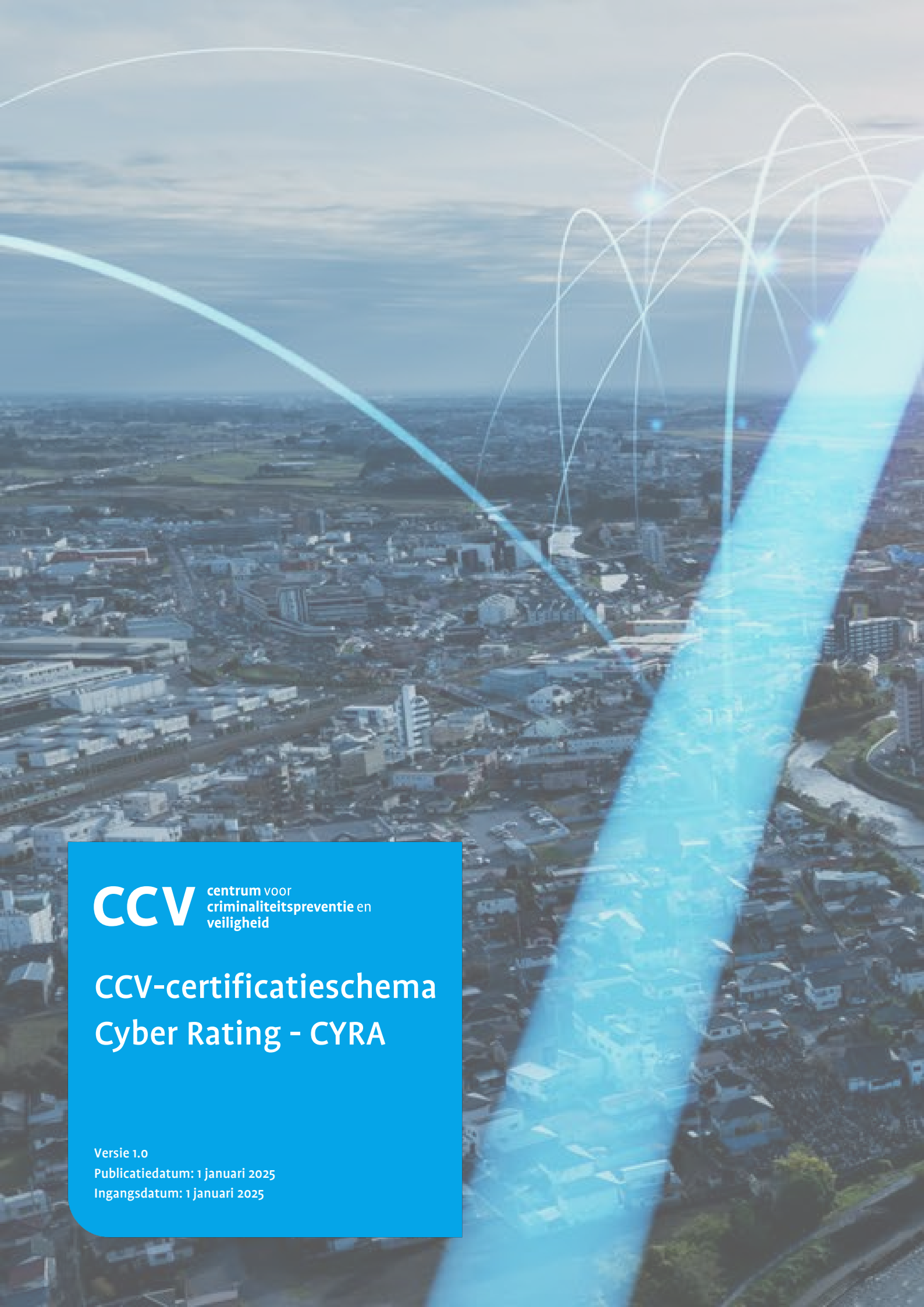


CCV centrum voor criminaliteitspreventie en veiligheid

CCV-certificatieschema Cyber Rating - CYRA

Versie 1.0
Publicatiedatum: 1 januari 2025
Ingangsdatum: 1 januari 2025

Voorwoord

Dit certificatieschema volgt de relevante eisen conform ISO/IEC 17021-1 voor managementsystemen gericht op de beoordeling van cyberweerbaarheidsniveaus (Cyber Rating) en weerbaarheid tegen digitale ondermijning.

