CCV centrum voor criminaliteitspreventie en veiligheid

CCV Certification scheme

Cyber Rating – CYRA

Version 2.0
Publication date: November 1, 2025
Effective date: Januari 1, 2026

Foreword

This certification scheme follows the relevant requirements of ISO/IEC 17021-1 for management systems, focusing on the assessment of digital resilience levels (Cyber Rating). It consists of four scopes:

- CYRA-IT – digital resilience of organisations;
- CYRA-NDO – resilience of organisations against Digital Criminal Infiltration;
- CYRA-Health Care– digital resilience of organisations in the Health Care sector;
- CYRA-OT – digital resilience of organisations that use Operational Technology (OT).

The 'Centrum voor Criminaliteitspreventie en Veiligheid' (Centre for Crime Prevention and Safety - CCV) is the administrator of the certification scheme. The Committee of Interested Parties on Cyber Security has advised positively on the adoption of this scheme.

Table of contents

1 Introduction

1.1 General

1.1.1 Background

The protection of information systems, computers and automated processes is complex. The potential damage resulting from digital vulnerabilities can be considerable, particularly for small and medium-sized enterprises (SMEs). Financial losses, the loss of business data or production capacity, and reputational damage occur frequently.

It is the responsibility of each business owner to manage the risks to their business continuity and to strengthen their resilience against cyberattacks or other digital threats. As part of a supply chain, an organisation may equally expect its partners to demonstrate digital resilience, just as those partners rely on the resilience of the organisation itself.

In many cases, merely implementing technical measures for basic digital security is not sufficient. Organisational measures are also required to ensure that the organisation as a whole is resilient to digital threats. Resilience does not only concern the prevention of cyber incidents, but also the management and mitigation of their consequences.

An essential part of cybersecurity is the periodic identification and assessment of digital risks, the evaluation of digital resilience, and the implementation of measures to improve the organisation's level of resilience.

Established methodologies are provided in the ISO/IEC 27001 standard for information security, the related NEN 7510 series (for IT in the Health Care sector), and the IEC 62443 series for Operational Technology (OT). These standards are particularly suitable for larger organisations and internationally active entities, as they are widely recognised and accepted. However, for many SMEs, achieving the level required by ISO/IEC 27001, NEN 7510 or IEC 62443 can be a considerable step, creating a threshold that hinders them from systematically improving their digital resilience. Meanwhile, clients within supply chains, increasingly influenced by legislation and regulation, are more frequently demanding evidence that their suppliers have adequately addressed their digital resilience.

To support organisations in strengthening their digital resilience, an assessment and certification model has been developed: Cyber Rating, abbreviated as CYRA. This model is based on ISO/IEC 27001 and ISO/IEC 27701 for IT systems; on the derived NEN 7510 standard series for organisations within the Health Care sector; and on parts 2-1 and 3-3 of the IEC 62443 series for organisations using Operational Technology (OT). CYRA provides organisations with a clearly defined pathway to develop the breadth and maturity required to comply with these standards.

1.1.2 Objective

The objective of cybersecurity is to make an organisation resilient to cyber threats and to mitigate their potential harmful effects. This is achieved through the implementation of organisational, human-centred, technical and physical information-security measures. Examples of frameworks for such measures include the ISO/IEC 27001 and ISO/IEC 27701 standards, the NEN 7510 series, and the IEC 62443 series. The objective of these measures is to prevent damage and, where incidents nevertheless occur, to limit their impact as much as possible, thereby safeguarding business continuity.

The objective of Cyber Rating (CYRA) assessment and certification model is to support organisations in determining their current level of digital resilience. The criteria for this assessment are derived from the aforementioned standards. Where applicable, CYRA also assists organisations in

determining their resilience against Digital Criminal Infiltration (NDO) or the digital resilience of their Operational Technology (OT). In addition, the model provides insight into the growth path towards the desired level of digital resilience.

Determining the level of digital resilience within organisations (covering IT, including NDO, OT and Health Care) aims to give the organisation clear insight into its current state of digital resilience. Where desired, this can also provide understanding of its resilience against Digital Criminal Infiltration or its digital resilience of OT. Furthermore, this process enables the organisation, where necessary, to gradually reduce, eliminate or avoid vulnerabilities and risks. In this way, the organisation can strengthen its overall digital resilience, as well as its resilience against Digital Criminal Infiltration and its digital resilience of OT.

The objective of independently certifying an organisation's level of digital resilience is to justify trust in the organisation's own assessment. This applies to the assessment of digital resilience, resilience against Digital Criminal Infiltration, and digital resilience of OT. Independent certification also contributes to reducing the failure- and risk-related costs for third parties, which may arise if the assumed levels of digital resilience, resilience against Digital Criminal Infiltration or digital resilience of OT are, in reality, absent.

A CYRA certificate enables the organisation, based on its own ambitions as well as client requirements, to demonstrate and report the achieved level of digital resilience, resilience against Digital Criminal Infiltration, or digital resilience of OT.

Defining the levels of digital resilience derived from the ISO/IEC 27001, ISO/IEC 27701, NEN 7510 and IEC 62443 standards, together with the levels of resilience against Digital Criminal Infiltration and digital resilience of OT, and the procedures applied by the certification body for their assessment, serves the following objectives:

- to provide a recognisable method for determining digital resilience, resilience against Digital Criminal Infiltration and digital resilience of OT;
- to ensure harmonised and consistent implementation;
- to inform the market about the way certification of digital resilience levels, resilience against Digital Criminal Infiltration and digital resilience of OT is structured and carried out.

1.1.3 Responsibilities

The organisation is responsible for conducting the assessment of:

- its digital resilience, and/or
- its resilience against Digital Criminal Infiltration (NDO), and/or
- its digital resilience of OT.

In addition, the organisation is responsible for defining and implementing the control measures required to achieve the desired level.

1.1.4 Reading guide

The requirements and conditions set out in this certification scheme are applied in the processing of an application for a certificate relating to an organisation's level of digital resilience, its level of resilience against Digital Criminal Infiltration, or its level of digital resilience of OT.

This certification scheme contains:

- the requirements for the levels of digital resilience, resilience against Digital Criminal Infiltration, and digital resilience of OT (Chapter 2);
- the conditions for certification (Chapter 3);
- the harmonised procedures that the certification body shall apply when processing a certification application (Chapter 4);

- a description of the certificate issued by the certification body to the organisation, and the certification mark to be applied (Chapter 5).

1.2 Scope

The scope of this certification scheme concerns the certification of the following subdomains:

A. CYRA-IT: the level of digital resilience of an organisation, divided into the levels Entry, Basic, Intermediate and Advanced, and within each level into the maturity levels Ad Hoc (1), Best Effort (2) and Defined (3). This subdomain is intended for organisations for which the ISO/IEC 27001 and ISO/IEC 27701 standards do not yet offer a practical solution, but which wish or are required to gain insight into their level of digital resilience.

B. CYRA-NDO: the resilience of an organisation against Digital Criminal Infiltration, assessed according to the maturity levels Ad Hoc (1), Best Effort (2) and Defined (3), in combination with the organisation's digital resilience as described under subdomain A or C, at a minimum of Entry level and Ad Hoc (1) maturity levels.

C. CYRA-Health Care: The level of digital resilience of an organisation in the Health Care sector, divided into the levels Entry, Basic, Intermediate and Advanced, and within each level into the maturity levels Ad Hoc (1), Best Effort (2) and Defined (3). This subdomain is intended for organisations for which the NEN 7510 standard series does not yet provide a practical solution, but which wish or are required to gain insight into their level of digital resilience.

D. CYRA-OT: The level of digital resilience of OT, divided into the levels Entry, Basic, Intermediate and Advanced, and within each level into the maturity levels Ad Hoc (1), Best Effort (2) and Defined (3). This subdomain is intended for organisations for which parts 2-1 and 3-3 of the IEC 62443 standard series do not yet offer a practical solution, but which wish or are required to gain insight into the digital resilience of their operational technology.

Annex A provides an overview of the scope.

Organisations can be certified for one or more subdomains. Certification for subdomain B is only possible in combination with subdomain A or C.

Certification bodies can obtain a licence for this certification scheme either for the complete scheme or for the specific subdomain(s) for which they intend to conclude certification contracts. A licence for subdomain A and/or C automatically includes subdomain B. The certification body is not permitted to conduct assessments outside the scope of its licence.

1.3 Relation to laws and regulations

The certification scheme is not driven by legislation and regulations. The certification scheme is governed by private law and does not contain any legal requirements.

