeppad ten opzichte van de uit de IEC 62433-serie geselecteerde totale set beheersmaatregelen is als volgt:

- Entry = 30%
- Basic = 60%
- Intermediate = 80%
- Advanced = 100%

Bijlage B – Inhoudsopgave Toetsingskader CYRA

B.1 Algemeen

Het CCV heeft het Toetsingskader CYRA vastgesteld. Het beschrijft de beheersmaatregelen die organisaties behoren te nemen voor hun digitale weerbaarheid en/of weerbaarheid tegen digitale ondermijning en/of digitale weerbaarheid van OT. Aan de hand van de vragen per beheersmaatregel in het online beoordelingsinstrument bepaalt de organisatie of aan de eisen voor een beheersmaatregel is voldaan, en welk volwassenheidslevel behaald is.

B.2 Inhoudsopgave Toetsingskader CYRA-IT niveau Entry

ENTRY	NORMELEMENT UIT ISO 27001
B.2.1. Organisatie	
■ Beleidsregels voor informatiebeveiliging en privacy	5.1
■ Toegangsbeveiliging	5.15
■ Registratie en uitschrijving van gebruikers	5.16
■ Toegangsrechten	5.18
■ Rollen en verantwoordelijkheden bij informatiebeveiliging en privacy	5.2
■ Monitoring van, beoordeling van en beheer van veranderingen in de dienstverlening van leveranciers	5.22
■ Informatiebeveiliging in ongunstige situaties	5.29
B.2.2. Personeel	
■ Screening	6.1
■ Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	6.3
■ Telewerken	6.7
■ Rapportage van informatiebeveiligingsgebeurtenissen	6.8
B.2.3. Fysiek	
■ Fysieke beveiligingszone	7.1
B.2.4. Technologisch	
■ Genereren, bewaren en beoordelen van logbestanden	8.15
■ Beschermen van informatie in netwerken en ondersteunende systemen	8.20
■ Veiligheid in het gebruik van netwerkdiensten garanderen.	8.21
■ Garanderen van goed en effectief gebruik van versleuteling om vertrouwelijkheid, integriteit en beschikbaarheid te garanderen in lijn met van toepassing zijnde wet- en regelgeving.	8.24
■ Beleid voor beveiligd ontwikkelen van software en systemen	8.25
■ Informatiebeveiligingseisen in ontwerp en aanschaf van applicaties.	8.26
■ Wijzigingsbeheer	8.32

ENTRY	NORMELEMENT UIT ISO 27001
■ Beveiligde inlogprocedures.	8.5
■ Technische en organisatorische bescherming tegen malware	8.7
■ Voorkomen van exploitatie van technische kwetsbaarheden	8.8
	Paragraaf uit ISO 27701
B.2.5. Privacy	
■ Doeleinden van de organisatie	B.8.2.2
■ Registraties met betrekking tot het verwerken van persoonsgegevens	B.8.2.6

B.3 Inhoudsopgave Toetsingskader CYRA-IT niveau Basic

BASIC NIVEAU BASIC BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU ENTRY, AANGEVULD MET	NORMELEMENT UIT ISO 27001
B.3.1. Organisatie	
■ Classificatie van informatie	5.12
■ Informatiebeveiligingsbeleid voor leveranciersrelaties	5.19
■ Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	5.20
■ Toeleveringsketen van informatie- en communicatietechnologie	5.21
■ Informatiebeveiliging voor het gebruik van clouddiensten	5.23
■ Lering uit informatiebeveiligingsincidenten	5.27
■ Privacy en bescherming van persoonsgegevens	5.34
■ Gedocumenteerde bedieningsprocedures	5.37
■ Informatie en analyse over dreigingen	5.7
■ Inventarisatie van informatie en andere samenhangende bedrijfsmiddelen	5.9
B.3.2. Personeel	
■ Arbeidsvoorwaarden	6.2
■ Vertrouwelijkheids- of geheimhoudingsovereenkomst	6.6
B.3.3. Fysiek	
■ Beveiliging van bekabeling	7.12
■ Veilig verwijderen of hergebruiken van apparatuur	7.14
■ Fysieke toegangsbeveiliging	7.2
■ Kantoren, ruimten en faciliteiten beveiligen	7.3
■ Monitoren van de fysieke beveiliging	7.4
■ Beschermen tegen bedreigingen van buitenaf	7.5
■ Werken in beveiligde gebieden	7.6
■ 'Clear desk'- en 'clear screen'-beleid	7.7
■ Plaatsing en bescherming van apparatuur	7.8
■ Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	7.9

