CCV centrum voor criminaliteitspreventie en veiligheid

CCV certification scheme

Cyber Security Awareness Training

Version 1.0
Publication date: 1 February 2025
Effective date: 1 May 2025

Foreword

This certification scheme is aimed at quality management system certification of awareness training providers according to NEN-EN-ISO/IEC 17021-1.

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

The certification scheme is structured according to the model used by the CCV for quality management system certification schemes that are implemented under accreditation. All aspects necessary for execution under accreditation have been addressed. At a time to be determined in consultation with the Commission of Interested Parties, certification bodies may be required to implement the underlying certification scheme under accreditation.

Despite all the care taken to compile this publication, the Centre for Crime Prevention and Safety cannot accept any liability for any damage that may arise from any errors that may appear in it.

Table of contents

1 Introduction

1.1 General

1.1.1 Introduction

Protecting digital systems and keeping them secure is important for every business. It only takes one vulnerability in a system for the damage to be extensive. It is up to the organisation to protect itself against attacks, vulnerabilities, or other threats. This can be done by organising security consisting of digital, organisational and people-orientated measures. A company that wants to protect itself against cyber crime needs this to be done properly, with safe products and installed or carried out by a professional and via high quality services. Organisational and people-orientated measures can be improved by providing personnel with high quality awareness training. Both information technology (IT) and operational technology (OT) may require additional protection. All of this is often difficult for the entrepreneur to assess properly on his or her own. Certification schemes for cyber security awareness trainings offer a good solution for this purpose. This certification scheme focuses on awareness training.

1.1.2 Purpose

The cyber security dictionary[1] gives the following definition of security awareness: “The extent to which people recognise risks and are aware that they can jeopardise the security of information.”

To limit the risks of cyber incidents, employees should be aware of cyber security risks. Security awareness is the extent to which people are aware of these risks. Training leads to knowledge and awareness. The aim of security awareness training is that people become aware of their role and responsibility and recognise threats. This awareness and these skills form a basis to prevent or avert security incidents.

Awareness training needs to be carried out professionally. Government and private parties have a need for guaranteed quality of such training. This assurance is possible with certification of awareness training providers.

The aim of the certification of awareness training is:

- To stimulate the quality of awareness training offered, and by doing so to reduce the costs of failure and risks for clients that may occur when the supposed quality of the training is not delivered.
- To provide clients with a legitimate confidence that the awareness training provider will provide awareness trainings that meet the requirements set in advance.

The aim of this document, the certification scheme, is to lay down the requirements for awareness training providers, and to describe the implementation of certification. This should lead to harmonised implementation. An additional goal is informing the market how certification of awareness training is organised and carried out.

1.1.3 Responsibilities

Any organisation responsible for its systems or data is also responsible for the security of digital systems and for taking the corresponding measures, including those on an organisational level. This involves making the organisation, including its staff, resilient against cyber crime and other cyber security threats. That may include the periodic training of personnel on the issue of cyber security awareness. In this certification scheme, these parties are referred to as the client.

[1] Reference: Cybersecurity woordenboek 2021, Cyberveilig Nederland i.s.m. Cybersecurity Alliantie

The awareness training provider is responsible for ensuring that the quality management system complies with the requirements set out in the certification scheme. This forms the basis for his responsibilities towards clients in executing the awareness training, knowledge testing, and reporting to the client.

1.1.4 Reading guide

The certification scheme contains:

- conditions for the quality management system (chapter 2);
- conditions for obtaining and maintaining the certificate (chapter 3);
- harmonised working methods to be used by the certification body when processing a certification application and maintaining the certificate (chapter 4);
- description of the certificate issued by the certification body and the certification mark to be applied (chapter 5).

1.2 Scope

The scope of this certification scheme is the quality management system of cyber security awareness training providers. Processes, procedures and qualifications that meet the criteria set out in this certification scheme should lead to awareness training courses that fulfil the client's expectations and demands and are in line with contract specifications agreed with the client.

This certification scheme has two sub scopes:

Certification level 1: The quality management system is certified for providing separately delivered (one time) awareness training sessions

Certification level 2: The quality management system is certified for providing integrated awareness training courses (integrated course level)

Notes for clarification

a If not specified, requirements in this certification scheme apply to both level 1 and 2.

b Level 2 holds additional requirements compared to level 1. Thus, if a service provider is certified under level 2, this implies it also meets all the requirements under level 1.

c Some forms of awareness training or awareness tools can be *additional* parts of an integrated training course (level 2), but cannot be delivered independently under certification under level 1. See annex A for examples.

d Forms of awareness training not mentioned in annex A are at the discretion of the certification body. If needed, the certification body will bring the issue at hand to the attention of the CCV, for a unified implementation of the certification scheme.

1.3 Relation to laws and regulations

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

However, this certification scheme leads to awareness training under certification, which can be highly useful for organisations to demonstrate their compliance to laws and regulations.

This applies to organisations that need to directly adhere to NIS2 (in the Netherlands leading to the Cyberbeveiligingswet), as one of the elements in the NIS2 directive is raising cyber security awareness and the use of awareness training. It can also apply to partners/providers in a supply chain to NIS2 parties.

1.4 Relationship chart

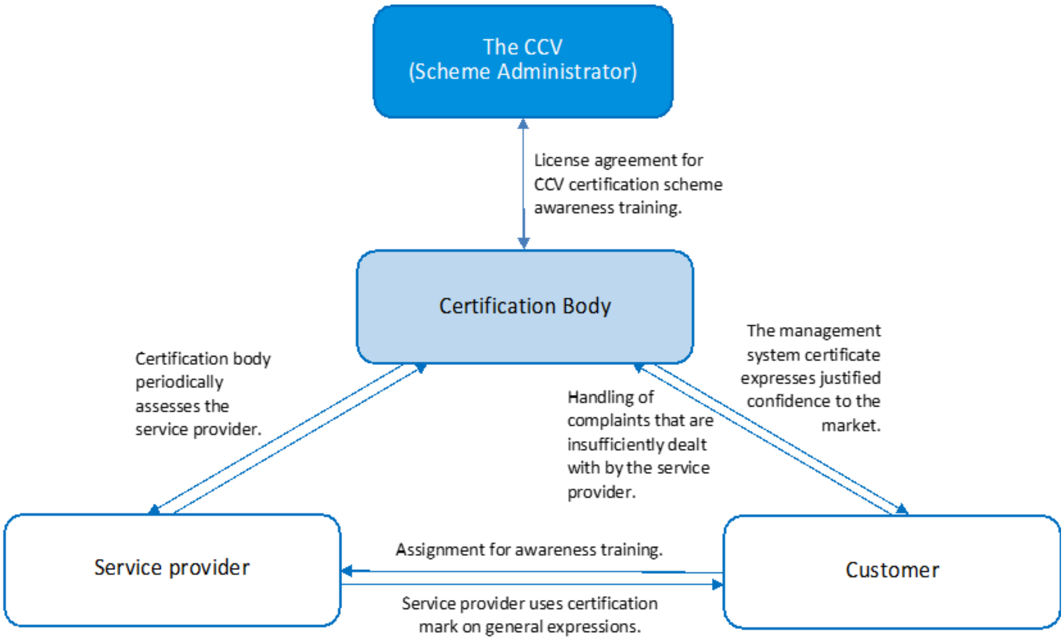

The CCV
(Scheme Administrator)
License agreement for CCV certification scheme awareness training.
Certification Body
Certification body periodically assesses the service provider.
Handling of complaints that are insufficiently dealt with by the service provider.
The management system certificate expresses justified confidence to the market.
Service provider
Assignment for awareness training.
Service provider uses certification mark on general expressions.
Customer

Figure 1 - Overview of parties involved in certification

1.5 Transitional provisions

The certification scheme is a new scheme and has no predecessor. Therefore, no transitional provisions are necessary.