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.

.

Inhoud

1 Inleiding

1.1 Algemeen

1.1.1 Introductie

Cybersecurity behoort een standaard onderdeel te zijn van de bedrijfsvoering van elke organisatie. Onderdeel van cybersecurity is periodieke risico-inventarisatie, evaluatie (assessment) van de cyberweerbaarheid, en het nemen van maatregelen om de cyberweerbaarheid van de organisatie te verhogen.

Een methode is opgenomen in de norm ISO/IEC 27001. Deze is 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-niveau groot zijn, waardoor organisaties een drempel ervaren om hun cyberweerbaarheid op orde te brengen.

Ook van het midden- en kleinbedrijf wordt echter verwacht dat het werkt aan cyberweerbaarheid. Organisaties in dit segment zijn vaak onderdeel van een toeleverancierskeken. Opdrachtgevers in die keten vragen onder invloed van wet- en regelgeving steeds vaker bewijs dat de toeleverancier voldoende aandacht heeft besteed aan zijn cyberweerbaarheid.

Om het midden- en kleinbedrijf te helpen met versterking van de cyberweerbaarheid is er een assessment- en certificatiemodel beschikbaar: Cyber Rating, afgekort CYRA. Dit model is gebaseerd op ISO/IEC 27001 en ISO/IEC 27701. Het biedt organisaties een duidelijk omschreven pad om te groeien naar de breedte en de volwassenheid die nodig zijn om aan die beide normen te voldoen.

1.1.2 Doel

Doel van cybersecurity is het weerbaar maken van een organisatie tegen cyberdreigingen en de mogelijke schadelijke effecten daarvan, door organisatorische, mensgerichte, technische en fysieke informatiebeveiligingsmaatregelen te nemen, zoals bijvoorbeeld beschreven in de normen ISO/IEC 27001 en ISO/IEC 27701 zodat schade wordt voorkomen en in voorkomend geval zoveel mogelijk wordt beperkt en bedrijfscontinuïteit wordt gewaarborgd.

Doel van het assessment- en certificatiemodel Cyber Rating (CYRA) is een organisatie aan de hand van criteria afgeleid van de normen ISO/IEC 27001 en ISO/IEC 27701 te helpen met het bepalen van zijn actuele niveau van cyberweerbaarheid en desgewenst de weerbaarheid tegen digitale ondermijning, en het groeipad naar het gewenste niveau.

Doel van het bepalen van het niveau van cyberweerbaarheid en de weerbaarheid tegen digitale ondermijning van een organisatie is de organisatie inzicht te geven in de huidige staat van zijn cyberweerbaarheid en desgewenst zijn weerbaarheid tegen digitale ondermijning en hem, voor zover nodig, in staat te stellen om in stappen eventuele kwetsbaarheden en risico's te verminderen of weg te nemen of te vermijden om daarmee zijn cyberweerbaarheid en zijn weerbaarheid tegen digitale ondermijning te versterken.

Doel van het onafhankelijk certificeren van het niveau van cyberweerbaarheid en weerbaarheid tegen digitale ondermijning is het onderbouwen van het vertrouwen in de eigen beoordeling die de organisatie van zijn cyberweerbaarheid of weerbaarheid tegen digitale ondermijning heeft gemaakt, en daarmee het verminderen van faal- en risicokosten voor derden die kunnen optreden als veronderstelde cyberweerbaarheid of weerbaarheid tegen digitale ondermijning 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 cyberweerbaarheid of weerbaarheid tegen digitale ondermijning inzichtelijk te maken en daarover te kunnen rapporteren.

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

- Het bieden van een herkenbare methode voor bepaling van cyberweerbaarheid en weerbaarheid tegen digitale ondermijning;
- Geharmoniseerde en consistente uitvoering;
- Informeren van de markt hoe certificatie van cyberweerbaarheidsniveaus en niveaus van weerbaarheid tegen digitale ondermijning is ingericht en wordt uitgevoerd.

1.1.3 Verantwoordelijkheden

De organisatie is verantwoordelijk voor het assessment van zijn cyberweerbaarheid en/of zijn weerbaarheid tegen digitale ondermijning, en voor 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 cyberweerbaarheidsniveau en het niveau van weerbaarheid tegen digitale ondermijning van een organisatie.