BASIC NIVEAU BASIC BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU ENTRY , AANGEVULD MET		NORMELEMENT UIT ISO 27001
B.3.4. Technologisch		
■ Beheersing van informatie die wordt opgeslagen of verwerkt op werkplekken en/of mobiele apparaten.		8.1
■ Wissen van informatie		8.10
■ Voorkomen van gegevenslekken		8.12
■ Back-up van informatie		8.13
■ Beschermen van operationele systemen door procedures en maatregelen voor de installatie van software		8.19
■ Beheren van speciale toegangsrechten		8.2
■ Beperking toegang tot informatie		8.3
		Paragraaf uit ISO 27701
B.3.5. Privacy		
■ Overeenkomst met de klant		B.8.2.1
■ Bekendmaking van onderaannemers die worden ingezet voor het verwerken van persoonsgegevens		B.8.5.6
■ Verplichtingen van klanten		B.8.2.5

B.4 Inhoudsopgave Toetsingskader CYRA-IT niveau Intermediaate

INTERMEDIATE NIVEAU INTERMEDIATE BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY EN BASIC , AANGEVULD MET:		NORMELEMENT UIT ISO 27001
B.4.1. Organisatie		
■ Aanvaardbaar gebruik van informatie en overige bedrijfsmiddelen		5.10
■ Teruggeven van bedrijfsmiddelen		5.11
■ Informatie labelen		5.13
■ Authenticatie-informatie		5.17
■ Verantwoordelijkheden en procedures		5.24
■ Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen		5.25
■ Respons op informatiebeveiligingsincidenten		5.26
■ Scheiding van taken		5.3
■ Vaststellen van toepasselijke wetgeving en contractuele eisen		5.31
■ Intellectuele eigendomsrechten		5.32
■ Beschermen van registraties		5.33
■ Naleving van beveiligingsbeleid/-normen		5.36
■ Directieverantwoordelijkheden		5.4
■ Informatiebeveiliging in projectbeheer		5.8
B.4.2. Personeel		

INTERMEDIATE NIVEAU INTERMEDIATE BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY EN BASIC , AANGEVULD MET:		NORMELEMENT UIT ISO 27001
■ Beëindiging of wijziging van verantwoordelijkheden van het dienstverband		6.5
B.4.3. Fysiek		
■ Opslagmedia		7.10
■ Nutsvoorzieningen		7.11
■ Onderhoud van apparatuur		7.13
B.4.4. Technologisch		
■ Beschikbaarheid van informatie-verwerkende faciliteiten		8.14
■ Monitoren van activiteiten		8.16
■ Kloksynchronisatie		8.17
■ Scheiding in netwerken		8.22
■ Testen van beveiliging tijdens ontwikkeling en acceptatie		8.29
■ Uitbestede softwareontwikkeling		8.30
■ Capaciteitsbeheer		8.6
		Paragraaf uit ISO 27701
B.4.5. Privacy		
■ Opdracht die inbreuk oplevert		B.8.2.4
■ Retournering, doorgifte of verwijdering van persoonsgegevens		B.8.4.2
■ Registraties van de verstrekking van persoonsgegevens aan derden		B.8.5.3

B.5 Inhoudsopgave Toetsingskader CYRA-IT niveau Advanced

ADVANCED NIVEAU ADVANCED BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY, BASIC EN INTERMEDIATE , AANGEVULD MET		NORMELEMENT UIT ISO 27001
B.5.1. Organisatie		
■ Informatietransport		5.14
■ Verzamelen van bewijsmateriaal		5.28
■ ICT-gereedheid voor bedrijfscontinuïteit		5.30
■ Onafhankelijke beoordeling van informatiebeveiliging		5.35
■ Contact met overheidsinstanties		5.5
■ Contact met speciale belangengroepen		5.6
B.5.2. Personeel		
■ Disciplinaire procedure		6.4
B.5.3. Technologisch		
■ Maskeren van gegevens		8.11
■ Speciale systeemhulpmiddelen gebruiken		8.18
■ Toepassen van web-filters		8.23