2 Awareness training process requirements

2.1 General

The quality management system is aimed at fulfilling the client's expectations and demands, and contract specifications agreed with the client.
The quality management system requirements are the requirements according to NEN-EN-ISO 9001 and parts of NEN-ISO/IEC 27001. Specific additions relate to process requirements, technical equipment requirements and personnel requirements. The additions are specified in this chapter. The quality management system will be audited according to the ISO 9001 requirements.
This chapter describes aspects of the process that is required for adequate awareness training. Some of these process steps also lead to documents provided to the client.

2.2 Quote and intake process

The awareness training provider runs a quote and intake process for each client, in which the client's expectations and demands are clarified. This leads to a training plan (2.3).

2.3 Training plan

The quote and intake process leads to a training plan, agreed between the awareness training provider and the client, which meets the requirements in table 2.3.1.

TABLE 2.3.1 – TRAINING PLAN

NR	ASSESSMENT ASPECT	REQUIREMENT
2.3.1.1	Language of training is clear for the client	The quote or training plan clarifies whether the training will be given in Dutch or English or provides the client a choice between those languages.
2.3.1.2	Scope; clarification and limitation of training topics	Quote and/or training plan describes: ■ scope in terms of topics/risks to be addressed in the training; ■ training goals; ■ if applicable, client-specific issues or concerns, linked to training goals. ■ (While setting up a training plan, the service provider checks and documents whether specific issues or concerns are applicable.) *In addition, for* ***Integrated courses (Level 2)*** ■ how the different elements of the integrated course relate to the client-specific training goals; ■ how the proposed training goals relate not only to wishes as expressed by the client, but also to outcomes of a questionnaire (or other method) by which the awareness training provider has measured cyber security awareness levels in the organisation.

TABLE 2.3.1 – TRAINING PLAN

NR	ASSESSMENT ASPECT	REQUIREMENT
2.3.1.3	Description of participants	The plan mentions: ■ the number of participants; ■ whether all personnel will be trained or specific subgroups; ■ whether the training offered differentiates in subgroups, and whether this leads to differentiating in testing; ■ If such differentiation is made, a description of backgrounds (department names and or function types)[2]; ■ If a choice is made *not* to differentiate in the training towards subgroups, this is made explicit.
2.3.1.4	Stimulating participation[3]	The plan: ■ mentions a percentage of personnel to follow and complete the training; this goal is agreed between awareness training provider and client; ■ clearly describes the responsibilities and required actions of both the awareness training provider and the client; ■ clearly describes how participants of interactive training sessions (on location or online) are stimulated to actively participate and contribute. **For integrated courses (level 2),** in addition**:** The client's organisation may receive new personnel members during the period in which the integrated awareness course is executed. The training plan describes how such possible new members of personnel will be included in the training course.
2.3.1.5	Testing	**For separately delivered courses** (by providers certified under level 1 or 2), testing as described below is always offered as an option in the quote/intake/planning process. As part of his QMS, the service provider has a method for testing participants in place to apply to any form of awareness training he offers, and he applies this at a sample of the training he delivers yearly. (Sample size can be context-dependent and is at the discretion of the auditor.) **For integrated courses** (under certification Level 2), these tests are applied for each client. ■ The plan describes the method for testing personnel's knowledge concerning cyber security awareness. ■ This method fits both the specific training goals and the type of organisation. ■ The awareness training provider may offer the client a choice in how test results will be reported back to the client:

[2] The extent to which differentiating in subgroups is required depends on the client and his wishes. This also has consequences for the level of differentiating in reporting on results of the training.

[3] These criteria demand setting an explicit goal for participation and providing the client with information to do his part for reaching it. The report on the training as given (2.5) provides numbers on realised participation, to reflect on that goal. However, actually reaching the participation goal is partly outside of the awareness training provider's responsibility, Therefore that aspect is not a requirement in this scheme.

TABLE 2.3.1 – TRAINING PLAN

NR	ASSESSMENT ASPECT	REQUIREMENT
		a At the level of the whole organisation or the whole of the trained group, and/or b Differentiated at team or department level. If the awareness training provider offers option b, the agreed plan is explicit about the client's choice. ■ The plan stipulates in what form the correct answers to the test, in reference to given answers, will be shared with participants. ■ For separately delivered training sessions (under level 1 or 2): The training plan refers to both the knowledge tests to be executed prior to the training and after the training. For this level, for separately delivered training sessions, the knowledge test "prior to" can be done at the start of the training. **For integrated courses (level 2):** ■ The final version of the training plan includes the *outcome* of the test executed prior to the training and refers to a test after the training. If training is given to the client's personnel repetitive or cyclical, and testing "prior to and after the training" is harder to define, knowledge testing is executed periodically, the frequency in line with the goals of the training plan and with the training aspects and modules provided, but with a minimum of once a year.
2.3.1.6	Evaluating	The plan describes how the result of the training in the client's organisation will be evaluated (using testing of participants, see above, as part of the input). Evaluation also includes the number of participants, as related to the set goals. The plan describes who is responsible for registration of participation: the client of the awareness training provider. When a training format requires a group evaluation (for instance gamification), the plan describes how this evaluation will be designed and how all participants will be actively involved.
2.3.1.7	Design	■ The training plan: – Describes which training method(s) is/are used; – Explains in short how examples of cyber security incidents used in the training relate to learning goals; – How all topics mentioned in the plan are properly addressed (possible in different training formats); ■ The training plan describes how at least part of the training is tailor made or the result of specific selections of available training material; the training focusses on specific (cultural) conditions in the client's organisation. **For level 2,** in addition the following applies: ■ The plan explains how the different forms or modules of the integrated course relate to each other and how this contributes to reaching the goals of the course. ■ When the training plan includes 'phishing test', it confirms that targets are selected and e-mails are designed via a standardized method within the awareness training provider and by considering specific