Het certificatieschema bevat:

- De eisen aan de cyberweerbaarheidsniveaus en de weerbaarheid tegen digitale ondermijning (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:

A. het cyberweerbaarheidsniveau van een organisatie, onderverdeeld in de niveaus Entry, Basic, Intermediate en Advanced, en per niveau naar volwassenheidsniveau 1. Ad Hoc, 2. Best Effort en 3. Defined, 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 cyberweerbaarheidsniveau.

B. de weerbaarheid van een organisatie tegen digitale ondermijning in combinatie met de cyberweerbaarheid van die organisatie op minimaal niveau Entry in volwassenheidsniveau 1 (Ad Hoc).

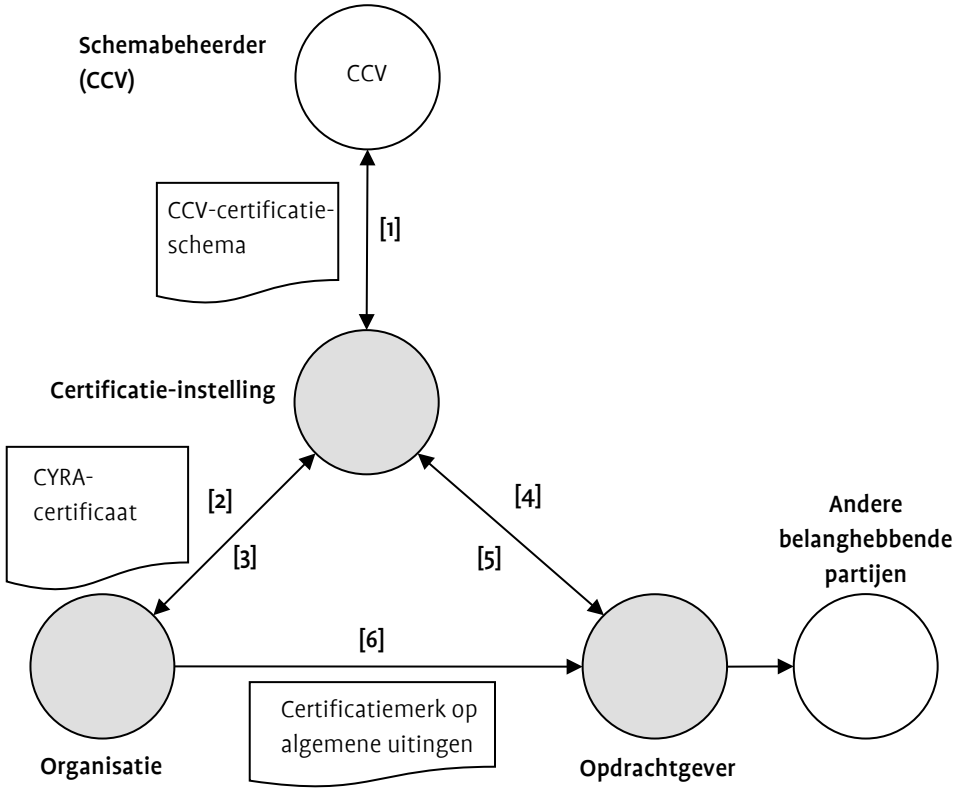
Bijlage A bevat een overzicht van het toepassingsgebied.

Organisaties kunnen zich voor een van beide gebieden of voor allebei laten certificeren. Certificatie-instellingen bieden certificatie voor beide gebieden aan.

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 cyberweerbaarheidsniveaus en niveaus van weerbaarheid tegen digitale ondermijning

Legenda:

[1] De certificatie-instelling heeft een licentieovereenkomst met het CCV (§ 4.1.1).

[2] De organisatie bepaalt het niveau van cyberweerbaarheid en/of weerbaarheid tegen digitale ondermijning (hoofdstuk 2) en vraagt certificatie aan (§ 3.2).

[3] De certificatie-instelling beoordeelt het niveau van cyberweerbaarheid en/of weerbaarheid tegen digitale ondermijning 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

Dit certificatieschema is nieuw en kent geen overgangsbepalingen.