ADVANCED NIVEAU ADVANCED BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY, BASIC EN INTERMEDIATE, AANGEVULD MET	NORMELEMENT UIT ISO 27001
■ Principes voor engineering van beveiligde systemen	8.27
■ Veilig coderen	8.28
■ Scheiding van ontwikkel-, test- en productieomgevingen	8.31
■ Bescherming van testgegevens	8.33
■ Beheersmaatregelen betreffende audits van informatiesystemen	8.34
■ Toegangsbeveiliging op programmabroncode	8.4
■ Configuratiebeheer	8.9

B.6 Inhoudsopgave Normkader Digitale Ondernijning

NORMKADER DIGITALE ONDERMIJNING BEOORDELING VAN HET NORMKADER DIGITALE ONDERMIJNING VINDT PLAATS IN COMBINATIE MET BEOORDELING VAN DE BEHEERSMAATREGELEN VOOR HET GEKOZEN NIVEAU UIT HET TOETSINGKADER CYRA-IT OF CYRA-ZORG	NORMELEMENT UIT ISO 27001
■ Beleidsregels voor informatiebeveiliging en privacy Heeft de organisatie actuele beleidsregels omtrent informatiebeveiliging en privacy?	5.1
■ Informatie en analyse over dreigingen Wordt er gekeken naar bedreigingen op het gebied van informatiebeveiliging?	5.7
■ Inventarisatie van informatie en andere samenhangende bedrijfsmiddelen Worden de met informatie samenhangende bedrijfsmiddelen vastgelegd?	5.9
■ Classificatie van informatie Hanteert de organisatie een classificatiemechanisme?	5.12
■ Screening Wordt de achtergrond van personeel geverifieerd?	n.v.t., aanvullend aspect NDO 1
■ Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging Wordt kennis van het personeel op peil gebracht/gehouden?	6.3
■ Meldpunt ondernijning Wordt gebruik gemaakt van een ondernijningsmeldpunt?	n.v.t., aanvullend aspect NDO 2
■ 'User endpoint devices' Wordt gebruikersapparatuur (laptop, PC, tablet, smartphone) dat als onderdeel van de werkplek fungeert beschermd?	8.1
■ Genereren, bewaren en beoordelen van logbestanden Wordt er gebruik gemaakt van logbestanden?	8.15

B.7 Inhoudsopgave Toetsingskader CYRA-Zorg niveau Entry

ENTRY NIVEAU ENTRY BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU ENTRY VAN CYRA-IT , AANGEVULD MET		NORMELEMENT UIT NEN 7510
Organisatie		
■ HLT – Analyse en specificatie van informatiebeveiligingseisen		5.38

B.8 Inhoudsopgave Toetsingskader CYRA-Zorg niveau Basic

BASIC NIVEAU BASIC BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU BASIC VAN CYRA-IT , AANGEVULD MET		NORMELEMENT UIT NEN 7510
Organisatie		
■ HLT – Openbaar beschikbare gezondheidsinformatie		5.41

B.9 Inhoudsopgave Toetsingskader CYRA-Zorg niveau Intermediate

INTERMEDIATE NIVEAU INTERMEDIATE BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU INTERMEDIATE VAN CYRA-IT , AANGEVULD MET		NORMELEMENT UIT NEN 7510
Organisatie		
■ HLT – Zorgontvangers op unieke wijze identificeren		5.39

B.10 Inhoudsopgave Toetsingskader CYRA-Zorg niveau Advanced

ADVANCED NIVEAU ADVANCED BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU ADVANCED VAN CYRA-IT , AANGEVULD MET		NORMELEMENT UIT NEN 7510
Organisatie		
■ HLT – Validatie van getoonde/geprinte gegevens		5.40
■ HLT – Communicatie in noodsituaties		5.42
■ HLT – Incidenten extern melden		5.43