TABLE 2.3.1 – TRAINING PLAN		
NR	ASSESSMENT ASPECT	REQUIREMENT
		circumstances or concerns regarding the organisation of the client. Note: phishing test is not a format that can be delivered separately under certification, but an additional tool, that can be used as part of awareness training.
2.3.1.8	Spreading lessons and insights	Lessons are presented clearly and explicitly. The plan describes how these lessons and insights will be effectively shared with the client and all of the personnel members that are in scope in the training assignment. This includes members of personnel who were in scope in the assignment but did not participate. (Especially relevant for forms of training in which this is not obvious, such as escape rooms, tabletop sessions, crisis exercises.) The plan describes that the awareness training provider, in cooperation with the client, will inform the client's personnel after the awareness activity about the activity and the potential risks that could have been recognised. The maximum time period between the training and this information to personnel is made explicit in the plan. If the training provider does not offer additionally spreading of messages and insights, this choice is made explicit and is motivated in the plan.
2.3.1.9	Ethics	The plan explains the ethics concerned in awareness training and testing; how the awareness training provider strives for optimal impact by making the training acceptable to both the client and his personnel. This includes a reflection on techniques used and on privacy. (This can be either a generic text from the awareness training provider or client specific text, depending on the techniques used and possible client-specific concerns.)
2.3.1.10	Mitigating alerts	Some of the formats of awareness training can inadvertently trigger real cyber security (monitoring) alerts. The plan describes how the awareness training provider and client will try to avoid and if necessary, deal with such alerts, internally or as received by third parties, to avoid unintended damage or costs.
2.3.1.11	Temporarily disabling of security measures	If the client needs to temporarily disable security measures, the plan makes the client aware of this. If relevant, the client's business continuity plan will be taken into account.
2.3.1.12	Time frame	The plan includes a clear and realistic time frame, including a date for start and - if known - end.

2.4 Additional process requirements

The quality management system relates to performance of awareness training on cyber security in one or more formats. Examples of such formats are provided in Annex A.

If part of the training process is executed web based /digitally, a user-friendly interface is implemented. The service provider is aware of Web Content Accessibility Guidelines and has a documented self assessment (or external assessment) stating that the relevant parts of his training are WCAG compliant. A possible form of a documented self assessment is a completed and up to date checklist. This criterium can be relevant both for (parts of) training sessions themselves and/or for knowledge tests (see below).

The awareness training, that can be performed in one or more of the formats as described in Annex A, can be preceded and followed by a knowledge test. As mentioned in 2.3.1.5 such testing of participants will be executed with at least part of the separately provided training sessions or formats (provided under certification level 1 or 2). As part of his QMS, the service provider has a method in place for testing participants to apply to all forms of awareness training he offers. He applies this at a sample of the training he delivers yearly, as an instrument of quality control and to demonstrate impact. (Sample size can be context-dependent, and is at the discretion of the auditor.)

For integrated course (under Level 2) testing is executed at each client's organisation.

The test prior to the training is intended to establish a baseline. For level 2, it is also intended to identify specific points requiring attention in the training itself. The test after the training is intended to establish to what extent the participants have strengthened their knowledge and awareness concerning their own role in cyber security.

Further criteria for these knowledge tests are described in table 2.4.1

TABLE 2.4.1 - KNOWLEDGE TEST

NR	ASSESSMENT ASPECT	REQUIREMENT
2.4.1.1	Scope and focus	■ For knowledge test prior to training: The knowledge test is scoped to establish a baseline. Additionally, for **Level 2:** preliminary training goals are partly based on assumptions, by client and/or awareness training provider, concerning the level of awareness/pre-existing knowledge among the client's personnel. The knowledge test is scoped to validate or correct these assumptions. ■ For knowledge test after training **(level 1 and 2):** matches plan, including the client's specific needs.
2.4.1.2	Validity of questions	After training: Relation between knowledge test and training goals: the scope of questioning or assignment is such that it can be useful, for both the service provider and the client, to get insight in to what extend the training goals as set in the training plan are reached.
2.4.1.3	Validity of answering options	Questions and possible answers make it possible to weigh whether the participant has understood enough of specific topics, in relation to the training goals in the training plan.
2.4.1.4	Readability	Questions are formulated in such a manner that it is reasonable to assume that they can be understood by all users concerned; they test the learning goals, not higher language proficiency levels.
2.4.1.5	Flexibility of content – client specific and over time	The format of the test makes it possible to make changes in content of the test, both to adapt to specific needs of specific clients, and to update the tests if developments in cyber security and threats make this necessary.

TABLE 2.4.1 - KNOWLEDGE TEST

NR	ASSESSMENT ASPECT	REQUIREMENT
2.4.1.6	Direct and constructive feedback	■ The test provides feedback to the participant during or directly after the test; which questions were correct, and which were not; which topics require extra attention? (For the subset of questions on which such feedback is possible.) ■ This data is also reported to the client (in many cases the user's employer). This is done at the level of the whole of the client's organisation and/or at team or department level;; depending on what was agreed in the training plan.
2.4.1.7	Reporting to users	Delivered in line with the agreed upon training plan.
2.4.1.8	Output of organisational level / for clients	■ For test prior to training: results are ordered and analyses in such manner that the training plan can refer to them. ■ For test after training: the output provides results for the final report to the client, at least providing insight into: a to what extent the user's knowledge has grown during the training (comparison to test prior to or at the start of the training); b what elements require the client's further attention. Note: if the service provider has executed the knowledge testing fully anonymously, in the sense that the service provider itself also cannot link participant X, Y or Z's answers to the "prior to" knowledge test with the "after" knowledge test by the same participant, this analysis will be done only at group or client's organisation level.
2.4.1.9	Openness on use of data	Prior to doing the test, the user's information about how the data from the test is reported to the employer; aggravated on (1) organizational level and/or (2) at team or department level.
2.4.1.10	Security	Security of user data is up to standard; by a combination of technical and organizational measures, the chance of unauthorized access is limited. The awareness training provider can demonstrate that these aspects are thoroughly integrated into its quality management system. Prior certificates with relevant scope can be used as part of this evidence.

Note

Alternative forms of testing can be conducted. In such cases, the chosen method(s) is explained and motivated in the training plan. Measuring effect on behaviour, instead of on knowledge, is one of those alternatives, of the method and validation of correlation between measurements and the awareness training are convincing. This is at the discretion of the auditor.

2.5 Training report

Upon completion of the training activities, the awareness training provider provides a written training report.

Minimum requirements for the training report are included in table 2.5.1

TABLE 2.5.1 - CONTENT OF TRAINING REPORT

NR	ASSESSMENT ASPECT	REQUIREMENT
2.5.1.1	Content	The training report contains at least the following items: - Management summary. - Representation of the client (who) and the client's demand. - Scope and activities carried out. The report describes the implementation of the training. In particular, any aspects implemented differently to the description in the quote or plan is mentioned. - The report contains text that explicitly clarifies the following two points: – The training provided is intended to strengthen knowledge and awareness within the client's organisation. – However, such training does not provide guarantees that personnel will show behaviour in line with cyber security awareness in day-to-day operations. - Test results on knowledge of personnel; prior and after the training provided. - (If applicable; see 2.3 and 2.4) - In case of phishing tests, as a sub element of delivered awareness training, the report describes at least the number of personnel that received the e-mail, the number of people that clicked on links/buttons, and/or sent or filled in data. - The number of people participating, and the number of people finishing the training, in relation to the participation goal as set in the training plan. - Conclusions and recommendations. - Recommendations at least relate to employees who did not participate or with low results on the test and if relevant, mention topics not or not fully addressed in this training course.[4] - If the testing plan contains differentiation in subgroups of personnel, in training and/or tests, this is reflected in the report.
2.5.1.2	Language	The report is drawn up in the language as agreed upon in the quote or training plan.