1.6 Wijzigingen ten opzichte van de vorige versie

Dit certificatieschema is nieuw en kent geen voorgaande versie.

2 Eisen aan weerbaarheidsniveaus

2.1 Algemeen

2.1.1 Toetsingskader CYRA

De eisen voor certificatie zijn vastgelegd in het Toetsingskader CYRA. Bijlage B bevat de inhoudsopgave van het Toetsingskader CYRA. Het Toetsingskader CYRA heeft betrekking op de cyberweerbaarheid van de organisatie (2.1.2) en op de weerbaarheid van de organisatie tegen digitale ondermijning (2.1.3).

2.1.2 Eisen aan de cyberweerbaarheid van een organisatie

De eisen aan de cyberweerbaarheid 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 volwassenheidsniveaus. Bijlage C geeft een specificatie van de drie volwassenheidsniveaus 1. Ad Hoc, 2. Best effort en 3. Defined.

2.1.3 Eisen aan de weerbaarheid van een organisatie tegen digitale ondermijning

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 niveau Entry van de eisen aan de cyberweerbaarheid van de organisatie.

2.2 Eigen beoordeling

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

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

De organisatie moet voor de eigen beoordeling gebruikmaken van het online beoordelingsinstrument dat voor dit certificatieschema beschikbaar is. 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 en welk volwassenheidsniveau is behaald.

De eigen beoordeling leidt tot een eigen verklaring van de organisatie over het bereikte niveau van cyberweerbaarheid en desgewenst/of de weerbaarheid tegen digitale ondermijning. 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 cyberweerbaarheid en/of weerbaarheid tegen digitale ondermijning. 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 cyberweerbaarheid en/of weerbaarheid tegen digitale ondermijning ten minste voldoet aan de eigen verklaring als bedoeld in hoofdstuk 2.

De organisatie voorziet de certificatie-instelling onverwijld van alle opgevraagde informatie en gegevens. Het niet nakomen hiervan kan leiden tot de sancties beschreven in paragraaf 4.4 (schorsing) en 4.5 (intrekking).

3.2 Aanvraag van certificatie

3.2.1 Online beoordelingsinstrument

De organisatie doet de aanvraag met gebruikmaking van het online beoordelingsinstrument dat aan dit certificatieschema is verbonden. De organisatie maakt duidelijk of de aanvraag geldt voor de cyberweerbaarheid, de weerbaarheid tegen digitale ondermijning of voor de combinatie van deze twee.

3.2.2 Gegevens bij aanvraag

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

- Een eigen verklaring als bedoeld in paragraaf 2.2 met specificatie van het niveau Entry, Basic, Intermediate of Advanced en desgewenst/of de weerbaarheid tegen digitale ondermijning, en het volwassenheidsniveau 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 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 volwassenheidsniveau.

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 Instandhouden van het certificaat

3.3.1 Handhaven weerbaarheidsniveau

De organisatie zorgt na certificatie dat zijn cyberweerbaarheidsniveau en/of zijn weerbaarheidsniveau tegen digitale ondermijning 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 organisatie;
- Wijzigingen in de vestiging of de bedrijfsactiviteiten die van invloed zijn op het cyberweerbaarheidsniveau en/of de weerbaarheid tegen digitale ondermijning of 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 zijn eigen verklaring wil veranderen, kan hij 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 volwassenheidsniveau, 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 beoordelingsinstrument dat voor dit certificatieschema beschikbaar is, en waarin de organisatie zijn gegevens heeft geregistreerd en zijn niveau van cyberweerbaarheid en/of weerbaarheid tegen digitale ondermijning 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:

Informatiebeveiliging	Gekwalificeerd ISO 27001-auditor of:	
	Kennis	Professionele opleiding of training op universitair werk- en denkniveau
		Met succes minimaal vijf dagen training voltooid, inclusief onderwerpen als ISMS-audits en auditmanagement. Bijvoorbeeld Lead Auditor ISO 27001 certificering
		Relevante IT-beveiligingscertificeringen. Certificeringen zoals bijvoorbeeld CISSP of CISM
	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 (zoals een training waar ISO 27701 Annex B onderdeel vanuit maakt, certificering als bijvoorbeeld CIPP/E of ECPC-B dan wel praktijkervaring als Functionaris Gegevensbescherming)	
Digitale ondermijning	Aanvullend op de kwalificatie-eisen voor Informatiebeveiliging en Privacy: kennis van het Normkader Digitale Ondermijning (NDO).	

