centrum voor criminaliteitspreventie en veiligheid

CCV certification scheme

Cyber Security Pen Test

Version 2.0
Publication date: 1 January 2024
Effective date: 1 April 2024

Foreword

This certification scheme is aimed at the certification of penetration tests - hereafter referred to as 'pen tests' for short - according to NEN-EN-ISO/IEC 17065.

Het ‘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.

The certification scheme is structured according to the model used by the CCV for service 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

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 company to protect itself against attacks, vulnerabilities, or other threats. Cyber security services ensure that digital systems are properly secured, in line with the risk of a cyber incident. This security consists of a combination of digital security and organisational measures. A company that wants to protect itself against cybercrime needs this to be done properly, with safe products and installed or carried out by a professional. This is often difficult for the enterprise to assess properly on its own. Certification schemes for cyber security services offer a good solution for this purpose. This certification scheme focuses on pen testing.

1.1 General

1.1.1 Purpose

A pen test results in concrete, technical recommendations to reduce the vulnerability of a digital system. Pen testing must be carried out professionally. Government and private parties have a need for guaranteed quality of pen tests. This assurance is possible with service certification of pen tests.

The aim of the certification of the pen test is to reduce the costs of failure and risks for customers that may occur when the supposed quality of the pen test is not up to an industry recognised standard. Certification allows clients to have a legitimate confidence that the supplied pen test, provided with the certification mark, meets the requirements set in advance.

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

1.1.2 Responsibilities

The recipient is responsible for the security of digital systems and for taking the corresponding measures. This includes the periodic execution of a pen test.

The organisation providing the pen test - hereafter "the service provider" - is responsible for ensuring that the pen test to which the certification mark is applied (see section 5.1) complies with the requirements set out in the certification scheme.

1.1.3 Reading guide

The certification scheme contains:

- requirements to be met by the pen test, how this is assessed and when to approve or disapprove the pen test (chapter 2);
- conditions for the service provider to obtain and maintain the service certificate (chapter 3);
- harmonised working methods used by the certification body when processing a certification application and maintaining the service certificate (chapter 4);
- description of the certificate issued by the certification body to the service provider, the test report with certification mark issued by the service provider to the client (chapter 5).

1.2 Scope

The scope is the execution of the pen test, including test reporting, or the execution of a vulnerability assessment, including test reporting. Vulnerability scans (see 6.1) are excluded.

When a service provider delivers pen tests under the certification scheme, all his pen tests (including vulnerability assessments) are delivered in accordance with the criteria in this scheme and are delivered with the CCV certification mark. This includes pen tests performed as part of the following services (this list is not exhaustive):

- White box security test
- Grey box security test
- Black box security test
- Crystal box security test
- DigiD pen test
- Fat client (client/server application investigation)
- Internal pen test
- Mobile app security test
- Wi-Fi security test

Intermediate partial tests and spot checks are excluded from the certification mark.

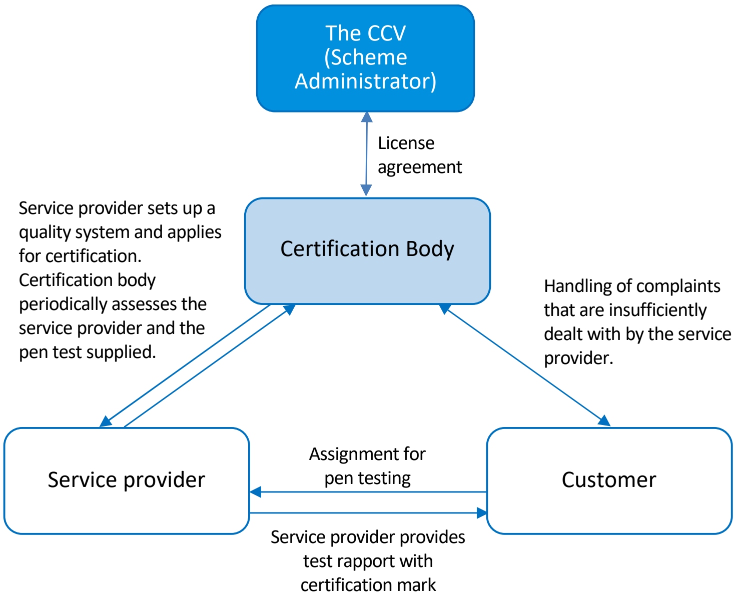
For specific cases that can form exceptions to the rule ‘all pen tests under certification’ and conditions for such exceptions see section 4.5.2.