[4] The recommendations can include other topics, including encountered circumstances in the client's organisation that can have negative impact on behaviour of personnel relating to cyber security.

3 Conditions for the awareness training provider

3.1 General

The conditions to be met by the awareness training provider are specified in this chapter.

The awareness training provider's quality management system is aimed at continuous securing of the quality of cyber security awareness training as specified in chapter 2. In the following sections and sub sections the requirements of the quality system are further elaborated.

The awareness training provider must be able to continuously demonstrate to the certification body (regardless of other certifications already obtained such as ISO), that the quality management system requirements (section 3.2) and the conditions for application and maintenance of the certificate (section 3.3) are fully met.

The awareness training provider provides the certification body with all requested information and data. Failure to do so may result in the sanctions described in sections 4.6 (suspension) and 4.7 (withdrawal).

3.2 Quality management system requirements

3.2.1 Organisation and responsibilities

The awareness training provider has an overview of the employees whose work influences the quality of the awareness training to be delivered. Tasks, responsibilities and authorities of these employees and their hierarchical relationships are recorded.

The employees are aware of the quality system, work according to it and is informed about changes.

3.2.1.1 Working under supervision

Employees who are not (yet) demonstrably qualified may only work under the supervision of qualified employees. When providing the awareness training, the qualified employee can be responsible for a maximum of two non-qualified employees. The qualified employee is ultimately responsible for the execution of the awareness training and the reports delivered.

3.2.1.2 Continuity

For the sake of continuity of operations, the awareness training provider organises replacement of experts. Hired personnel may be used (see section 3.2.5).

3.2.2 Qualifications

The quality of the work delivered strongly depends on the competence of the personnel: the right people must do the right work. Only qualified personnel is deployed for the tasks mentioned. The awareness training provider establishes that all employees involved in tasks indicated in the certification scheme meet the qualification requirements. For this purpose, the awareness training provider must:

- determine the necessary competence of the personnel who perform work under its authority that affects the organisation's performance in the field of awareness training;
- ensure that this personnel is competent based on appropriate education, training or experience;

- where appropriate, take measures to acquire the necessary competence and evaluate the effectiveness of the measures taken. The awareness training provider establishes a programme for each qualified employee for monitoring and evaluating the competences set. This programme is kept up to date.
- retain appropriate documented information as evidence of competence. There is an annual evaluation whether the qualification requirements are still met.

Note

Suitable measures may include, for example: providing training, mentoring, or appointing to another position those already employed; or hiring or contracting competent persons.

The Executive Board of the awareness training provider appoints an employee who is responsible for employee qualification for awareness training. The appointee has in-depth knowledge of this certification scheme and disposes of HBO working and thinking level.

To keep the knowledge level within the organisation up to standard, the awareness training provider has a written policy and procedures on training, development and knowledge sharing.

All employees involved in the awareness training (from start to finish) and/or those who have access to the information (permanent staff or externally hired) are in possession of a relevant 'certificate of conduct' (COC) - in Dutch: Verklaring omtrent het gedrag (VOG) - as referred to in the Judicial and Criminal Records Act, Article 28. The VOG/COC is not be older than three years.

The awareness training provider makes use of qualified content developers and trainers only.

Minimum requirements for content developer and trainer are included in table 3.2.2.

TABLE 3.2.2 - CRITERIA FOR TRAINER / CONTENT DEVELOPER

NR	ASSESSMENT ASPECT	REQUIREMENT
3.2.2.1	Qualification	Criteria to be formulated by the person in the organisation who is responsible for employee qualifications (see above). The awareness training provider sets internal qualification criteria and internal qualification training or development plans for employees to reach and maintain those qualifications. These plans are followed up via a PDCA-cycle. In addition, an awareness training given to clients is attended at least 3 times and is given under supervision of a qualified trainer at least once, before the qualification of a trainer can be reached. (Note: in case of small awareness training providers, this criterium can be met either in cooperation with other training providers, or by providing documentation on 5 earlier awareness training , as executed for clients.)
3.2.2.2	Experience (applies to trainer, not to content developer)	At least 1 year of experience in the relevant form of training. Experience as an intern does not qualify.
3.2.2.3	Knowledge of and ability to work with	This certification scheme; broad outlines of the whole scheme, and in depth concerning the parts directly relevant to one’s own role.

TABLE 3.2.2 - CRITERIA FOR TRAINER / CONTENT DEVELOPER

NR	ASSESSMENT ASPECT	REQUIREMENT
	this certification schema	
3.2.2.4	Language proficiency	Dutch language on level C1 and/or English language on level C1
3.2.2.5	Maintaining qualification	According to the awareness training provider's training and evaluation plan. In addition, a trainer gives the relevant kind of training at least once a year to maintain the qualification.

3.2.3 Measuring means and equipment

The awareness training provider has an overview of software or tooling that is deployed in the context of providing awareness training, including software or tooling used for knowledge tests. The awareness training provider declares that all software and tooling used is acquired and used in a legal manner and that he has licenses for all commercial software used. In case of doubt the awareness training provider must be able to provide the certification body with proof.

The awareness training provider demonstrates that all aspects of the awareness training, including tests, meet the criteria of the Web Content Accessibility Guidelines.

3.2.4 Outsourcing

The awareness training provider may subcontract work to another awareness training provider who provides awareness training.

The following applies:

- The awareness training provider assesses in advance, based on the requirements in section 3.2 and the requirements in chapter 2, whether the other awareness training provider is suitable for performing the specific work to be outsourced. If the assessment cannot be carried out, or cannot be carried out on time, or cannot be carried out with a positive conclusion, the awareness training provider cannot subcontract the task.
- In the event of a positive conclusion to the assessment, the awareness training provider remains responsible for the quality of the outsourced work and for the awareness training provided.
- If the awareness training provider to whom part of the awareness training is outsourced carries out the work under valid quality management system certification in accordance with the CCV Certification Scheme Cyber Security Awareness Training, the awareness training provider may assume that the contractor is suitable for carrying out the outsourced work. The scope and depth of the investigation of the contractor's suitability by the awareness training provider are in that case limited to verification of the contractor's management system certificate.
- The awareness training provider is responsible for the whole of the report to the client and the analyses it contains.

Note

if pre-existing content from a third party, for instance e-learnings, are integrated in the awareness training, this paragraph also applies.