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 beoordelingsinstrument 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 beoordelingsinstrument. Een afzonderlijke rapportage wordt niet verstrekt. De organisatie vindt eventuele afwijkingen terug in het online beoordelingsinstrument zelf.

TABEL 1: TIJDSBESTEDING

	Aantal dagen tenminste
Toetsing niveau Entry	0.75*
Toetsing niveau Basic	1
Toetsing niveau Intermediate	2
Toetsing niveau Advanced	2,5
Toetsing weerbaarheid tegen digitale ondermijning	1,5 **

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

** Beoordeling van weerbaarheid tegen digitale ondermijning is inclusief toetsing van niveau Entry, en kan *niet* op afstand ('remote') plaatsvinden.

Indien de organisatie binnen 1 jaar na certificatie het niveau van zijn eigen verklaring wil veranderen, kan hij 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 Volwassenheidsniveau
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 van niveau Entry vindt in principe op afstand ('remote', online) plaats, tenzij naar het oordeel van de certificatie-instelling beoordeling op de locatie waarop de eigen verklaring betrekking heeft noodzakelijk is. Beoordeling van de andere niveaus en van de weerbaarheid tegen digitale ondermijning vindt plaats op de locatie waarop de eigen verklaring betrekking heeft.

De auditor beoordeelt in hoeverre de eigen beoordeling van de organisatie overeenkomt met de eisen van het niveau en het volwassenheidsniveau 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 volwassenheidsniveau (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 volwassenheidsniveau zijn geïmplementeerd.

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 ligt onder het bij aanvraag verklaarde niveau of volwassenheidsniveau, kan de auditor onder de volgende voorwaarden tot een positief oordeel komen over dat lagere niveau of volwassenheidsniveau:

- 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 volwassenheidsniveau.

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 cyberweerbaarheid en/of de weerbaarheid tegen digitale ondermijning niet aan het vastgestelde niveau of volwassenheidsniveau 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 cyberweerbaarheidsniveau of het weerbaarheidsniveau tegen digitale ondermijning 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 maatregen 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 oorzaakanalyse 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 schriftelijk over de schorsing, met een kopie per e-mail.

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 cyberweerbaarheidsniveau en/of het certificaat voor weerbaarheid tegen digitale ondermijning.

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 de het certificaat voor het cyberweerbaarheidsniveau en/of het certificaat voor weerbaarheid tegen digitale ondermijning 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 schriftelijk over de intrekking, met een kopie per e-mail.

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 de het certificaat voor het cyberweerbaarheidsniveau en/of het certificaat voor weerbaarheid tegen digitale ondermijning.

4.6.3 Nieuwe aanvraag

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

5 Certificatiemerk en certificaat

5.1 Certificatiemerk

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 cyberweerbaarheid van de organisatie en/of de weerbaarheid van de organisatie tegen digitale ondermijning 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 gedeponeerd.

Voor cyberweerbaarheid wordt het woordbeeldmerk aangevuld met het woordmerk Cyber Security en CYRA - IT, zoals aan de rechterzijde afgebeeld.

Voor weerbaarheid tegen digitale ondermijning wordt het woordbeeldmerk aangevuld met het woordmerk Cyber Security en CYRA - NDO, 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.

CYBER SECURITY
CYRA - IT

CYBER SECURITY
CYRA - NDO

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 voldoen aan de eisen uit 5.2.2 of 5.2.3. Een gecombineerd certificaat is niet toegestaan.

5.2.2 Certificaat cyberweerbaarheidsniveau (CYRA – IT)

Het certificaat voor het cyberweerbaarheidsniveau bevat minimaal de volgende gegevens:

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

  <Certificatie-instelling> verklaart dat het cyberweerbaarheidsniveau 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 cyberweerbaarheidsniveau <Entry – Basic – Intermediate – Advanced> in volwassenheidsniveau <Level 1 / 2 / 3>.

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

- Een uniek certificatienummer;
- De datum van uitgifte;
- De datum tot wanneer het certificaat geldig is;

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

- 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>.