1.4 Relationship chart

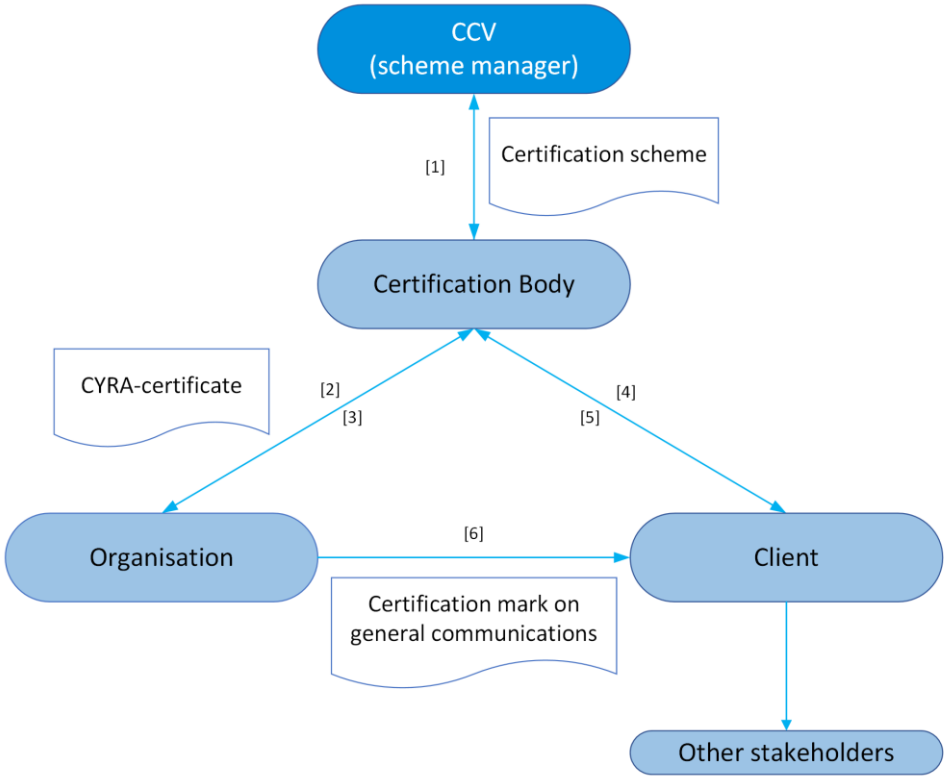

Figure 1 – Overview of parties involved in the certification of levels of digital resilience, resilience against Digital Criminal Infiltration, and digital resilience of OT

Legend:

[1] The certification body holds a licence agreement with the CCV (§ 4.1.1).

[2] The organisation determines its level of digital resilience and/or resilience against Digital Criminal Infiltration and/or digital resilience of OT (see Chapter 2) and submits an application for certification (§ 3.2).

[3] The certification body assesses the level of digital resilience and/or resilience against Digital Criminal Infiltration and/or digital resilience of OT that the organisation has determined for itself (see Chapter 4).

[4] The CYRA certificate signals justified trust to the market.

[5] Clients can submit complaints to the certification body if the organisation has not handled them appropriately.

[6] The organisation can use the certification mark in general communications if the specified requirements are met. Use of the certification mark on products or services is not permitted.

1.5 Transitional Provisions

1.5.1 For certificate holders of subdomains A and B

Version 2.0 of this certification scheme enters into force on January 1, 2026. Certificate holders for subdomains A and B are required to comply with version 2.0 from that date onwards. Subdomains C and D are newly introduced; therefore, no transitional arrangements apply to these subdomains.

This certification scheme can be applied from the date of publication.

1.5.2 For certification bodies

A licence for version 1.0 will automatically be converted on the effective date into a licence for subdomains A and B of version 2.0. Version 1.0 will expire on 1 July 2026, after which certification bodies will no longer make certification decisions in accordance with version 1.0.

Version 2.0 will be applied from the effective date for all new certification applications. Certification bodies holding a licence for version 1.0 can continue to process certification applications for subdomains A and B. Certification applications for subdomains C and D can be processed if the certification body has agreed with the CCV to extend its licence to include these subdomains.

Any additional assessment will, as of January 1, 2026, be carried out against all requirements of version 2.0. The provisions set out in paragraph 4.3.3.4 apply accordingly.

1.6 Changes compared to the previous version

The main changes in version 2.0 compared to version 1.0 are as follows:

- The scope in section 1.2 has been expanded with subdomain C (CYRA-Health Care) and subdomain D (CYRA-OT). The text in the Foreword and several paragraphs in Chapter 1 have been updated accordingly;
- The term cyber resilience has been replaced with digital resilience;
- A transitional arrangement has been added in section 1.5 for certificate holders and certification bodies;
- In section 2.1, the requirements for subdomains C (CYRA-Health Care) and D (CYRA-OT) have been included;
- Section 2.2 now specifies that the online CCV self-assessment tool CYRA will be used as the basis for certification;
- The intent of Chapters 3, 4 and 5 has been adjusted to reflect the broader scope of the scheme, now including CYRA-Health Care and CYRA-OT;
- In section 4.3.1.2, qualification requirements have been added for certification personnel engaged in CYRA-OT assessments;
- The qualification requirements in section 4.3.1.2 for CYRA-IT have been updated in line with changes to ISO 27006;
- In section 4.3.3.1, the time allocation for the assessment of CYRA-OT has been added;
- Section 5.1 includes the certification marks for CYRA-Health Care and CYRA-OT, and section 5.2 contains the provisions for their use. In addition, the requirements for the certification statement and the content of the certificates have been revised;
- Section 6.2 includes new terms and abbreviations to reflect the expanded scope of the scheme towards CYRA-Health Care and CYRA-OT;
- Section 6.3 includes additional normative references in relation to the expanded scope of the scheme towards CYRA-Health Care and CYRA-OT;
- Annex A has been expanded with overviews of the assessment levels for CYRA-Health Care (section A.3) and CYRA-OT (section A.4);
- Annex B has been expanded with the table of contents for the assessment model of CYRA-Health Care (subdomain C) and CYRA-OT (subdomain D).

2 Requirements for digital resilience levels

2.1 General

2.1.1 CYRA Assessment Model

The certification requirements are defined in the CYRA Assessment Model.

The CYRA Assessment Model covers the digital resilience of the organisation (2.1.2), the resilience of the organisation against Digital Criminal Infiltration (2.1.3), the digital resilience of the organisation in the Health Care sector (2.1.4), and the digital resilience of the organisation with OT (2.1.5).

The CCV publishes the full text of the control measures and the corresponding maturity levels on its website www.hetccv.nl. These are included in the online CCV self-assessment tool, available at https://cyberrating.nl/. For clarity and alignment with this certification scheme, Annex B lists the table of contents of the online self-assessment tool. The version published at https://cyberrating.nl/ is leading and authoritative.

2.1.2 Requirements for the digital resilience of an organisation (CYRA-IT)

The requirements for the digital resilience of an organisation are derived from the standards ISO/IEC 27001 and ISO/IEC 27701, and are specified across four levels: Entry, Basic, Intermediate and Advanced; Each level is divided into three maturity levels. Annex C provides a specification of these three maturity levels: 1. Ad Hoc, 2. Best effort and 3. Defined.

2.1.3 Requirements for the resilience of an organisation against digital criminal infiltration (CYRA-NDO)

The requirements for the resilience of an organisation against Digital Criminal Infiltration represent a specific application of the requirements set out in ISO/IEC 27001, supplemented with requirements for business processes that are essential for strengthening resilience against Digital Criminal Infiltration. The requirements for resilience against Digital Criminal Infiltration apply in combination with, at minimum, the Entry level of the requirements for an organisation's digital resilience. The maturity level of an organisation's resilience against Digital Criminal Infiltration will be at least equal to the maturity level of its overall digital resilience.

2.1.4 Requirements for the digital resilience of an organisation in the health care sector (CYRA-Health Care)

The requirements for the digital resilience of an organisation in the Health Care sector are derived from the NEN 7510 standard series and are specified across four levels: Entry, Basic, Intermediate and Advanced. Each level is divided into three maturity levels. Annex C provides a specification of these three maturity levels: 1. Ad Hoc, 2. Best effort and 3. Defined.

2.1.5 Requirements for the digital resilience of OT (CYRA-OT)

The requirements for the digital resilience of OT within an organisation are derived from parts 2-1 and 3-3 of the IEC 62443 standard series and are specified across four levels: Entry, Basic, Intermediate and Advanced. Each level is divided into three maturity levels. Annex C provides a specification of these three maturity levels: 1. Ad Hoc, 2. Best effort and 3. Defined.

2.2 Self-Assessment

The organisation will carry out its own assessment of its level of digital resilience, and/or its resilience against Digital Criminal Infiltration, and/or its digital resilience of OT.

For each level, the organisation will determine the maturity level for every control measure.

The organisation will use the online self-assessment tool made available by the CCV for this certification scheme via https://cyberrating.nl/. This tool contains all the requirements from the CYRA Assessment Model as established by the CCV. Based on questions for each control measure, the organisation determines the level at which the control measures have been implemented (Entry, Basic, Intermediate or Advanced) and the maturity level achieved (1. Ad Hoc, 2. Best Effort, or 3. Defined).

The self-assessment results in the organisation's own declaration of the achieved level of digital resilience, resilience against Digital Criminal Infiltration, and/or digital resilience of OT. This declaration forms the starting point for certification.