3.2.5 Hiring

The awareness training provider may hire personnel to carry out the work. All requirements for the personnel employed by the awareness training provider as stated in chapter 3, also apply to hired personnel.

3.2.6 Primary processes

The awareness training provider demonstrates that the primary business processes are sufficiently secured and implemented (e.g., in the form of procedures and work instructions), so that the quality of awareness trainings delivered is secured.
As part of this is, the training provider has a system for knowledge tests in place, adhering to criteria in 2.3.1.5 and 2.4.1.

3.2.6.1 Security policy

The awareness training provider has a security policy that covers, as a minimum, the systems used for the awareness training, as well as the data obtained from clients in the context of the awareness training. This policy includes, as a minimum:

- concrete technical security measures to protect client information;
- concrete time limits for the storage and cleansing of data regarding the awareness training;
- description of the means the awareness training provider offers to exchange data - such as the awareness training report in a secure manner - with the client, so that confidential data is never stored unencrypted or sent via public networks;
- measures for the safe deletion of data;
- agreements on a confidentiality agreement to be concluded with employees who have access to data and information of the client.

3.2.6.2 Procedures

The awareness training provider has procedures for running a quote and intake process with the client, specifying a training plan, accepting an order to provide awareness training, carrying out awareness trainings and knowledge tests and providing the client with a training report.

3.2.7 Document management, registrations and archiving

The awareness training provider takes care of a well-organised archiving of all data and documents related to the requirements as stated in the certification scheme.

The awareness training provider has knowledge of the following documents:

- the documents mentioned in section 6.2, including the documents referred to therein;
- the written procedures and work instructions resulting from the certification scheme.

The awareness training provider keeps these documents up to date and inform its employees accordingly.

The awareness training provider has the following registrations:

- overview of employees[5] , duties, powers and responsibilities, hierarchical relationships (section 3.2.1);
- qualifications of personnel (section 3.2.2 and 3.2.5); subcontracted work (section 3.2.4);
- complaints (section 3.2.8);
- recovery and corrective actions (section 3.2.9);
- results of evaluations (section 3.2.10);
- documents in which the order to the awareness training provider is laid down (e.g., consent of the client on execution of the definitive training plan, contract, order confirmation, own registration of a verbal order, e-mail).

The data of the awareness training provider is kept for a period of at least one year[6].

3.2.8 Complaints

The awareness training provider has a written procedure for complaints, complaint analysis, resolution and corrective action to prevent recurrence.

The awareness training provider confirms the receipt of a complaint in writing to the complaining party within a maximum of two weeks. The awareness training provider settles the complaint within at most two months and send a written message to the complaining party. In the written message the awareness training provider states whether the complaint is justified, if not, why not and if so, what measures the awareness training provider has taken or will take.

3.2.9 Correction and corrective measures

The awareness training provider has a written procedure for correction and corrective action. In case of errors and deviations found, the awareness training provider takes corrective action in addition to the correction. Corrective measures are aimed at preventing the error from occurring again. In the event of deviations established by the certification body, specific conditions apply, see section 4.5.3 and section 4.5.6.

3.2.10 Evaluation

The awareness training provider is able to demonstrate that all the conditions referred to in this chapter (conditions for certification) and chapter 2 (requirements for awareness training) are permanently met. To this end, the awareness training provider makes an annual analysis:

- the complaints received and the way in which they are dealt with;
- periodically evaluation of the activities of operational staff against the prescribed working methods;
- periodically testing the quality system for effective implementation;
- in the case of an awareness training provider with only one staff member and no hired personnel, by exception the audit of the certification body may be used for this purpose.

3.3 Requirements for application and maintenance

3.3.1 Application data

Upon application, the awareness training provider provides the certification body with the following data:

- proof of legal registration[7];

[5] This also includes hired personnel (see section 3.2.5) and personnel carrying out evaluation (section 3.2.10)

[6] Due to legislation, longer retention periods may apply to certain documents.

[7] In the Netherlands, this is registration in the Trade Register of the Chamber of Commerce. Online consultation of the Trade Register is permitted.

- a declaration by an authorised person[8] that the awareness training provider will comply with the requirements, conditions and obligations stated in the certification scheme;
- if applicable: the presence of several branches that provide awareness training.
- the quality manual / documented quality management system[9];
- the reports of the most recent internal audit and management review.

In addition, the awareness training provider provides the certification body with all necessary information and data upon request.

3.3.2 Status during application

Until the initial assessment has been concluded with a positive decision, it is not permitted to publish any reference to the application for certification. In individual contacts and contracts reference may be made to this.

3.3.3 Access to information

The awareness training provider ensures that personnel of or on behalf of the certification body that needs to observe the activities of the certification body, have access to all relevant information and that they can attend awareness training.

3.3.4 Planning

The awareness training provider provides the certification body with all information about all awareness training (for instance when, which client, what kind of training, which trainer) to be delivered and/or delivered, so that the certification body can plan its own activities. The degree of detail shall be determined in mutual consultation.

3.3.5 Amendments

The awareness training provider reports relevant changes in the organisation to the certification body in a timely manner. These are changes such as (not limited):

- mergers and acquisitions;
- changes in the organisational structure;
- changes in the quality system, which affect the:
  - quality of the awareness training;
  - quality assurance of the awareness training;
  - implementation of the certification scheme;
- changes in the contents and status of other certificates (as far as these affect the implementation of the certification scheme).

3.3.6 Limitation of scope

Not applicable

[8] In most cases, this will be the chief executive officer, a management team member or the quality manager.

[9] “Manual” and “documented” shall not be read as synonyms for red tape. The quality management system should be as light as possible and as elaborate as necessary to meet the requirements of the certification scheme.

4 Conditions for the certification body

4.1 General

This chapter specifies harmonised procedures for the implementation of the certification scheme by certification bodies. These are binding for the certification bodies concerned.

4.2 Requirements for the certification body

4.2.1 General

Certification bodies can conclude certification contracts with awareness training providers if they have a licence agreement for the certification scheme[10] with the CCV.

This certification scheme is not yet implemented under accreditation.

4.2.2 Use of ISO 17021-1

This certification scheme is based on harmonised implementation under NEN-EN-ISO/IEC 17021-1.

When implementing this certification scheme, the certification body uses NEN-EN-ISO/IEC 17021-1 and implements it completely, supplemented by the provisions from this certification scheme. Where this scheme does not provide any details, the certification body itself must implement the necessary details. The certification body informs the scheme manager by submitting the subject for harmonisation.

Certification bodies may, as far as not conflicting with this certification scheme, apply their own certification regulations and procedures. In case of conflict with provisions of this certification scheme, this certification scheme is binding. In the situation where there is a conflict regarding implementation, but the same objective is pursued, the certification scheme is not binding. This is subject to a written agreement between CCV and the certification body.

Documents and interpretations on a national and international level are applicable when designated by the national accreditation body.