5.2.3 Certificaat weerbaarheid tegen digitale ondermijning (CYRA – NDO)

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

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

<Certificatie-instelling> verklaart dat het weerbaarheidsniveau tegen digitale ondermijning 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 in volwassenheidsniveau <Level 1 / 2 / 3>.

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

- Een uniek certificatienummer;
- De datum van uitgifte;
- De datum tot wanneer het certificaat geldig is;

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

- 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.
Certificaat	Document dat de certificatie-instelling verstrekt aan de organisatie met een verklaring over het cyberweerbaarheidsniveau of het niveau van weerbaarheid tegen digitale ondermijning.
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 belanghebbende en betrokken partijen vertegenwoordigd.
EN	Europese Norm, uitgegeven door CEN of CENELEC (European Committee for (Electrotechnical) Standardization).
IEC	International Electrotechnical Commission. Een IEC-norm is een internationale norm die wordt uitgegeven door IEC.
ISMS	Information Security Management System.
ISO	International Organization for Standardization. Een ISO-norm is een Internationale norm die wordt uitgegeven door ISO.
NAW-gegevens	Gegevens die betrekking hebben op naam, adres en woonplaats.
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 cyberweerbaarheid of weerbaarheid tegen digitale ondermijning wil vaststellen, heeft vastgesteld of door een certificatie-instelling onafhankelijk wil laten beoordelen.

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.

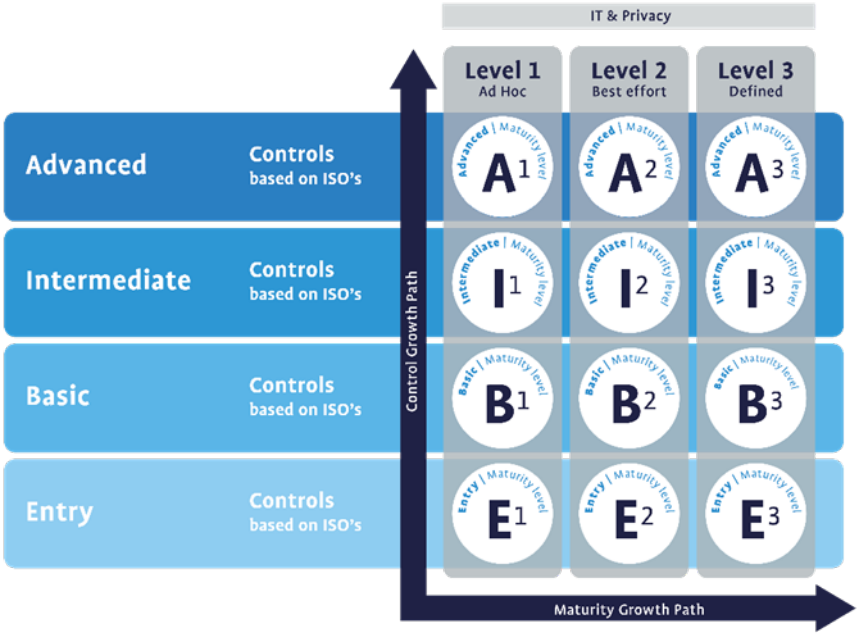
Een certificatie-instelling moet beschikken over alle normatieve normen en documenten.

NORM	ONDERWERP	VERKRIJGBAAR BIJ
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	Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems - Part 1: General	NEN, Delft
ISO/IEC 27701	Veiligheidstechnieken – Uitbreiding op ISO/IEVC 27001 en ISO/IEC 27002 voor privacy-informatiesystemen – Eisen en richtlijnen	NEN, Delft
	CCV-reglement Kwaliteitslogo	CCV, Utrecht
	CCV-reglement Beoordelen overstappende certificaathouder	CCV, Utrecht

Bijlage A - Overzicht CYRA beoordelingsniveaus en levels

A.1 Toetsingskader cyberweerbaarheid

Het toetsingskader voor cyberweerbaarheid bestaat uit 12 onderdelen: de niveaus Entry, Basic, Intermediate en Advanced en op elk niveau de volwassenheidsniveaus 1 t/m 3. De onderlinge samenhang is zichtbaar gemaakt in figuur 2.