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 service certification


The CCV (Scheme Administrator)
License agreement
Certification Body
Service provider sets up a quality system and applies for certification. Certification body periodically assesses the service provider and the pen test supplied.
Handling of complaints that are insufficiently dealt with by the service provider.
Service provider
Customer
Assignment for pen testing
Service provider provides test rapport with certification mark

1.5 Transitional provisions

This certification scheme Cyber Security Pen Test version 2.0 replaces version 1.0.
Version 2.0 is effective per 1 April 2024. After this date all initial and periodic assessments will be performed based on this scheme.

There may be service providers who have been assessed based on scheme version 1.0 until 1 April 2024 and still need to take recovery and corrective measures in (the first half of) 2024. After implementing these measures and positive findings by the certification body, they receive a certificate based on scheme version 1.0 (or in the case of a periodic assessment, keep the original certificate).

All assessments, initial and periodic, executed per 1 April 2024 and leading to a positive conclusion result in a new certificate based on scheme version 2.0 for the service provider.

1.6 Main changes compared to version 1.0

- The certification scheme is translated in English. This certification scheme will be only published in English.
- Section 1.2: the scope is clarified, among other things, with examples of pen tests.
- Section 1.5: provides transitional provisions from version 1.0 to version 2.0.
- In chapter 2 requirements have been added and edited. It concerns requirements of:
  - test plan
  - testing process
  - findings and test report.
- In section 3.2.1.1 makes it possible to work with employees not (yet) demonstrably qualified, if working under supervision. Here a criterion is added stating that the supervising qualified pen tester needs to provide at least 50% of the total time used for the pen test.
- Section 3.2.2, qualifications, asks for at least one year of working experience. This criterium is clarified, by adding that experience as intern does not qualify.
- In 3.2.3, an assumption is made into an explicit criterion; all third-party tooling uses by a service provider is acquired and used in a legal manner.
- In chapter 4 the sections 4.4.2 and 4.5.2 about time spent and sample have been edited, largely based on two documents published under version 1.0 of the scheme, aimed at harmonised implementation.

2. Service requirements

With service certification, the requirements for the service provided under certificate are central.

2.1 General

All technical and administrative requirements with which the pen test supplied under certificate must comply, and the way in which this is assessed, are included in this chapter. Failure to meet the requirements in this chapter constitutes rejection.

2.2 Assessment methods, requirements, approval and rejection

In this section, the assessment methods listed in table 2a are used.

Table 2a: Assessment methods

METHODOLOGY	DESCRIPTION
(A) Administrative	Assessment of administrative documents such as design documents, certificates and reports A1: Assessment of completeness A2: Assessment of correctness NOTE *Assessment A1 and A2 can only be carried out if the documents are present*

2.2.1 Test plan

Table 2b: Test plan

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT	REJECTION IF
Language of test report is acceptable for each client	The quote or test plan clarifies whether the test report will be written in Dutch or English or provides the client a choice between those languages.	A1	This information or choice is not presented to clients.
Concrete technical limitation of the test object	Quote and/or test plan describes scope in terms of IP addresses/host names/specific applications and this corresponds to the report.	A1	The scope has not been unambiguously determined before commencement and/or does not correspond to the scope description in the report.
Preparing for possible incidents	There is an agreement on how to deal with possible incidents during the pen test.	A1	There is no test plan or other written agreement exchanging contact information for direct technical contact (e.g. trusted contacts) in the event of an incident.

2.2.2 Testing process

Table 2c: Test process

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT	REJECTION IF
Defined methodology	The service provider has a defined, standardized methodology to perform a penetration test[1]. (The methodology can be proprietary or based on an open standard.)	A1	The service provider cannot demonstrate a defined methodology.
Record of executed tests	A record is kept of actually executed tests on specific parts of the object/environment that was tested. (For instance, via a checklist).	A1	Pen test files do not contain these records.
Continuous improvement methodology	When during a pen test issues are encountered not properly addressed in the defined standardized methodology, they lead to addition or other structural improvements of the defined methodology.	A1	The process of continuous improvement cannot be demonstrated by the service provider.
Consult with customer about test object	The service provider / pen tester consults the customer prior to the test, to understand what the test object includes, and what the normal functioning of the test object is. The findings are included in a short report or log.	A1	The service provider / pen tester can't provide a short report or log of the consult with the customer.