Explanatory remark

NEN-EN-ISO/IEC 17021-1 and related document such as IAF-MD, are highly determinative for the quality level and harmonisation of the performing of certification under NEN-EN-ISO/IEC 17021-1. This certification scheme is limited to the subjects that are not harmonised by NEN-EN-ISO/IEC 17021-1 and related documents, and for which harmonisation is desirable.

Awareness training providers are not able to derive the procedural aspects from the certification scheme. Section 4.2.3 offers guidance for that topic.

In line with ISO 17021-1, for initial certification an initial audit is performed.

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

Surveillance audits follow in the first and second years following the certification decision.
Surveillance audits entail a limited evaluation of the quality management system.
Recertification audit follows in the third year, prior to expiration of certification. This entails a new full evaluation of the quality management system.

4.2.3 Communication with the client

The certification body is able to provide the awareness training provider by way of information and/or on request of the awareness training provider with detailed information on:

- the contents, context and purpose of the certification scheme;
- the contents, context and purpose of NEN-EN-ISO/IEC 17021-1 and the documents and interpretations on a national and international level that have been designated as applicable by the national accreditation body;
- the procedures, methods, regulations regarding (not limitative):
  - application;
  - budget of hours and costs for performing certification assessments;
  - planning;
  - audit program and planning;
  - phasing of initial assessment and re-assessment;
  - surveillance assessment;
  - use of certification mark;
  - plan-do-check-act approach;
  - non-conformities and corrective actions;
  - suspension and withdrawal;
  - disputes and appeals;
  - termination of the certification contract.

This information can be general information or related to specific parts of the certification scheme.

4.3 Requirements for performing certification

4.3.1 Qualifications

The certification body establishes the qualifications of the certification personnel involved, with substantiation that the qualification requirements set in this certification scheme are met.
Competency requirements (knowledge and skills) may be substantiated by education and experience.

The certification body establishes a training programme for newly qualified certification staff, aimed at achieving the required competences.

The certification body establishes a programme for each qualified employee for monitoring and evaluating the competences set. This programme is kept up to date.

Normative for qualification are the competences of the certification personnel. Education, experience and skills may contribute to substantiating the required competences.

See NEN-EN-ISO/IEC 17021-1.

For the certification scheme is the following minimum applicable:

- Competences as auditor – general – conform ISO 17021-1;
- competences for the professional expertise as an auditor for assessing a quality management system of the awareness training provider.

To comply with the requirements of ISO 17021-1, the certification body establishes the competences in sufficient detail. This applies not only for the auditors involved, but also for the certification personnel involved in the certification process, e.g. in (not limited):

- processing the application, quotation;
- qualifying the certifying staff;
- monitoring the certifying staff;
- reviewing audit reports;
- decision;
- administrative processing of certificates;
- handling of complaints.

4.3.2 Assessment techniques

In addition to the audit techniques described in NEN-EN-ISO/IEC 17021-1 (interviews, observations and administrative verification), the assessment techniques conform ISO/IEC 27006, annex D may also be applicable.

Assessment of the process requirements and technical requirements takes place during the initial assessment, every surveillance assessment and reassessment.

Observations of ongoing awareness training is not a standard procedure, but can be applied, at the discretion of the certification body.

4.3.3 Time spent

Different factors can influence the total audit time, amongst which: whether a service provider has other certificates with a relevant scope (i.e. ISO 9001 or other CCV cyber security certificates), number of employees, how many different forms of training are offered and the number of training assignments per year. The following time spent is assumed:

Initial audit and recertification
Preparation time for the entire assessment takes 2 hours.

For assessment of the quality system, the starting point for the initial assessment is 6 hours.
If the service provider already has relevant other certificates which justify a less extensive assessment of the quality system, this can be reduced to a lower limit of 4 hours at initial assessment.

The number of hours can also be increased if it concerns a service provider that carries out many training sessions per year, a large number of personnel is involved, the organisation is complex and/or the way the quality system is organised makes the assessment more time-consuming. No maximum applies here.

Full reporting (on quality system + service-oriented control) takes 4 hours.

Note

For an initial audit, without relevant prior other certificates, assuming checks of 2 training files (see 4.4) , this accumulates to 16 hours.

For recertification, see 4.4 for number of training files, and time for training files as mentioned below.

Surveillance audits - QMS
Preparation time for the entire assessment takes 2 hours.

For assessment of the quality system, the starting point for the periodic assessment is 4 hours. If the service provider already has relevant other certificates that justify a less extensive assessment of the quality system, this can be reduced to a lower limit of 3 hours at periodic assessment. The number of hours can also be increased if it concerns a company that delivers many training sessions per year, a large number of personnel is involved, the organisation is complex and/or the way the quality system is organised makes the assessment more time-consuming. No maximum applies here.

Full reporting (on quality system + service-oriented control[11]) takes 4 hours.

Note

For surveillance audits, without relevant prior other certificates, this accumulates to 12 hours, excluding time required for checks on training files.

Training files
For checks on executed training, via the sample size given in 4.4, the following minima per file are assumed:

- 1 to 3 files: 2 hours per file
- 4 to 5 files: 1 ½ hours per file
- 6 or more files: 1 hour per file

Notes for clarification
- Example: if 7 files need to be checked, a total time spent of 7 hours is assumed.
- These three sample sizes overlap in time to be spend; they are to be considered as rough indications only.

Evaluation of time spent
At the end of the audit, be it in the form of initial, surveillance or recertification, the certification body provides an evaluation of the time spent in relation to the set objective and, where necessary, adjusts the audit planning, the audit programme and the time spent, including (if necessary) an addition to the audit carried out.

The certification body provides a fully documented foundation for the audit planning, the audit programme, the time expenditure and the adjustments to this for the purpose of harmonisation investigation by the CCV.

4.3.4 Complaints and appeals
The certification body handles complaints and appeals according to its regulation that is applicable under accreditation.

4.3.5 Publication
In addition to NEN-EN-ISO/IEC 17021-1:
After a positive decision, the certification body publishes the details of the awareness training provider on https://hetccv.nl/bedrijven. This website is owned and managed by the CCV.

4.3.6 Additional assessment
In addition to NEN-EN-ISO/IEC 17021-1:

[11] For time assumed for service orientated assessment, see table B.

The certification body may carry out additional assessments if there is reason to do so. Reasons may be:

- the results of other assessments;
- complaints that the awareness training or the awareness training provided does not meet the requirements set;
- complaints about misleading or incorrect use of the certification mark;
- publications;
- own observations by the certification body;
- information from interested parties, such as the government and/or insurers.

Implementation, reporting, review, decision making and possible sanctions are subject to the provisions set in this certification scheme.

4.4 Sample sizes on executed training

The service provider provides the certification body with insight in all of its executed training assignments over the previous period. The certification body decides which files it checks.

Initial certification audits: at least two files of executed trainings are checked.

- For level 1, this means two files per form or category of provided trainings.
- For level 2, this means two files of integrated courses as provided, plus, if relevant, two files per form or category of separately delivered training sessions.

Surveillance audits and recertification audits: checks are done based on the following sample sizes.