B.11 Inhoudsopgave Toetsingskader CYRA-OT niveau Entry

ENTRY			
NORMELEMENT UIT IEC 62443-2-1		NORMELEMENT UIT IEC 62443-3-3	
B.9.1. SPE 1 – Organisational security measures			
■ Security risk mitigation	ORG. 1.2		
■ Security roles and responsibilities	ORG. 1.3		
■ Security awareness training	ORG. 1.4		
■ Security risk mitigation	ORG 2.1		
B.9.2. SPE 2 – Configuration management			
■ Change control	CM 1.4	■ Software and information integrity	SR 3.4
B.9.3. SPE 3 – Network and communications security			
■ Segmentation from non-IACS zones	NET 1.1	■ Network segmentation	SR 5.1
■ Documentation of zones and network zone interconnections	NET 1.2		
■ Network accessible services	NET 1.7	■ Software process and device identification and authentication	SR 1.2
■ Wireless protocols	NET 2.1		
■ Wireless network segmentation	NET 2.2	■ Zone boundary protection	SR 5.2
■ Wireless properties and addresses	NET 2.3		
■ Remote access applications	NET 3.1	■ Access via untrusted networks	SR 1.13
■ Remote access connections	NET 3.2	■ Access via untrusted networks	SR 1.13
■ Remote access termination	NET 3.3	■ Remote session termination	SR 2.6
B.9.4. SPE 4 – Component security			
■ Component hardening	COMP 1.1	■ Least functionality	SR 7.7
■ Dedicated portable media	COMP 1.2		
■ Malware protection software validation and installation	COMP 2.3		
■ Data retention policy	DATA 1.4	Information persistence	SR 4.2
B.9.5. SPE 5 – Protection of data			
■ Key management	DATA 1.6	■ Authenticator management	SR 1.5
B.9.6. SPE 6 – User access control			

ENTRY			
NORMELEMEN UIT IEC 62443-2-1		NORMELEMEN UIT IEC 62443-3-3	
■ User identity assignment	USER 1.1	■ Human user identification and authentication	SR 1.1 RE(1)
■ User identity assignment	USER 1.1	■ Account management	SR 1.3
■ User identity removal	USER 1.2	■ Account management	SR 1.3
■ Access rights assignment	USER 1.4	■ Authorization enforcement	SR 2.1
■ Least privilege	USER 1.5	■ Account management	SR 1.3
■ Human user authentication	USER 1.8	■ Human user identification and authentication	SR 1.1
■ Consecutive login failures	USER 1.15	■ Unsuccessful login attempts	SR 1.11
■ Screen lock	USER 1.18	■ Session lock	SR 2.5
■ Component authentication	USER 1.19	■ Software process and device identification and authentication	SR 1.2
■ Authorization	USER 2.1	■ Wireless access management	SR 1.6
B.9.7. SPE 7 – Event and incident management			
■ Log entries	EVENT 1.5	■ Auditable events	SR 2.8
■ Vulnerability handling	EVENT 1.9		
B.9.8. SPE 8 – System integrity and availability			
■ Continuity management	AVAIL 1.1		

B.12 Inhoudsopgave Toetsingskader CYRA-OT niveau Basic

BASIC			
NIVEAU BASIC BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU ENTRY, AANGEVULD MET			
NORMELEMEN UIT IEC 62443-2-1		NORMELEMEN UIT IEC 62443-3-3	
B.10.1. SPE 1 – Organisational security measures			
■ Supply chain security	ORG 1.6		
■ Physical access control	ORG 3.1		
B.10.2. SPE 2 – Configuration management			
■ Asset inventory baseline	CM 1.1	■ Control system component inventory	SR 7.8
■ Infrastructure drawing/documentation	CM 1.2		
B.10.3. SPE 3 – Network and communications security			
■ Segmentation from non-IACS zones	NET 1.1	■ Network segmentation	SR 5.1 RE(1)