2.2.3 Automated tests – tooling

Automated tests can be used to carry out a pen test: tooling. Tooling is only used as an aid and is not leading in the execution of a pen test. Findings are not exclusively based on the use of tooling but are verified by a subject matter expert (3.2.2 qualifications). When tooling is used, a selection of the tools to be used to demonstrate possible vulnerabilities is made based on the test plan. The tools to be used must be shown to be suitable for carrying out the pen test or vulnerability assessment.

Table 2d: Automated tests

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT	REJECTION IF
Automated tests	All findings from the automated test have been manually verified or reviewed by a qualified Pen tester	A1	Automated tests have not been manually verified or reviewed by a qualified Pen tester

[1] The object or environment can be a particular type of operating system, an application, middleware, infrastructure, a cloud environment, etc.

2.2.4 Manual tests

Table 2e: Manual tests

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT	REJECTION IF
Manual tests	Manual tests have been carried out	A1	Only automated tests have been carried out

2.2.5 Findings and test report

Upon completion of the pen test activities, the service provider of the pen test provides a written report, the test report. The qualified Pen tester is ultimately responsible for the execution of the pen test and reporting to the client.

The test report shall contain at least the following sections:

Table 2f: Findings and test report

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT	REJECTION IF
Test report – Contents	The test report must contain at least the following items: - Executive summary - Representation of the customer (who) and the customer demand - Scope and activities carried out, indicating at least: - which security measures have been disabled by the customer to be able to carry out the pen test, and - explains which actions have been implemented on which systems - IP addresses used for the pen test - Conclusions - Recommendations - List of technical findings, including for each finding a risk assessment based on risk methodology with analysis of the impact and likelihood of occurrence and a recommendation for resolution	A1	No report has been delivered, or the report is incomplete.
Pen test findings	The findings of the pen test must be described in such a way that the client or the responsible IT employee himself can deduce that a finding is justified.	A2	The findings are not described in a traceable way.

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT	REJECTION IF
	Note: The level of detail used to report to a client about these findings (including logs for example) is up to the service provider, as long as the criterium is met. If it is not included in the report, the service provider should keep this data for assessment by the certification body.		
Test report - language	The report shall be drawn up in the Dutch or English language, as mentioned in the quote or test plan provided to the client.	A2	The report was not delivered in the agreed language.
Test report – certification mark	The report shall bear the mark referred to in 5.1 of this s, indicating that the pen test has been conducted correctly by qualified personnel, compliant with CCV certification scheme Cyber Security Pen Test 2.0.	A2	The mark is not affixed; or the pen test was not carried out correctly; or the pen test was not carried out by qualified personnel.

3. Conditions for the service provider

This chapter describes the conditions to be met by the organisation providing the certified service (the service provider).

3.1 General

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

The service provider provides the certification body with all requested information and data. Failure to do so may result in the sanctions described in sections 4.9 (suspension) and 4.10 (withdrawal).

3.2 Quality system requirements

Service certification is primarily about meeting the requirements as described in chapter 2. The quality system has a supporting character, aimed at the continuous securing of the quality of the pen test executed under certificate. In the following sub sections the requirements of the quality system are further elaborated.

3.2.1 Organisation and responsibilities

The service provider has an overview of the employees whose work influences the quality of the pen test 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 are 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 pen test service, 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 service and the reports delivered and has provided at least 50% of the total time used for the pen test.

3.2.1.2 Continuity

For the sake of continuity of operations, replacement of the experts must be organised by the service provider. 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. The service provider establishes that all employees involved in tasks indicated in the certification scheme meet the qualification requirements. Only qualified personnel is deployed for the tasks mentioned. Qualifications are kept up to date and registered. There is an annual evaluation whether the qualification requirements are still met.

Employees are qualified by the employee in charge based on practical certificates.