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

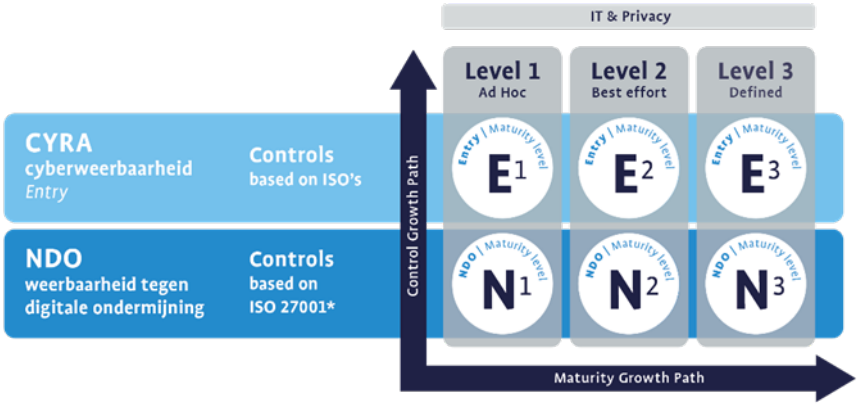
Een organisatie moet ten minste voldoen aan de beoordelingsaspecten van niveau Entry, Level 1 (Ad Hoc) om voor een certificaat CYRA-IT in aanmerking te komen.

Het groeipad 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

Het normkader Digitale Ondermijning (NDO) bestaat uit 9 beoordelingsaspecten. Deze worden in hun geheel beoordeeld in samenhang met de beoordelingsaspecten voor het niveau Entry van het toetsingskader voor cyberweerbaarheid. De onderlinge samenhang is zichtbaar gemaakt in figuur 3.



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

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 cyberweerbaarheid en/of weerbaarheid tegen digitale ondermijning. 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 volwassenheidsniveau behaald is.

De volledige tekst van de beheersmaatregelen en de te behalen volwassenheidsniveaus is opgenomen in het online beoordelingsinstrument. Ten behoeve van eenduidige koppeling met dit certificatieschema is in deze bijlage de inhoudsopgave van het online beoordelingsinstrument vermeld.

B.2 Inhoudsopgave Toetsingskader CYRA 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

ENTRY	NORMELEMENT UIT ISO 27001
■ 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
■ 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 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

BASIC NIVEAU BASIC BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU **ENTRY**, AANGEVULD MET	**NORMELEMENT UIT ISO 27001**
■ 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
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 niveau Intermediate

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

INTERMEDIATE NIVEAU INTERMEDIATE BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS **ENTRY** EN **BASIC**, AANGEVULD MET:	**NORMELEMENT UIT ISO 27001**
■ Beschermen van registraties	5.33
■ Naleving van beveiligingsbeleid/-normen	5.36
■ Directieverantwoordelijkheden	5.4
■ Informatiebeveiliging in projectbeheer	5.8
B.4.2. Personeel	
■ 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 niveau Advanced

ADVANCED NIVEAU ADVANCED BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS **ENTRY, BASIC** EN **INTERMEDIATE**, AANGEVULD MET	**NORMELEMENT 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
■ 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 Ondermijning

NORMKADER DIGITALE ONDERMIJNING BEOORDELING VAN HET NORMKADER DIGITALE ONDERMIJNING VINDT PLAATS IN COMBINATIE MET BEOORDELING VAN DE BEHEERSMAATREGELEN VOOR HET NIVEAU **ENTRY** UIT HET TOETSINGKADER CYRA	**NORMELEMENT 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 ondermijning **Wordt gebruik gemaakt van een ondermijningsmeldpunt?**	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

Bijlage C – Volwassenheidsniveaus

Het certificatieschema maakt gebruik van een indeling in drie volwassenheidsniveau: 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 niveaus:

NIVEAU 1: AD HOC	NIVEAU 2: BEST EFFORT	NIVEAU 3: DEFINED
Aan de beheersmaatregel uit de ISO 27001/27701 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. niveau 1 wordt op een beheerste geplande wijze invulling gegeven aan ten minste de uit ISO 27001/27701 geselecteerde onderdelen van de beheersmaatregel.	De beheersmaatregel is volledig geïmplementeerd, gestandaardiseerd en aantoonbaar. De organisatie is proactief. Implementatie voldoet op het niveau dat overeenkomt met de eisen voor ISO 27001/27701.

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

CCV centrum voor criminaliteitspreventie en veiligheid

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
Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

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