3 Conditions for certification

3.1 General

The organisation can request the certification body to carry out an independent assessment of its self-declaration concerning its digital resilience, its digital resilience in the Health Care sector, its resilience against Digital Criminal Infiltration, and/or its digital resilience of OT. This chapter describes how the application process works, what is required, and which conditions apply during the validity period of the certificate.

At the time of application (paragraph 3.2) and throughout the validity period of the certificate (paragraph 3.3), the organisation will always be able to demonstrate to the certification body that its level of digital resilience, resilience against Digital Criminal Infiltration, and/or digital resilience of OT meets at least the level declared in its self-declaration, as described in Chapter 2.

The organisation will immediately provide the certification body with all requested information and data. Failure to comply with this requirement can lead to the sanctions described in paragraphs 4.5 (Suspension) and 4.6 (Withdrawal).

3.2 Application for certification

3.2.1 Online assessment tool

The organisation submits its application using the online CCV self-assessment tool associated with this certification scheme. The organisation specifies whether the application concerns digital resilience, digital resilience in the Health Care sector, resilience against Digital Criminal Infiltration, a combination of these, and/or digital resilience of OT.

3.2.2 Required information for application

When applying for certification, the organisation provides the following information to the certification body:

- A self-declaration generated from the CCV self-assessment tool, as referred to in paragraph 3.2.1, covering digital resilience (including, where applicable, digital resilience in the Health Care sector), specifying the level (Entry, Basic, Intermediate or Advanced) and/or resilience against Digital Criminal Infiltration, and/or digital resilience of OT, specifying the level (Entry, Basic, Intermediate or Advanced) and the corresponding maturity level (1. Ad Hoc, 2. Best Effort or 3. Defined) to which the assessment applies;
- Proof of legal registration indicating the nature of the business operations and activities;

> In the Netherlands, this is demonstrated through registration in the Trade Register of the Chamber of Commerce. Online consultation of the Trade Register is accepted.

- A declaration by an authorised representative confirming that the organisation will comply with the requirements, conditions and obligations set out in this certification scheme;

> This can, for example, be signed by the managing director, a member of the management team, or the quality manager.

- The location, or in the case of multiple sites, an overview of all locations or organisational units to which the self-declaration applies;
- The activities of the organisation covered by the self-declaration.

The organisation will also provide the certification body, upon request, with any additional information and data required.

To qualify for certification, the organisation will have implemented each control measure at the maturity level corresponding to the applied level of certification.

3.2.3 Status during the application process

During the evaluation of the application, the organisation is not permitted to publish any reference to the certification application. However, it can refer to the application in individual communications and contracts.

3.3 Maintenance of the certificate

3.3.1 Maintaining the level of resilience

After certification, the organisation will ensure that its level of digital resilience, and/or its resilience against Digital Criminal Infiltration, and/or its digital resilience of OT continues to meet, throughout the validity period of the certificate, at least the level determined during the assessment.

3.3.2 Changes

The organisation will promptly report relevant developments and changes within the organisation to the certification body, including but not limited to:

- Contractually and legally reportable cybersecurity incidents;
- Mergers and acquisitions;
- Changes in location or business activities that affect the level of digital resilience, resilience against Digital Criminal Infiltration, and/or digital resilience of OT, or that impact the application of this certification scheme;
- Changes in the content or status of other certificates, insofar as these influence the implementation of this certification scheme.

3.4 Change of level

If the organisation wishes to change the level stated in its self-declaration within one year after certification, it can request a new certification assessment for the desired level. The application process will follow the provisions set out in section 3.2.

If the certificate was issued more than one year ago, an organisation wishing to obtain certification for a different level or a different maturity level will submit a new application in accordance with section 3.2.

3.5 Continuation of certification

Upon expiry of the validity of the certificate, the organisation can submit a new application for certification in accordance with section 3.2.

NOTE for clarification

When the certificate expires, the organisation will lose the right to use the certification mark. See section 5.1.3.

4 Requirements for the application of certification

4.1 General

This chapter defines harmonised procedures for the application of this certification scheme by certification bodies. These procedures are binding for all certification bodies involved.

4.2 Requirements for the certification body

4.2.1 General

Certification bodies can enter into certification contracts for CYRA certification with organisations if they hold a valid accreditation for assessments in accordance with ISO/IEC 27006-1 or ISO/IEC 27001, and have a valid licence agreement with the CCV for this certification scheme.

The model agreement for certification bodies is published on the CCV website: www.hetccv.nl.

NOTE
This certification scheme is not yet conducted under accreditation.

4.2.2 Relationship with and use of ISO/IEC 17021-1

This certification scheme is based on the application of ISO/IEC 17021-1.

Where the certification scheme does not provide detailed guidance, the certification body will define and document the necessary level of detail and bring this to the harmonisation meeting with the CCV.

Certification bodies can apply their own regulations and procedures, provided these do not conflict with this certification scheme. In the event of a conflict, the provisions of this certification scheme are binding.

Documents and interpretations issued by the accreditation organisation, both nationally and internationally, that relate to ISO/IEC 17021-1 are applicable.

NOTE
ISO/IEC 17021-1 and the related documents, such as the IAF MD documents, already provide extensive direction for the quality level and harmonisation of the application of certification under ISO/IEC 17021-1.
This certification scheme is therefore limited to those subjects that are not harmonised within ISO/IEC 17021-1 and its related documents, but for which harmonisation is desirable.
Clients of the certification body cannot derive from this scheme the procedural aspects of certification; section 4.2.3 provides the relevant guidance for those aspects.

4.2.3 Communication with the organisation

4.2.3.1 Provision of Information about the scheme

The certification body will be able to provide, during information sessions or upon request by the organisation, detailed information regarding:

- the content, context and purpose of the certification scheme;
- the content, context and purpose of ISO/IEC 17021-1, and the related documents linked to its national and international application;
- the procedures, methods and regulations to be followed, including but not limited to:
  - Application;
  - Estimation of time and costs for conducting the certification assessment;
  - Planning;
  - Audit plan;
  - Use of certification marks;
  - Nonconformities and corrective actions;
  - Suspension and withdrawal;
  - Appeals and disputes;
  - Termination of the certification contract.

This information can be of a general nature or can relate to specific parts of the certification scheme.

4.2.3.2 Online assessment tool

The certification body will use the online CCV assessment tool available through https://cyberrating.nl/ for this certification scheme to assess the organisation's self-declaration. This tool contains the data registered by the organisation and reflects its determined levels of digital resilience, resilience against Digital Criminal Infiltration, and/or digital resilience of OT.

4.2.3.3 Benchmarking

Using the online assessment tool referred to in section 4.2.3.2, the certification body collects anonymised data from organisational assessments for the purpose of benchmarking. The data to be collected and the method of processing will be further agreed between the scheme manager and the certification body. The certification body will arrange, within the certification contract, the organisation's consent for the collection and processing of anonymised data.

4.3 Requirements for the application of certification

4.3.1 Qalifications

4.3.1.1 General

The certification body will document and maintain verifiable records of the qualifications of all certification personnel involved. The certification body will demonstrate that its certification personnel meet the qualification criteria specified in this certification scheme. These qualification criteria are described as competence requirements (knowledge and skills).

The certification body will establish a training programme for newly qualifying certification personnel, aimed at ensuring compliance with the required competence criteria.

For qualified certification personnel, the certification body will establish a programme for monitoring and evaluating their performance.

The determining factor for qualification is the competence of the personnel. Education, experience and other skills can contribute to demonstrating the required competences.

The certification body will define competences in sufficient detail to meet the requirements of ISO/IEC 17021-1. This applies not only to the auditors involved, but to all certification personnel participating in the certification process, including but not limited to:

- Processing applications and quotations;
- Qualifying certification personnel;
- Monitoring certification personnel;
- Reviewing audit reports;
- Making certification decisions;
- Administrative processing of certificates;
- Handling complaints.

4.3.1.2 Specific requirements for auditors

For this certification scheme, the following minimum qualifications apply:

Subdomain A	**Information Security**	Qualified ISO 27001 Auditor, or:	
		Knowledge	Higher Professional Education (HBO) working and thinking level.
			Understanding of the content, intent and context of the control measures from the standard.
			Relevant education in IT security or ICT, combined with appropriate training in ISMS auditing and audit management.
		Experience	At least two years of full-time practical experience in an information-security role or function.
			Experience gained through participation in at least four ISMS audits, including at least one initial audit and one mid-cycle audit. This participation includes assessment of documentation, risk assessments, implementation reviews and preparation of audit reports.
	Privacy	Demonstrable privacy knowledge or experience regarding data processors, for example through training that includes ISO 27701 Annex B, certification such as CIPP/E or ECPC-B, or practical experience as a Data Protection Officer.	
Subdomain B	**Digital Criminal Infiltration**	In addition to the qualification requirements for Information Security and Privacy as set out for subdomains A and/or C: Knowledge of the Normative Framework for Digital Criminal Infiltration (NDO).	
Subdomain C	**Information Security in the Health Care Sector**	Qualified NEN 7510 Auditor for Administrators (B) or Health-Care Institutions (Z), of:	
		Knowledge	Higher Professional Education (HBO) working and thinking level.
			Understanding of the content, intent and context of the control measures from the standard.
			Relevant education in IT security or ICT, combined with appropriate training in ISMS auditing and audit management.
		Experience	At least two years of full-time practical experience in an information-security role or function.