NUMBER OF TRAINING SERVICES DELIVERED PER YEAR	NUMBER OF CHECKS
0	-[12]
1	1
2 to 10	2
11 to 30	3
31 to 50	4
51 to 100	5
101 to 150	7
151 to 300	9
301 and more	11

In case of certification on level 1, this table is applied to every category or form of training that is offered.
(Example: if a service provider delivers 26 workshops and 41 table top exercises, this leads to checks on 3 files of delivered workshops, and checks on 4 files of delivered table top exercises.)

[12] If less than one training referred to in Chapter 2 is delivered per calendar year, the certification body must make further agreements with the service provider under which condition the service certificate issued by the certification body will remain valid. If the service provider does not provide awareness training according to this certification scheme for two consecutive years, the certification body must suspend the certificate.

In case of certification on level 2, the same sample size mentioned above is used for delivered integrated training courses. If an integrated training course is delivered to a client recurrently, it the assignment by the client counts, in the context of this table, as one integrated training course per year.

If a service provider under level 2 also delivers separately delivered or "one off" training sessions, checks by the certification body are also executed on those services. In those cases, in addition to checks on integrated courses as described above, the follow table applies:

NUMBER OF TRAINING SERVICES DELIVERED PER YEAR (SEPARATE TRAINING SERVICES, BY PROVIDER UNDER LEVEL 2)	NUMBER OF CHECKS
1 to 5	1
6 to 30	2
31 to 50	3
51 to 100	4
101 to 150	5
151 to 300	7
301 and more	9

The certification body will see to a reasonable distribution of different forms of training provided, and/or different branches of the service provider, if applicable. In addition, the certification body has the option to witness the process of awareness training, as a live ongoing process, as provided to a specific client.

4.5 Deviations

4.5.1 General

A situation which is not in accordance with the requirements is considered a deviation. Based on the definitions in sections 4.5.2 and 4.5.5, the certification body classifies deviations as major or minor.

The certification body communicates deviations to the awareness training provider at the conclusion of the audit.

4.5.2 Major - Quality System

- One or more requirements from the certification scheme have not been implemented, or based on objective observations the situation raises significant doubt as to whether the quality system provides sufficient support for the awareness training provider to deliver awareness training that meet the requirements set, or
- The same deviation had been found in the last assessment, or
- Failure to register complaints and/or failure to follow up on complaints, or
- Misuse of the certification mark, or
- Fraud, deception of the certification body or deliberately providing incorrect or incomplete information to the certification body.

4.5.3 Major – Consequences

In the event of major deviations, the awareness training provide presents an action plan within a period to be determined by the certification body, not exceeding seven working days.

Errors made are corrected immediately. The plan of action consists at least of:

- an analysis focused on the root cause and/or root causes of the deviation. This analysis includes in any case (not limited) the possible causes in the process of implementing awareness training and the possible causes in the failure of control processes;
- actions to remedy the deviation (correction);
- solutions aimed at preventing recurrence and securing them (corrective actions);
- the assessment of the effectiveness of the implementation of these solutions (e.g. with an internal audit).

The awareness training provider fully documents the corrective actions to be implemented according to the action plan, so that they are verifiable by the certification body. The period for execution of the action plan is at most two months.

4.5.4 Major - Assessment by the certification body

The certification body assesses the action plan for efficiency and effectiveness in relation to the non-conformity found within a period of no more than seven working days from the agreed date of receipt.

During the implementation period, the certification body may intermediately assess the implementation of the action plan and the solutions proposed by the awareness training provider are implemented. If implementation of the corrective action plan lags behind, the certification body may suspend the awareness training provider.

The certification body assesses the implementation of the corrections and the implementation of the corrective measures, to establish that the nonconformity has been removed. The assessment method depends on the nature of the nonconformities. If necessary, an additional assessment is carried out for verification.

The following terms and procedures are applicable:

- In case of initial assessment: conform the regulation of the certification body;
- In case of surveillance assessment, additional assessment and reassessment: within three months. The certification body may extend the period for corrections and corrective actions once, with substantiation, by a period of two months.

If the deviations have not been lifted, the suspension procedure is applicable (see section 4.6.1).

4.5.5 Minor - Quality System

- The absence of, not having implemented or not having maintained one of the requirements from the certification scheme, which has not led to a major deviation, or
- Failure to maintain one or more of the conditions of this certification scheme (including financial obligations and the regulations for use of the certification mark).

4.5.6 Minor – Consequences

The awareness training provider shall be given a period of two months to take corrective action. The corrective measures must include at least:

- an analysis focused on the root cause and/or root causes of the deviation. This analysis includes in any case (but not be limited to) the possible causes in the process of implementing awareness training and the possible causes in the failure of control processes;
- action to remedy the deviation (correction);
- solutions aimed at preventing recurrence and securing them (corrective actions);

- the assessment of the effectiveness of the implementation of these solutions (e.g. with an internal audit).

The awareness training provider shall fully document the corrective actions to be implemented, so that the certification can verify them.

4.5.7 Minor - Assessment by the certification body

To ascertain that the nonconformity has been remedied, the certification body assesses the implementation of the corrections and the implementation of the corrective measures. The method of assessment depends on the nature of the nonconformities. If necessary, an additional assessment shall be carried out for verification.

The certification body applies the terms and procedures conform the regulations of the certification body.

4.6 Suspension

4.6.1 Suspension

The awareness training provider will be suspended:

- when failing to provide a plan of action on time when determining a major deviation (see section 4.5.3), or;
- for an action plan that does not sufficiently guarantee that corrections will be carried out and/or that does not sufficiently guarantee the execution of the cause analysis and implementation of corrective measures (see sections 4.5.3 and 4.5.6), or;
- if the corrective actions for both major and minor deviations have not led to the remedying of the deviation(s) within the set (extended) timeframe (see sections 4.5.3 and 4.5.6), or;
- in the event of non-compliance with the conditions for certification (including financial obligations and obligations concerning the use of the certification mark), or;
- if the awareness training provider damages the interests and image of the certification scheme, the certification body and/or the CCV.

The certification body documents the assessor's advice, the review and decision-making process and the decision in full, including the substantiation.

The certification body informs the awareness training provider of the suspension by registered letter or by e-mail with confirmation of receipt.

4.6.2 Consequences of suspension

The certification body publishes the suspension on https://hetccv.nl/bedrijven. From the moment of suspension, the awareness training provider may not use the certification mark. Nor may the awareness training provider refer to the certified status of the quality management system.

4.6.3 Lifting the suspension

When the certification body establishes that all deviations have been removed, the suspension shall be lifted. The certification body informs the awareness training provider in writing of this and cancels the publication of the suspension. From the date stated in writing by the certification body, use of the certification mark shall be permitted again.

A suspension lasts a maximum of six months.

4.7 Withdrawal

4.7.1 Withdrawal

The certificate shall be revoked if the awareness training provider is unable to remedy the deviations found within the period of suspension.