BASIC			
NIVEAU BASIC BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU ENTRY, AANGEVULD MET			
■ Segmentation from non-IACS zones	NET 1.1	■ Application partitioning	SR 5.4
■ Internal network access control	NET 1.6	■ Access via untrusted networks	SR 1.13
■ Internal network access control	NET 1.6	■ Zone boundary protection	SR 5.2
■ Internal network access control	NET 1.6	■ Deny by default, allow by exception	SR 5.2 RE(1)
■ Network accessible services	NET 1.7	■ Use control for portable and mobile devices	SR 2.3
■ Network time distribution	NET 1.9	■ Timestamps	SR 2.11
B.10.4. SPE 4 – Component security			
■ Malware free	COMP 2.1		
■ Security patch authenticity/integrity	COMP 3.1		
■ Security patch validation and installation	COMP 3.2		
B.10.5. SPE 5 – Protection of data			
■ Data classification	DATA 1.1	■ Protection of audit information	SR 3.9
■ Data retention policy	DATA 1.4	■ Control system recovery and reconstitution	SR 7.4
■ Cryptographic mechanisms	DATA 1.5	■ Use of cryptography	SR 4.3
■ Data Integrity	DATA 1.7	■ Communication integrity	SR 3.1
B.10.6. SPE 6 – User access control			
■ User identity assignment	USER 1.1	■ Unique identification and authentication	SR 1.6 RE(1)
■ User identity persistence	USER 1.3		
■ Session integrity	USER 1.16	■ Session integrity	SR 3.8
B.10.7. SPE 7 – Event and incident management			
■ Logging	EVENT 1.4	■ Auditable events	SR 2.8
■ Logging	EVENT 1.4	■ Audit storage capacity	SR 2.9
B.10.8. SPE 8 – System integrity and availability			
■ Backup	AVAIL 2.1	■ Control system backup	SR 7.3
■ Backup non-interference	AVAIL 2.2	■ Control system backup	SR 7.3 BR
■ Backup media	AVAIL 2.4		
■ Backup restoration	AVAIL 2.5	■ Control system recovery and reconstitution	SR 7.4 BR

B.13 Inhoudsopgave Toetsingskader CYRA-OT niveau Intermediate

INTERMEDIATE			
NIVEAU INTERMEDIATE BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY EN BASIC, AANGEVULD MET			
NORMELEMENT UIT IEC 62443-2-1		NORMELEMENT UIT IEC 62443-3-3	
B.11.1. SPE 1 – Organisational security measures			
■ Processes for discovery of security anomalies	ORG 2.2	■ Security functionality verification	SR 3.3
■ SP reviews	ORG 2.4		
B.11.2. SPE 3 – Network and communications security			
■ Segmentation from non-IACS zones	NET 1.1	■ Zone boundary protection	SR 5.2
■ User messaging	NET 1.8	■ General purpose person-to-person communication restrictions	SR 5.3
B.11.3. SPE 4 – Component security			
■ Malware protection	COMP 2.2	■ Malicious code protection	SR 3.2
■ Security patch mitigation	COMP 3.5		
B.11.4. SPE 5 – Protection of data			
■ Data confidentiality	DATA 1.2	■ Information confidentiality	SR 4.1
■ Safety system configuration mode	DATA 1.3		
■ Data Integrity	DATA 1.7	■ Protection of audit information	SR 3.9
B.11.5. SPE 6 – User access control			
■ Password protection	USER 1.11	■ Strength of password-based authentication	SR 1.7
■ Shared and disclosed/compromised passwords	USER 1.12		
■ User login failure displays	USER 1.14		
■ Concurrent sessions	USER 1.17	■ Concurrent session control	SR 2.7
■ Separation of duties	USER 2.2	■ Authorization enforcement	SR 2.1
B.11.6. SPE 7 – Event and incident management			
■ Event detection	EVENT 1.1	■ Audit log accessibility	SR 6.1
■ Event detection	EVENT 1.1	■ Auditable events	SR 2.8
■ Event detection	EVENT 1.1	■ Continuous monitoring	SR 6.2
■ Event detection	EVENT 1.1	■ Response to audit processing failures	SR 2.10
■ Incident handling and response	EVENT 1.8		
B.11.7. SPE 8 – System integrity and availability			
■ Resource availability management	AVAIL 1.2	■ Denial of service protection	SR 7.1

INTERMEDIATE			
NIVEAU INTERMEDIATE BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY EN BASIC, AANGEVULD MET			
NORMELEMENT UIT IEC 62443-2-1		NORMELEMENT UIT IEC 62443-3-3	
■ Resource availability management	AVAIL 1.2	■ Resource management	SR 7.2
■ Failure-state	AVAIL 1.3	■ Deterministic output	SR 3.6