			Work experience in, or demonstrable knowledge of, the Health Care sector.
			Experience gained through participation in at least four ISMS audits, including at least one initial audit and one mid-cycle audit. This participation includes assessment of documentation, risk assessments, implementation reviews and preparation of audit reports.
	Privacy	Demonstrable privacy knowledge or experience regarding data processors, for example through training that includes ISO 27701 Annex B, certification such as CIPP/E or ECPC-B, or practical experience as a Data Protection Officer.	
Subdomain D	The qualification requirements for Information Security as defined under subdomain A apply, plus: ISA-certification as Risk Assessment Specialist (https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program) or a recognised certificate covering at least parts 2-1 and 3-3 of IEC 62443 or Demonstrable training in Operational Technology (OT), such as (not limited to) the ISA IC-32 training certificate (https://www.isa.org/training/course-description/ic32).		

4.3.2 Processing of applications

The certification body will process every application and verify that all information provided is complete and accurate. The certification body will request any additional information required to process the application and to prepare the corresponding quotation and schedule.

If the applicant already holds a valid certification agreement with another certification body, the certification body will process the application in accordance with the CCV Regulation on the Assessment of Transferring Certificate Holders.

4.3.3 Performance of assessments

4.3.3.1 Minimum audit time

The minimum required audit time is specified in Table 1 and is based on a single organisation operating from a single location. Audit time includes preparation time but excludes travel time.

The assessment will be conducted using the online CCV self-assessment tool, in which the organisation has entered its data and recorded its self-declaration. The auditor will base the assessment on this information and record all findings directly in the online CCV self-assessment tool. A separate audit report will not be issued; any identified nonconformities will be visible within the tool itself.

TABLE 1 – TIME ALLOCATION		
Assessment Level	Minimum Number of Days for Subdomains A and C	Minimum Number of Days for Subdomain D
Assessment of level Entry	0.75*	1
Assessment of level Basic	1.5	2
Assessment of level Intermediate	2	3
Assessment of level Advanced	2.5	3.5
Assessment of resilience against Digital Criminal Infiltration according to subdomain B (in addition to subdomain A or C)	0.5**	

* Assessment of level Entry will, in principle, be conducted remotely, see section 4.3.3.2.

** In addition to the assessment time for Entry, Basic, Intermediate or Advanced. Assessment of resilience against Digital Criminal Infiltration in combination with level Entry cannot be conducted remotely.

If the organisation wishes to change the level of its self-declaration within one year after certification, it can request a new certification assessment for the desired level. In that case, the time allocation specified in Table 2 will apply.

TABLE 2 – TIME ALLOCATION FOR CHANGE OF LEVEL				
	From Entry to	From Basic to	From Intermediate to	Adjustment of Maturity Level
To Entry				1 day
To Basic	0.5 day			1 day
To Intermediate	1.5 days	1 day		1 day
To Advanced	2 days	1.5 days	0.5 day	1 day

4.3.3.2 Assessment

The assessment will take place at the location to which the organisation's self-declaration applies. An exception applies for assessments at level Entry within subdomains A and C, which will, in principle, be conducted remotely (online), unless the assessment is combined with the assessment of resilience against Digital Criminal Infiltration in subdomain B, or unless, in the opinion of the certification body, an on-site assessment is necessary at the location covered by the self-declaration.

The auditor will assess the extent to which the organisation's self-assessment aligns with the requirements of the level and maturity level specified in the application. To this end, the auditor will validate the control measures corresponding to the chosen level (Entry, Basic, Intermediate, or Advanced) at the declared maturity level (Ad Hoc, Best Effort, or Defined), and, where applicable, the control measures relating to resilience against Digital Criminal Infiltration. To reach a positive conclusion, all control measures must be implemented at least at the chosen level and declared maturity level. If subdomain B is part of the assessment, the achieved maturity level of resilience against Digital Criminal Infiltration must be at least equal to the maturity level of the organisation's digital resilience.

If the auditor identifies a nonconformity, a positive conclusion cannot be reached until the issue has been corrected. Where the number of nonconforming control measures is less than 15% (rounded up) and the organisation resolves the identified nonconformities within eight weeks, a re-assessment can take place. Otherwise, the organisation will need to submit a new application. A re-assessment can be conducted remotely if, in the opinion of the auditor, the corrective actions allow for it.

If the organisation has not implemented a (part of a) control measure, the auditor cannot reach a positive conclusion unless the organisation provides justification that the (part of the) control measure is not applicable. If the implemented and demonstrated control measures collectively meet the requirements of a level immediately below the level or maturity level declared in the application, the auditor can reach a positive conclusion for that lower level or maturity level under the following conditions:

- The authorised person who submitted the certification application is available for consultation during the audit; and
- The authorised person agrees, before the audit is finalised, to certification at the next lower level or maturity level.

If all requirements for the applied-for level are met, the auditor can reach a positive conclusion.

In that case, the certification body will issue the organisation a certificate as referred to in chapter 5. The certificate will be valid for two years.

4.3.3.3 Supervision

The certification body is responsible for supervising the certificate holder throughout the validity period of the certificate.

4.3.3.4 Additional assessment

The certification body can conduct additional audits when there is reason to do so. Possible reasons include:

- Cybersecurity incidents reported by the organisation under section 3.2.2;
- Complaints indicating that the level of digital resilience and/or resilience against Digital Criminal Infiltration and/or the digital resilience of OT does not meet the established level or maturity level;
- Complaints regarding misleading or incorrect use of the certification mark;
- Publications about cybersecurity incidents;
- Observations made by the certification body itself;
- Information from interested parties, such as government bodies and/or insurers.

If, during the additional assessment, the auditor identifies a situation that does not comply with the requirements, a nonconformity will be recorded. Nonconformities can include:

- Failure to maintain compliance with one of the requirements of this certification scheme, or
- Failure to meet one or more conditions of this certification scheme (including financial obligations or rules for the use of the certification mark).

The certification body will communicate the nonconformities to the organisation at the conclusion of the assessment. For the correction of the nonconformity(ies), section 4.4 applies. For the application, reporting, review, decision-making and possible sanctions, the provisions set out in this certification scheme apply.

4.3.4 Complaints and appeals

The certification body will handle complaints and appeals in accordance with its own regulation, which is applied under the applicable accreditation.

4.3.5 Publication

The certification body will not publish any information about organisations that have applied for certification or about organisations that have been certified regarding their level of digital resilience, their level of resilience against Digital Criminal Infiltration, or the level of digital resilience of OT.

4.4 Correction of nonconformities

4.4.1 Corrective measures

If, during an additional assessment, the auditor identifies one or more nonconformities, the organisation will have eight weeks to take corrective measures. These corrective measures will at least include:

- An analysis focusing on the root cause or causes of the nonconformity. This analysis will identify both the scope and the potential causes;
- Actions required to eliminate the nonconformity (correction);
- Solutions aimed at preventing recurrence and ensuring control over these issues (corrective measures);
- Identification of the person responsible for the improvement actions and corrective measures;
- A defined deadline for completion of the improvement actions (correction and corrective measures);
- An assessment of the effectiveness of the improvement actions and the implementation of the solutions.

The organisation will document and implement the plan for corrective measures in full. The certification body will verify the implementation and effectiveness of these measures.

4.4.2 Assessment of correction by the certification body

The certification body will assess the execution of the corrections and the implementation of the corrective measures to determine that the nonconformity has been resolved. The method of assessment will depend on the nature of the nonconformity. Where necessary, an additional assessment will be carried out for verification purposes.

The certification body will apply the timeframes and procedures as defined in its own regulations.

4.5 Suspension

4.5.1 Suspension

The certificate will be suspended:

- When an improvement plan does not provide sufficient assurance that corrections will be carried out and/or does not adequately ensure completion of the root cause analysis and implementation of corrective measures (see section 4.4.1); or
- When the corrective measures for nonconformities have not resulted in resolution of the nonconformity or nonconformities within the specified timeframe (see section 4.4.1); or
- When the organisation does not comply with the conditions for certification (including financial obligations and obligations relating to the use of the certification mark) (see section 3.1).

The certification body will fully document the assessor's recommendation, the review and decision-making process, and the final decision, including justification.

The certification body will inform the organisation of the suspension by email.

4.5.2 Consequences of suspension

From the moment of suspension, the organisation is not permitted to use the certification mark or to make any reference to the certificate for the level of digital resilience, the certificate for resilience against Digital Criminal Infiltration, or the certificate for the level of digital resilience of OT.