The certification body informs the awareness training provider of the withdrawal by registered letter or by e-mail with acknowledgement of receipt.

4.7.2 Consequences of withdrawal

The certification body publishes the withdrawal on https://hetccv.nl/bedrijven

From the moment of withdrawal, the awareness training provider shall no longer use the certification mark or refer to the certified status of the quality management system.

4.7.3 New application

An awareness training provider of which the certificate has been revoked may again apply for an initial assessment in accordance with the certification scheme.

5 Certificate and certification mark

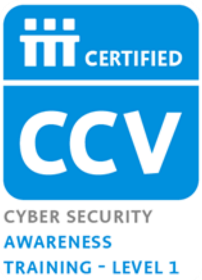
5.1 Certification mark

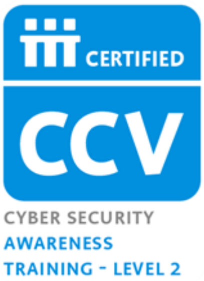
The certification mark, further called ‘the mark’, is the proof for clients that the certification body has a justified confidence that the quality management system of the awareness training provider complies with the requirements set in the certification scheme (as described in chapters 2 and 3) and that the contractual and regulatory conditions have been met. The mark is executed as a logo, see section 5.1.1.

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

5.1.1 Certification mark

The certification marks shown below are associated with this certification scheme.





5.1.2 Use of the mark by the certification body

The certification body uses the mark in accordance with the CCV’s “Reglement Kwaliteitslogo”. Main conditions for the use of the certification mark are:

- The certification body has a valid license with the CCV.
- Illustrative use on letterheads, website, folders and other publicity material with references to the certification scheme.

5.1.3 Use of the mark by the awareness training provider

The awareness training provider uses the mark in accordance with the CCV’s “Reglement Kwaliteitslogo”.

Main conditions for the use of the certification mark are:

- The awareness training provider has a valid certification contract13 and has not been suspended.
- Application of the mark only in information related to the certified quality management system;
- Illustrative use on letterheads, website, folders and other publicity material with references to the certification scheme.

5.2 Management system certificate

The certification body provides a management system certificate to the awareness training provider. This certificate shall be drawn up in the house style of the certification body.

The management system certificate contains at least the following data:

- Name and address of the certification body;
- Name and address of the awareness training provider (correspondence address);
- the texts

  "<Certification body> declares that the quality management system of < awareness training provider > complies with the requirements in the CCV-certification scheme Awareness Training Provider, version 1.0."

  "The scope is certification level 1: The quality management system is certified for providing separately delivered (one time) awareness training sessions."

  or

  "The scope is certification level 2: The quality management system is certified for providing integrated awareness training courses"

  And

  "<Certification body> licenses the mark shown here to <the awareness training provider> for use according to the CCV certification scheme."

- a unique certification number;
- date of issue/replacement;
- if applicable, the original issue date;
- the expiry date[14];
- (digital) signature (with name and function);
- the company logo of the certification body;
- the QMS-logo;
- the text:

  "Cyber security awareness training providers and third parties can check the status of a valid management system certificate with <certification body> or on <reference to https://hetccv.nl/bedrijven> "

  "This certificate remains the property of <certification body>."

[13] Startingpoint is that this certification contract is concluded with a certification body that has a valid license with the CCV for this certification scheme.

[14] Explanatory remark: conform ISO 17021, the certificate is valid for three years.

6 References

6.1 Terms and abbreviations

Assessment	Implementation of this certification scheme by the certification body at the awareness training provider of the cyber security awareness training.
Audit	Systematic, independent and documented process for obtaining audit evidence and objectively assessing it to determine the extent to which agreed audit criteria have been fulfilled
CCV	Centrum voor Criminaliteitspreventie en Veiligheid (Centre for Crime Prevention and Safety)
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.
Client	Person or organisation that purchases the cyber security awareness training and orders the awareness training provider to carry out the training.
Initial assessment	Assessment leading to a decision on certification and, in the event of a positive decision, issue of the management system certificate.
ISO	International Organization for Standardization. An ISO standard is an international standard issued by ISO.
NEN	Foundation Royal Dutch Standardisation Institute. The NEN publishes the Dutch standards.
Periodic assessment	Assessment aimed at confirmation that the requirements and conditions are still met, thereby maintaining certification.
Standard	Document in which the parties involved set down agreements with the aim of keeping to them.
Management system certificate	Document prepared by the certification body, declaring that the quality management system meets the requirements of the certification scheme
Awareness training provider	The organisation providing the cyber security awareness training.
VOG	Verklaring Omtrent Gedrag, Certificate of Conduct.

6.2 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). In case of a dynamic reference, the version with the transition periods as indicated by the manager of the document applies. 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 herein. A certification body possesses all normative standards and documents. The awareness training provider has at his disposal at least those standards and documents marked with an *.

STANDARD	TOPIC	AVAILABLE
NEN-EN-ISO 17021-1	Conformity assessment - Requirements for bodies performing audits and certification of management systems	NEN, Delft
NEN-EN ISO 9001	Requirements for quality management systems	NEN, Delft
NEN-EN ISO/IEC 27001	Requirements for information technology, security techniques, information security management systems	NEN, Delft
WCAG	Web Content Accessibility Guidelines *	World Wide Web Consortium (W3C)
	CCV-reglement kwaliteitslogo (regulation concerning use of CCV certification mark)	CCV, Utrecht

Annex A – Example of formats for awareness training

TABLE ANNEX A – CYBER SECURITY AWARENESS TRAINING – EXAMPLE OF FORMATS

TRAINING FORMAT	REQUIREMENTS THAT MAY NEED SPECIFIC ATTENTION
A. Examples of forms that can be delivered under Level 1	
Workshop (on location or online)	Testing of knowledge of individual participants is done both prior to or at the start of the workshop, and after the workshop. Participants are stimulated to actively participate and contribute.
Forms of gamification, such as: - educational escape room - tabletop session - crisis exercise	- Testing of knowledge of individual participants is done both prior to/at the start of the training, and after the training. - The cases/incidents are translated into more generic lessons. - All topics mentioned in the plan are properly addressed. (Possible in combination with part of the training in a different format.) - The session is followed by an interactive group evaluation.
Online "on demand" training (pre-recorded lessons or sessions) / e-learning	At least part of the training is tailor made or the result of specific selections of available material; it focusses on specific (cultural) conditions in the client's organisation.
B. Examples of forms/instruments that can be an additional element in an integrated training course under Level 2, but cannot be delivered independently under certification under Level 1	
Phishing test	- Targets are selected and e-mails are designed via a standardized method within the awareness training provider and by considering specific circumstances or concerns regarding the organisation of the client. - Analysis of results is shared with both the client and all its personnel, with clear and explicit lessons.
Cyber security mystery guest	- Scenario(s) is/are realistic in context of the specific client. - "Lessons learned" are presented in such a way that it can be shared with the client's staff.

CCV centrum voor criminaliteitspreventie en veiligheid

Centre for Crime Prevention and Safety |
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