B.14 Inhoudsopgave Toetsingskader CYRA-OT niveau Advanced

ADVANCED			
NIVEAU ADVANCED BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY, BASIC EN INTERMEDIATE, AANGEVULD MET			
NORMELEMENT UIT IEC 62443-2-1		NORMELEMENT UIT IEC 62443-3-3	
B.12.1. SPE 1 – Organisational security measures			
■ Security responsibilities training	ORG 1.5		
■ Secure developments and support	ORG 2.3		
B.12.2. SPE 2 – Configuration management			
■ Configuration settings	CM 1.3	■ Network and security configuration settings	SR 7.6
B.12.3. SPE 3 – Network and communications security			
■ Network segmentation from safety systems	NET 1.3		
■ Network disconnection from external networks	NET 1.5	■ Fail close	SR 5.2 RE(3)
B.12.4. SPE 4 – Component security			
■ Wireless network segmentation	COMP 2.2	■ Malicious code protection on entry and exit points	SR 3.2 RE(1)
■ Remote access termination	COMP 3.3		
■ Security patching retention of security	COMP 3.4		
B.12.5. SPE 5 – Protection of data			
■ Data confidentiality	DATA 1.2	■ Protection of confidentiality at rest or in transit via untrusted networks	SR 4.1 RE(1)
■ Data Integrity	DATA 1.7	■ Software and information integrity	SR 3.4
B.12.6. SPE 6 – User access control			
■ Least privilege	USER 1.5	■ Permission mapping to roles	SR 2.1 RE(2)
■ Software service authentication	USER 1.6	■ Software process and device identification and authentication	SR 1.2
■ Multifactor authentication (MFA)	USER 1.9	■ Multifactor authentication for untrusted networks	SR 1.1 RE(2)

ADVANCED NIVEAU ADVANCED BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS ENTRY, BASIC EN INTERMEDIATE, AANGEVULD MET			
■ User login display information	USER 1.13		
■ Session integrity	USER 1.16	■ Invalidation of session IDs after session termination	SR 3.8 RE(1)
■ Session integrity	USER 1.16	■ Unique session ID generation	SR 3.8 RE(2)
■ Authorization	USER 2.1	■ Authorization enforcement for all users	SR 2.1 RE(1)
■ Manual elevation of privileges	USER 2.4	■ Supervisor override	SR 2.1 RE(3)
B.12.7. SPE 7 – Event and incident management			
■ Event reporting	EVENT 1.2	■ Continuous monitoring	SR 6.2
■ Event reporting interface	EVENT 1.3	■ Continuous monitoring	SR 6.2
■ Event analysis	EVENT 1.7		
B.12.8. SPE 8 – System integrity and availability			
■ Backup	AVAIL 2.1	■ Backup verification	SR 7.3 RE(1)

Bijlage C – Volwassenheidslevels

Het certificatieschema maakt gebruik van een indeling in drie volwassenheidslevels: 1 (Ad Hoc), 2 (Best Effort) en 3 (Defined). Deze zijn ingegeven door de Capability Maturity Model Integration (CMMI) en voor CYRA vertaald naar de volgende levels:

LEVEL 1: AD HOC	LEVEL 2: BEST EFFORT	LEVEL 3: DEFINED
Aan de beheersmaatregel uit de ISO 27001/27701, de NEN 7510-serie of de IEC 62443-serie wordt op enige wijze invulling gegeven, zij het ad hoc en onvoorspelbaar. De organisatie is reactief en vaak bezig met 'brandjes blussen'. Succes is afhankelijk van individuele inspanningen.	T.o.v. level 1 wordt op een beheerste geplande wijze invulling gegeven aan ten minste de uit ISO 27001/27701, de NEN 7510-serie of de IEC 62443-serie geselecteerde onderdelen van de beheersmaatregel.	De beheersmaatregel is volledig geïmplementeerd, gestandaardiseerd en aantoonbaar. De organisatie is proactief. Implementatie voldoet op het level dat overeenkomt met de eisen voor ISO 27001/27701, de NEN 7510-serie of de IEC 62443-serie.
"Het is niet gedocumenteerd."	"Het is gedocumenteerd en we volgen de procedures."	"We hebben beleid en procedures, en volgen, toetsen en verbeteren ze periodiek."

Beantwoording van de vragen in het online beoordelingsinstrument maakt duidelijk op welk level de organisatie een beheersmaatregel heeft geïmplementeerd.



Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een onafhankelijke stichting die partijen en veiligheidsprofessionals helpt om Nederland veiliger en leefbaarder te maken.

Centrum voor Criminaliteitspreventie en Veiligheid
Churchillaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

T (030) 751 6700
E info@hetccv.nl
I www.hetccv.nl