4.5.3 Lifting of suspension

When the certification body determines that all identified nonconformities have been resolved, the suspension will be lifted. The certification body will notify the organisation of this in writing.

From the date stated in the written notice issued by the certification body, the use of the certification mark and reference to the certificate for the level of digital resilience, the certificate for resilience against Digital Criminal Infiltration, or the certificate for the level of digital resilience of OT will be permitted again.

A suspension will last for a maximum period of six months.

4.6 Withdrawal

4.6.1 Withdrawal

The certificate will be withdrawn if the organisation is unable to resolve the identified nonconformities within the suspension period.

The certification body will inform the organisation of the withdrawal by email.

4.6.2 Consequences of withdrawal

From the moment of withdrawal, the organisation is not permitted to use the certification mark or to make any reference to the certificate for the level of digital resilience, the certificate for resilience against Digital Criminal Infiltration, or the certificate for the level of digital resilience of OT.

4.6.3 New application

An organisation whose certificate for the level of digital resilience, the certificate for resilience against Digital Criminal Infiltration, or the certificate for the level of digital resilience of OT has been withdrawn can submit a new application for certification under this certification scheme.

5 Certification mark and certificate

5.1 Certification mark

The certification mark, hereinafter referred to as the mark, serves as evidence to clients that, based on the assessment conducted by the certification body, there is justified trust that the organisation's level of digital resilience, its resilience against Digital Criminal Infiltration, and/or its level of digital resilience of OT meets the requirements set out in this certification scheme (as described in Chapter 2), and that all contractual and regulatory conditions have been fulfilled.

The mark consists of a combination of a visual and textual element, as described in section 5.1.1.

Only the use of the mark as described in this certification scheme is permitted.

5.1.1 Certification marks

The word and image mark shown on the left is associated with this certification scheme. This word and image mark is a registered trademark.

For digital resilience under subdomain, the word and image mark is supplemented with the word mark Cyber Security and CYRA-IT, as shown on the right.

For resilience against Digital Criminal Infiltration under subdomain B, the word and image mark is supplemented with the word mark Cyber Security and CYRA-NDO, as shown on the right. This mark can only be used in combination with the mark for subdomain A or C.

For digital resilience under subdomain C, the word and image mark is supplemented with the word mark Cyber Security and CYRA-Health Care, as shown on the right.

For the digital resilience of OT under subdomain D, the word and image mark is supplemented with the word mark Cyber Security and CYRA-OT, as shown on the right.

The additions to the word and image mark indicate the association of the registered word and image mark with this certification scheme. Separate word marks are not used.

5.1.2 Use of the mark by the certification body

The certification body will use the mark in accordance with the CCV Regulation on Quality Marks. General requirements for the use of the mark are as follows:

- The certification body holds a valid licence issued by CCV.
- The mark is used in direct connection with the certification scheme and for illustrative purposes on stationery, in emails, on the website, in brochures and other publicity materials.

5.1.3 Use of the mark by the organisation

The organisation will use the mark in accordance with the CCV Regulation on Quality Marks. General requirements for the use of the mark are as follows:

- The organisation holds a valid certification contract with a certification body that has a valid CCV licence for the application of this certification scheme.
- The organisation is not suspended.
- The mark is used in direct connection with the location, processes, services and activities within the scope, and for illustrative purposes on stationery, in emails, on the website, in brochures and other publicity materials.

5.2 Certificate for the level of resilience

5.2.1 General

Following a positive decision on the assessment, the certification body will issue the organisation with a certificate for the level of resilience. The certificate will be designed in the house style of the certification body and will, as a minimum, comply with the requirements set out in section 5.2.2 or 5.2.4. A combined certificate is not permitted.

A certificate for the level of resilience against Digital Criminal Infiltration is not possible; in such cases, the statement regarding that level of resilience must be attached to the certificate for subdomains A and C as referred to in section 5.2.2.

Additional information may be included on the certificate, provided that it does not conflict with this certification scheme and/or with applicable legislation and regulations, and does not concern matters outside the scope of the assessment or the responsibility of the organisation.

NOTE
Contrary to ISO/IEC 17021-1, the certificate is valid for a period of two years

5.2.2 Certificate fort he level of digital resilience for subdomains A (CYRA-IT) and C (CYRA-Health Care)

The certificate for the level of digital resilience will contain at least the following information:

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

> **For example:** CYRA-Health Care Basic – Best Effort (2)

- Name, address and contact details of the certification body;
- Name, address and contact details of the organisation (correspondence address);
- The following text:

  <Certification body> declares that the level of digital resilience of <name of the organisation> for the location <location identifier> and the business activities <processes, services, activities within scope> complies with the requirements of the CCV Certification Scheme CYRA at the level of digital resilience <Entry – Basic – Intermediate – Advanced> (maturity level <Ad Hoc (1) / Best Effort (2) / Defined (3)>).

  <Certification body> grants <organisation> the licence to use the certification mark shown below in accordance with the CCV Regulation on Quality Marks.

- A unique certificate number;
- The date of issue/the date from which the certificate is valid;
- The expiry date of the certificate [issue date + 24 months];
- Signature, which may be digital (including name and position);
- The company logo of the certification body;
- The certification mark:

In the case of subdomain A – CYRA-IT

In the case of subdomain C– CYRA-Health Care

- The following text:
  - The status of this certificate can be verified with <certification body>.
  - This certificate remains the property of <certification body>.

5.2.3 Additional statement on resilience against digital criminal infiltration under subdomain B (CYRA-NDO)

If, in addition to the assessment under subdomain A or C, an assessment under subdomain B has also been conducted and successfully completed, the certificate referred to in section 5.2.2 will be supplemented with the following information:

- Header: CYRA-NDO – < Entry / Basic / Intermediate / Advanced> – <Ad Hoc (1) / Best Effort (2) / Defined (3)>
- The underlined part in the text of the statement issued by the certification body:

*<Certification body> declares that the level of digital resilience **and the level of resilience against Digital Criminal Infiltration** of <name of the organisation> for the location <location identifier> and the business activities <processes, services, activities within scope> comply with the requirements of the CCV Certification Scheme CYRA (maturity level <Ad Hoc (1) / Best Effort (2) / Defined (3))>.*

*<Certification body> grants <organisation> the licences for use of **the certification marks shown below** in accordance with the CCV Regulation on Quality Marks.*

- The certification mark:

Note for clarification: a combined certificate CYRA-IT & CYRA-NDO or CYRA-Health Care & CYRA-NDO contains two certification marks.

5.2.4 Certificate for the level of digital resilience of operational technology for subdomain D (CYRA–OT)

The certificate for the level of digital resilience of operational technology will contain at least the following information:

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

For example: CYRA-OT Intermediate – Defined (3)

- Name, address and contact details of the certification body;
- Name, address and contact details of the organisation (correspondence address);
- The following text:

<Certification body> declares that the digital resilience of operational technology of <name of the organisation> for the location <location identifier> and the business activities <processes, services, activities within scope> complies with the requirements of the CCV Certification Scheme CYRA at the level of digital resilience <Entry – Basic – Intermediate – Advanced> (maturity level <Ad Hoc (1) / Best Effort (2) / Defined (3))>.

<Certification body> grants <organisation> the licence to use the certification mark shown below in accordance with the CCV Regulation on Quality Marks.

- A unique certificate number;
- The date of issue;
- The expiry date of the certificate [issue date + 24 months];
- Signature, which may be digital (including name and position);
- The company logo of the certification body;

- The certification mark:

- The following text:
  - The status of this certificate can be verified with <certification body>
  - This certificate remains the property of <certification body>.

6 References

6.1 Legislation and regulations

This section is not applicable to this certification scheme.

6.2 Terms and abreviations

Nonconformity	A situation that does not comply with the requirements set out in the certification scheme.
Audit	Systematic, independent and documented process for obtaining audit evidence and objectively assessing it in order to determine the extent to which agreed audit criteria have been fulfilled
Assessment	The application of this certification scheme by the certification body at the organisation.
CCV	Centrum voor Criminaliteitspreventie en Veiligheid (Centre for Crime Prevention and Safety)
CYRA	Cyber Rating
Certificate	Document prepared by the service provider containing a statement regarding the incident response service provided.
Certification mark	Word or figurative mark used to indicate conformity to requirements
Certification scheme	System of rules, procedures and management aspects for performing certification assessments.
Committee of Interested Parties	The committee within the CCV that determines the support for the scheme and advises the CCV on (amendments to) the certification scheme. Interested and involved parties are represented in this committee.
EN	European Standard, issued by CEN or CENELEC (European Committee for (Electrotechnical) Standardisation).
IACS	A collective term for systems and technologies that automatically control, operate and monitor industrial processes, such as PLCs (Programmable Logic Controllers), SCADA systems (Supervisory Control and Data Acquisition), and DCSs (Distributed Control Systems). In this scheme, these are referred to as Operational Technology (OT).
IEC	International Electrotechnical Commission. An IEC standard is an international standard issued by the IEC.
ISMS	Information Security Management System.
ISO	International Organisation for Standardization. An ISO standard is an international standard issued by ISO.
IT	Information Technology
NDO	Normkader Digitale Ondermijning / Normative Framework for Digital Criminal Infiltration
NEN	Royal Netherlands Standardization Institute (NEN). The NEN is the Dutch organisation responsible for issuing national standards.
Standard	A document in which agreements between relevant parties are established with the intention that they will be adhered to.
Client	The legal entity for whom or on whose behalf the organisation carries out work.