Qualifying practical certificates are certificates with a practical examination in a lab environment that are considered to be of sufficient quality by the sector. The 'entry level' certificates such as CEH and LPT are not taken into account. The list of relevant certificates (pen testing qualifications) is published by the CCV (www.hetccv.nl).

RESPONSIBLE FOR EMPLOYEE QUALIFICATIONS	
Qualification	By the Executive Board
Level	HBO work and thinking level
Knowledge of and ability to work with	This certification scheme

PEN TESTER	
Qualification	By responsible for employee qualifications
Practical certificate	Qualifications for pen testing, see CCV website
Experience	At least 1 year of experience in ICT services and performing pen tests. Experience as intern does not qualify.
Knowledge of and ability to work with	■ This certification scheme ■ For the test report: Dutch language on level C1 and/or English language on level C1
Maintaining qualification	According to the service provider's training and evaluation plan

To keep the knowledge level within the company up to standard, the service provider has a demonstrable policy on training, development and knowledge sharing.

All employees involved in the pen testing process and/or who have access to the information (permanent or externally hired) are in possession of a relevant 'certificate of conduct' (COC) - in Dutch: Verklaring omtrent gedrag (VOG) - as referred to in the Judicial and Criminal Records Act, Article 28. The VOG/COC may not be older than three years.

3.2.3 Measuring means and equipment

The service provider has an overview of tooling that is deployed in the context of delivering pen tests under certificate. The service provider declares that all 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 service provider can provide the certification body with proof.

3.2.4 Outsourcing

The service provider may subcontract work to another pen test service provider. Fully outsourcing a large part of pen testing assignments is not acceptable.

In addition, the following applies here:

The service provider shall assess in advance, based on the requirements in section 3.2 and the requirements in chapter 2, whether the other service 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 service provider cannot subcontract the task.

- In the event of a positive conclusion to the assessment, the service provider is and remains responsible for the quality of the outsourced work and for the certified pen test it provides.

- If the service provider to whom the pen test is outsourced carries out the work under valid service certification in accordance with the CCV Certification Scheme Cyber Security Pen Test, the service 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 service provider is in that case limited to verification of the contractor's service certificate.

3.2.5 Hiring

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

3.2.6 Primary processes

The service 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 the delivered pen test is secured.

Security policy

The service provider has a security policy that covers, as a minimum, the systems used in pen testing, as well as the data obtained from clients in the context of conducting pen tests. This policy shall include, as a minimum:

- concrete technical security measures to protect customer information;
- concrete time limits for the storage and cleansing of raw data resulting from a pen test, whereby the minimum storage time is one year[2], so that the certification body can perform a check;
- description of the means the service provider offers to exchange encrypted confidential data - such as the report - 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 customer.

Starting information and consent

The service provider must have procedures for accepting an order to perform a pen test. For this purpose, at least the following starting information must be available:

- the scope of the assignment in terms of IP addresses/host names;
- concrete technical limitation of the test object;
- project documentation.

The starting information forms the basis for the test plan (see 2.2.1). In addition to the starting information, the consent of all owners of systems in scope is necessary.

3.2.7 Document management, registrations and archiving

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

The service provider has knowledge of the following documents:

- the documents mentioned in section 6.2, including the documents referred to therein;

[2] Par. 4.5.2 offers an alternative approach for a limited subset of projects/clients, in case of special concerns regarding security.

- the written procedures and work instructions resulting from the certification scheme;

The service provider shall keep these documents up to date and inform its employees accordingly.

Registrations

The service provider has the following registrations:

- overview of employees[3] , 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 service provider is laid down (e.g., contract, order confirmation, own registration of a verbal order, e-mail);
- certificates and statements linked to address data of pen test performed.

The data of the service provider must be kept for a period of at least one year[4]. This refers to data regarding the quality system itself, but also to data regarding delivered pen tests (see 3.2.6) and pen test reports.

3.2.8 Complaints

The service provider shall have a written procedure for complaints, complaint analysis, resolution and corrective action to prevent recurrence.

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

3.2.9 Recovery and corrective measures

The service provider shall have a written procedure for recovery and corrective action. In case of errors and deviations found, the service provider shall take corrective action in addition to the correction. Corrective measures are aimed at preventing the error from occurring again. In the event of non-conformities established by the certification body, specific conditions apply, see section 4.8.3 and section 4.8.7.