Organisation	The entity that wishes to determine, has determined, or seeks to have independently assessed by a certification body its level of digital resilience, its resilience against Digital Criminal Infiltration, or the digital resilience of its operational technology.
OT	Operational Technology. A collective term for systems and technologies that automatically control, operate and monitor industrial processes, such as PLCs (Programmable Logic Controllers), SCADA systems (Supervisory Control and Data Acquisition), and DCSs (Distributed Control Systems). International term: IACS (see definition under IACS).

6.3 Standards and references

The standards and documents listed in the table below apply to this certification scheme, including interpretations published by the CCV. The version number is binding (static reference). These standards and documents are normative, unless indicated in this scheme that it concerns indicative reference. It is also possible to refer normatively or indicatively to parts of a standard or document, in which case the other parts of this standard or document have no significance for this scheme.

Other standards or documents referred to in these standards or documents apply as indicated therein.

A certification body must have access to all normative standards and documents.

STANDARD	SUBJECT	AVAILABLE AT
NEN-EN-IEC 62443-2-1	Security for industrial automation and control systems – Part 2-1: Requirements for establishing an IACS security program	NEN Delft
NEN-EN-IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: Requirements for system security and security levels	NEN, Delft
ISO/IEC 17021-1	Conformity assessment - Requirements for bodies performing audits and certification of management systems	NEN, Delft
ISO/IEC 27001	Requirements for information technology, security techniques, information security management systems	NEN, Delft
ISO/IEC 27002	Information security, cybersecurity and privacy protection – Code of practice for information security controls	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	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines	NEN, Delft
NEN 7510-1	Health informatics – Information security in health care – Part 1: Management system	NEN, Delft
NEN 7510-2	Health informatics – Information security in health care – Part 2: Information security controls	NEN, Delft
CCV Reglement Kwaliteitslogo	CCV Regulation on Quality Marks	CCV, Utrecht
	CCV Regulation on Assessing Transferring Certificate Holders	CCV, Utrecht

Annex A - Overview of CYRA assessment levels and maturity levels

A.1 CYRA assessment model for digital resilience (domain A)

The assessment model for digital resilience under Domain A is derived from the requirements of the ISO/IEC 27001 and ISO/IEC 27701 standards. It consists of twelve elements: the levels Entry, Basic, Intermediate, and Advanced, each subdivided into three maturity levels (1 to 3). The interrelationship between these levels and maturity levels is illustrated in Figure 2.

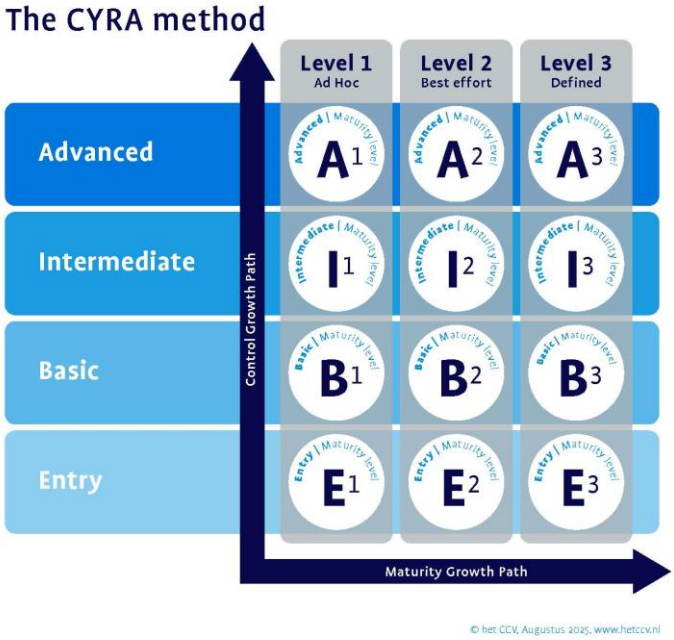

Figure 2: overview of levels and maturity levels in the CYRA Assessment Model.

An organisation must meet, as a minimum, the assessment criteria of Level Entry, Maturity Level 1 (Ad Hoc) to qualify for a CYRA-IT certificate.

The growth path in relation to the total set of control measures selected from ISO/IEC 27001 and ISO/IEC 27701 is as follows:

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

A.2 CYRA assessment model for resilience against Digital Criminal Infiltration (Domain B)

The Normative Framework for Digital Criminal Infiltration (NDO) for Domain B provides a specific interpretation of the requirements from ISO/IEC 27001, supplemented with additional requirements for business processes that are essential to strengthening resilience against digital criminal infiltration. It consists of nine assessment aspects, which are evaluated in full and in conjunction with the applicable assessment aspects from the CYRA assessment model for digital resilience under Domain A or C, at least at the Entry level (Maturity Level 1 – Ad Hoc). The interrelationship between these aspects is illustrated in Figure 3.

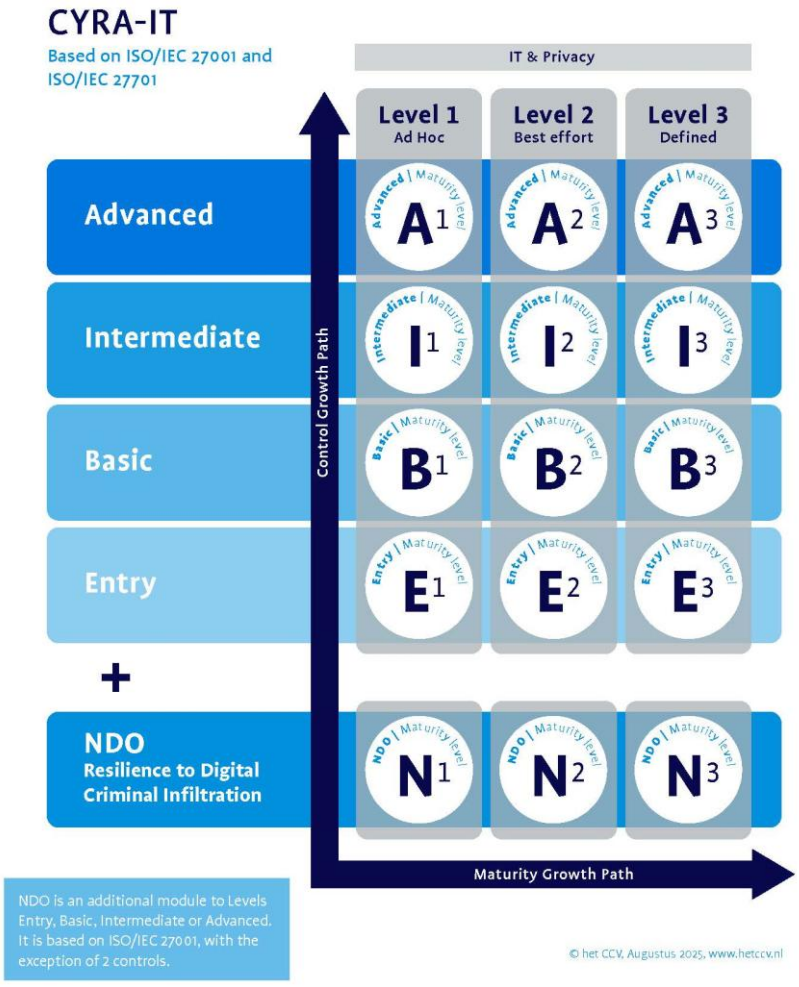

Figure 3: overview of interrelated assessment aspects and maturity levels in the CYRA Assessment Model for Resilience Against Digital Criminal Infiltration.

A.3 CYRA assessment model for digital resilience of organisations in Health Care (Domain C)

The CYRA assessment model for digital resilience of organisations in the health care sector under Domain C is derived from the requirements of the NEN 7510 standards series. It consists of twelve elements: the levels Entry, Basic, Intermediate, and Advanced, each subdivided into three maturity levels (1 to 3). The interrelationship between these levels and maturity levels is illustrated in Figure 4.

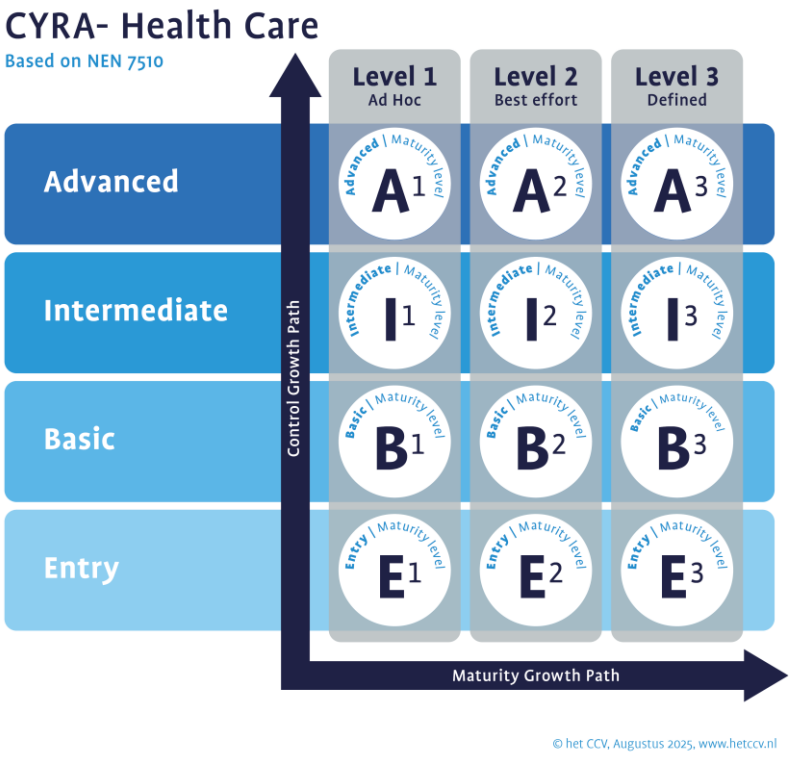

Figure 4: overview of levels and maturity levels in the CYRA Assessment Model for digital resilience of organisations in Health Care.

A health care organisation must meet, as a minimum, the assessment criteria of Level Entry, Maturity Level 1 (Ad Hoc) to qualify for a CYRA-Health Care certificate.

The growth path in relation to the total set of control measures selected from the NEN 7510 standards series is as follows:

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

A.4 CYRA assessment model for digital resilience of operational technology (Domain D)

The CYRA assessment model for digital resilience of operational technology under Domain D is derived from Parts 2-1 and 3-3 of the IEC 62443 standards series. It consists of twelve elements: the levels Entry, Basic, Intermediate, and Advanced, each subdivided into three maturity levels (1 to 3). The interrelationship between these levels and maturity levels is illustrated in Figure 5.

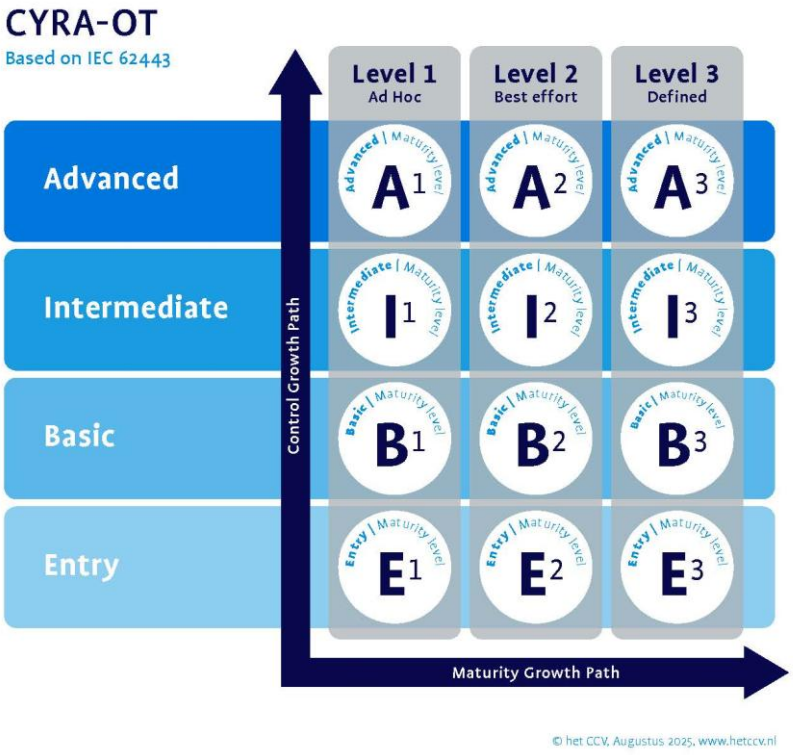

Figure 5: Overview of levels and maturity levels in the CYRA assessment model for digital resilience of operational technology..

The digital resilience of operational technology must meet, as a minimum, the assessment criteria of Level Entry, Maturity Level 1 (Ad Hoc) to qualify for a CYRA-OT certificate.

The growth path in relation to the total set of control measures selected from the IEC 62443 standards series is as follows:

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

Annex B – Table of contents of the CYRA assessment model

B.1 General

CCV has established the CYRA assessment model, which describes the control measures that organisations are expected to implement to strengthen their digital resilience, resilience against Digital Criminal Infiltration, and/or digital resilience of operational technology (OT). Using the questions for each control measure in the online assessment tool, the organisation determines whether the requirements for each control measure have been met and which maturity level has been achieved.

B.2 Table of contents of the CYRA-IT assessment model – Entry level

ENTRY	NORMATIVE ELEMENT FROM ISO 27001
B.2.1. Organisation	
■ Policy rules for information security and privacy	5.1
■ Access control	5.15
■ Registration and deregistration of users	5.16
■ Access rights	5.18
■ Roles and responsibilities for information security and privacy	5.2
■ Monitoring, assessment and management of changes in the service provision of suppliers	5.22
■ Information security in adverse situations	5.29
B.2.2. Personnel	
■ Screening	6.1
■ Awareness, education and training on information security	6.3
■ Remote working	6.7
■ Reporting of information security incidents	6.8
B.2.3. Physical	
■ Physical security perimeter	7.1
B.2.4. Technological	
■ Generating, storing and reviewing log files	8.15
■ Protecting information in networks and supporting systems	8.20
■ Ensuring security in the use of network services	8.21
■ Ensuring the correct and effective use of encryption to safeguard confidentiality, integrity and availability in line with applicable laws and regulations	8.24
■ Policy for secure development of software and systems	8.25
■ Information security requirements for the design and procurement of applications	8.26

ENTRY	NORMATIVE ELEMENT FROM ISO 27001
■ Change management	8.32
■ Secure login procedures	8.5
■ Technical and organisational protection against malware	8.7
■ Prevention of exploitation of technical vulnerabilities	8.8
	Clause from ISO 27701
B.2.5. Privacy	
■ Objectives of the organisation	B.8.2.2
■ Records related to the processing of personal data	B.8.2.6

B.3 Table of Contents CYRA-IT assessment model – Basic Level

BASIC **BASIC** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** LEVEL, SUPPLEMENTED WITH:	NORMATIVE ELEMENT FROM ISO 27001
B.3.1. Organisation	
■ Classification of information	5.12
■ Information security policy for supplier relationships	5.19
■ Inclusion of security aspects in supplier agreements	5.20
■ Supply chain for information and communication technology	5.21
■ Information security for the use of cloud services	5.23
■ Learning from information security incidents	5.27
■ Privacy and protection of personal data	5.34
■ Documented operating procedures	5.37
■ Information and threat analysis	5.7
■ Inventory of information and related business assets	5.9
B.3.2. Personnel	
■ Employment conditions	6.2
■ Confidentiality or non-disclosure agreement	6.6
B.3.3. Physical	
■ Cabling security	7.12
■ Secure disposal or reuse of equipment	7.14
■ Physical access control	7.2
■ Securing offices, rooms, and facilities	7.3
■ Monitoring of physical security	7.4
■ Protection against external and environmental threats	7.5
■ Working in secure areas	7.6
■ ‘Clear desk’ and ‘clear screen’ policy	7.7

BASIC **BASIC** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** LEVEL, SUPPLEMENTED WITH:	NORMATIVE ELEMENT FROM ISO 27001
■ Placement and protection of equipment	7.8
■ Security of equipment and assets off-premises	7.9
B.3.4. Technological	
■ Control of information stored or processed on workstations and/or mobile devices	8.1
■ Deletion of information	8.10
■ Prevention of data leaks	8.12
■ Backup of information	8.13
■ Protection of operational systems through procedures and measures for software installation	8.19
■ Management of privileged access rights	8.2
■ Restriction of access to information	8.3
	Clause from ISO 27701
B.3.5. Privacy	
■ Agreement with the client	B.8.2.1
■ Disclosure regarding subcontractors engaged in personal data processing	B.8.5.6
■ Client obligations	B.8.2.5

B.4 Table of contents CYRA-IT assessment model – Intermediate level

INTERMEDIATE **INTERMEDIATE** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** AND **BASIC** LEVELS, SUPPLEMENTED WITH:	NORMATIVE ELEMENT FROM ISO 27001
B.4.1. Organisation	
■ Acceptable use of information and other business assets	5.10
■ Return of business assets	5.11
■ Labelling of information	5.13
■ Authentication information	5.17
■ Responsibilities and procedures	5.24
■ Assessment and decision-making regarding information security incidents	5.25
■ Response to information security incidents	5.26
■ Separation of duties	5.3
■ Determination of applicable legislation and contractual requirements	5.31
■ Intellectual property rights	5.32
■ Protection of records	5.33
■ Compliance with security policies/standards	5.36
■ Management responsibilities	5.4
■ Information security in project management	5.8
B.4.2. Personnel	

INTERMEDIATE **INTERMEDIATE** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** AND **BASIC** LEVELS, SUPPLEMENTED WITH:	NORMATIVE ELEMENT FROM ISO 27001
■ Termination or change of employment responsibilities	6.5
B.4.3. Physical	
■ Storage media	7.10
■ Utilities	7.11
■ Maintenance of equipment	7.13
B.4.4. Technological	
■ Availability of information processing facilities	8.14
■ Monitoring of activities	8.16
■ Clock synchronisation	8.17
■ Network segregation	8.22
■ Security testing during development and acceptance	8.29
■ Outsourced software development	8.30
■ Capacity management	8.6
	Clause from ISO 27701
B.4.5. Privacy	
■ Assignment causing the breach	B.8.2.4
■ Return, transfer or deletion of personal data	B.8.4.2
■ Records of disclosures of personal data to third parties	B.8.5.3

B.5 Table of contents CYRA-IT assessment model – Advanced level

ADVANCED **ADVANCED** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY**, **BASIC** AND **INTERMEDIATE** LEVELS, SUPPLEMENTED WITH:	NORMATIVE ELEMENT FROM ISO 27001
B.5.1. Organisation	
■ Information transfer	5.14
■ Collection of evidence	5.28
■ ICT readiness for business continuity	5.30
■ Independent review of information security	5.35
■ Contact with government authorities	5.5
■ Contact with special interest groups	5.6
B.5.2. Personnel	
■ Disciplinary procedure	6.4
B.5.3. Technological	
■ Data masking	8.11
■ Use of special system utilities	8.18
■ Application of web filters	8.23

ADVANCED **ADVANCED** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY**, **BASIC** AND **INTERMEDIATE** LEVELS, SUPPLEMENTED WITH:	NORMATIVE ELEMENT FROM ISO 27001
■ Principles for the engineering of secure systems	8.27
■ Secure coding	8.28
■ Separation of development, test, and production environments	8.31
■ Protection of test data	8.33
■ Controls related to audits of information systems	8.34
■ Access control to program source code	8.4
■ Configuration management	8.9

B.6 Table of contents Normative Framework for Digital Criminal Infiltration (NDO)

NORMATIVE FRAMEWORK FOR DIGITAL CRIMINAL INFILTRATION (NDO) ASSESSMENT OF THE NORMATIVE FRAMEWORK FOR DIGITAL CRIMINAL INFILTRATION TAKES PLACE IN COMBINATION WITH THE ASSESSMENT OF THE CONTROL MEASURES FOR THE SELECTED LEVEL FROM THE CYRA-IT OR CYRA-HEALTH CARE ASSESSMENT MODEL.	NORMATIVE ELEMENT FROM ISO 27001
■ Policies for information security and privacy **Does the organisation have current policies regarding information security and privacy?**	5.1
■ Information and threat analysis **Are threats in the field of information security assessed?**	5.7
■ Inventory of information and related business assets **Are business assets related to information recorded?**	5.9
■ Classification of information **Does the organisation use an information classification mechanism?**	5.12
■ Screening **Are staff backgrounds verified?**	n/a, additional aspect NDO 1
■ Awareness, education, and training on information security **Is staff knowledge on information security developed and maintained?**	6.3
■ Digital Criminal Infiltration reporting point **Is a digital criminal infiltration reporting point used?**	n/a, additional aspect NDO 2
■ 'User endpoint devices' **Is user equipment (laptop, PC, tablet, smartphone) that functions as part of the workplace adequately protected?**	8.1
■ Generating, storing, and reviewing log files **Are log files used?**	8.15

B.7 Table of contents CYRA-Health Care assessment model – Entry level

ENTRY **ENTRY** LEVEL INCLUDES ALL CONTROL MEASURES FROM THE ENTRY LEVEL OF **CYRA-IT**, SUPPLEMENTED WITH	NORMATIVE ELEMENT FROM NEN 7510
Organisation	
■ HLT – Analysis and specification of information security requirements	5.38

B.8 Table of contents CYRA-Health Care assessment model – Basic level

BASIC **BASIC** LEVEL INCLUDES ALL CONTROL MEASURES FROM THE BASIC LEVEL OF **CYRA-IT**, SUPPLEMENTED WITH	NORMATIVE ELEMENT FROM NEN 7510
Organisation	
■ HLT – Publicly available health information	5.41

B.9 Table of contents CYRA-Health Care assessment model – Intermediate level

INTERMEDIATE **INTERMEDIATE** LEVEL INCLUDES ALL CONTROL MEASURES FROM THE INTERMEDIATE LEVEL OF **CYRA-IT**, SUPPLEMENTED WITH	NORMATIVE ELEMENT FROM NEN 7510
Organisation	
■ HLT – Uniquely identifying care recipients	5.39

B.10 Table of contents CYRA-Health Care assessment model – Advanced level

ADVANCED **ADVANCED** LEVEL INCLUDES ALL CONTROL MEASURES FROM THE ADVANCED LEVEL OF **CYRA-IT**, SUPPLEMENTED WITH	NORMATIVE ELEMENT FROM NEN 7510
Organisation	
■ HLT – Validation of displayed/printed data	5.40
■ HLT – Communication in emergency situations	5.42
■ HLT – External reporting of incidents	5.43

B.11 Table of contents CYRA-OT assessment model – Entry level

ENTRY			
NORMATIVE ELEMENT FROM IEC 62443-2-1		NORMATIVE ELEMENT FROM 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			
NORMATIVE ELEMENT FROM IEC 62443-2-1		NORMATIVE ELEMENT FROM 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 Table of contents CYRA-OT assessment model – Basic level

BASIC **BASIC** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** LEVEL, SUPPLEMENTED WITH:			
NORMATIVE ELEMENT FROM IEC 62443-2-1		NORMATIVE ELEMENT FROM 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 **BASIC** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** LEVEL, SUPPLEMENTED WITH:			
■ 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
■ Cryptongraphic 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 Table of contents CYRA-OT assessment model – Intermediate level

INTERMEDIATE **INTERMEDIATE** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** AND **BASIC** LEVLS, SUPPLEMENTED WITH:			
NORMATIVE ELEMENT FROM IEC 62443-2-1		NORMATIVE ELEMENT FROM 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 **INTERMEDIATE** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY** AND **BASIC** LEVLS, SUPPLEMENTED WITH:			
■ Resource availability management	AVAIL 1.2	■ Resource management	SR 7.2
■ Failure-state	AVAIL 1.3	■ Deterministic output	SR 3.6

B.14 Table of contents CYRA-OT assessment model – Advanced level

ADVANCED **ADVANCED** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY**, **BASIC** AND **INTERMEDIATE** LEVELS, SUPPLEMENTED WITH:			
NORMATIVE ELEMENT FROM IEC 62443-2-1		NORMATIVE ELEMENT FROM 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 **ADVANCED** LEVEL INCLUDES ALL CONTROL MEASURES FROM **ENTRY**, **BASIC** AND **INTERMEDIATE** LEVELS, SUPPLEMENTED WITH:			
■ 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)

Annex C – Maturity Levels

The certification scheme uses a classification of three maturity levels: 1 (Ad Hoc), 2 (Best Effort) and 3 (Defined). These levels are based on the Capability Maturity Model Integration (CMMI) and are translated into the following levels for CYRA:

LEVEL 1: AD HOC	LEVEL 2: BEST EFFORT	LEVEL 3: DEFINED
The control measure derived from ISO 27001/27701, the NEN 7510 series or the IEC 62443 series is applied in an ad hoc and unstructured manner. The organisation is reactive and often engaged in 'firefighting'. Success depends on individual efforts.	Compared to Level 1, the control measure is applied in a managed and planned way, covering at least the selected components from ISO 27001/27701, the NEN 7510 series or the IEC 62443 series.	The control measure is fully implemented, standardised and demonstrable. The organisation is proactive. Implementation meets the requirements of ISO 27001/27701, the NEN 7510 series or the IEC 62443 series.
"It is not documented."	"It is documented and we follow the procedures."	"We have policies and procedures, follow them, test them and improve them periodically."

The answers provided in the online assessment tool make clear at which level the organisation has implemented a control measure.

CCV centrum voor criminaliteitspreventie en veiligheid

The Centre for Crime Prevention and Safety (CCV) is an independent foundation that supports organisations and safety professionals in making the Netherlands a safer and more liveable place.

Centre for Crime Prevention and Safety
Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

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