3.2.10 Evaluation

The service provider can demonstrate that all the conditions referred to in this chapter (conditions for certification) and chapter 2 (requirements for service) are permanently fulfilled. To this end, the service provider makes an annual analysis:

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

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

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

3.3 Requirements for application and maintenance

3.3.1 Application data

The service provider provides the certification body with the following data upon application:

- proof of legal registration[5];
- a declaration by an authorised person that the service provider will comply with the requirements, conditions and obligations stated in the certification scheme;
- the possible presence of several branches, which provide pen tests.

The service provider also provides the certification body with all necessary information and data upon request (see section 4.3).

3.3.2 Status during application

Until the initial assessment has been concluded with a positive decision (see section 4.4), 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 service 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 the execution of the pen test.

3.3.4 Planning

The service provider provides the certification body with all information about all pen tests (for instance when, which customer, what kind of pen test, which pen tester) 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 service provider reports relevant changes in the organisation to the certification body in a timely manner. These are changes such as:

- mergers and acquisitions;
- changes in the organisational structure;
- changes in the quality system, which affect the:
  - quality of the pen test;
  - quality assurance of the pen test;
  - 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 in this certification scheme >

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

4. Conditions for the certification body

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

4.1 Requirements for the certification body

4.1.1 General

Certification bodies can conclude certification contracts with service providers if they have a licence agreement for the certification scheme[6] with the CCV.

This certification scheme is not yet implemented under accreditation.

This certification scheme assumes harmonised implementation under NEN-EN-ISO/IEC 17065. The documents and interpretations related to this on a national and international level are applicable by the national accreditation body.

When implementing this certification scheme, the certification body uses NEN-EN-ISO/IEC 17065 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 of this by submitting the subject for harmonisation.

Certification bodies may, as far as not conflicting with this certification scheme, apply their own regulations and procedures for service certification. 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.

4.1.2 Qualifications

4.1.2.1 General

The staff of the certification body shall be qualified based on the required competences. Competences are based on demonstrable "knowing" and "ability".

The certification body may, for the qualification of the personnel involved in the implementation of this certification scheme, impose additional requirements regarding diplomas, training and work experience in order to obtain more certainty that the required competencies can be met. It does not discharge the certification body from the obligation to form its own opinion, based on its own observations (e.g. observation in the field, interviews, assessment of reports, peer review), that the required competencies are met.

The certification body shall set up a training programme for newly qualified certifying staff, aimed at achieving the required competencies.

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

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

Certification staff directly involved in certification assessments (auditors, inspectors) shall be monitored at least once every three years.

The certification scheme lays down the general competences for auditors and personnel who perform the service-specific assessment. The certification body must detail the competences sufficiently in line with its own organisation to meet the requirements of NEN-EN-ISO/IEC 17065 and ISO 27001. This applies to all certification staff involved in the certification process, including staff conducting the audit and service-specific assessment and any subject-matter experts. The certification process includes (but is not limited to):

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

The certification body records the fulfilment of the required competences of the involved personnel, including the substantiation thereof.

The certification body determines for each employee involved for which activities the employee can be deployed.

4.1.2.2 Competences for conducting the audit

To carry out

- the assessment of the effective implementation of the quality assurance system (audit);
- the assessment of the procedures for using the certification mark,

the following competences apply as a minimum:

- the requirements according to NEN-EN-ISO/IEC 17021-1 annex A (table of knowledge and skills);
- knowledge of and ability to work with the certification scheme;
- being able to assess and weigh the possible effects of an observed deviation;
- being able to explain and communicate findings and deviations to the service provider;
- report the findings and deviations and their weighting in unambiguous writing.

4.1.2.3 Competences for carrying out the service-oriented assessment

To carry out:

- verification of project files,

the following competences apply as a minimum:

- the ability to evaluate the delivered pen test against the requirements set in chapter 2 of the certification scheme;
- being able to assess and weigh the possible effects of an observed deviation;
- being able to explain and communicate findings and deviations to the service provider;
- being able to report the findings and deviations and their weighting unambiguously in writing;
- the qualification requirements for the system part ISO 27001;
- have knowledge of and can work with the certification scheme;

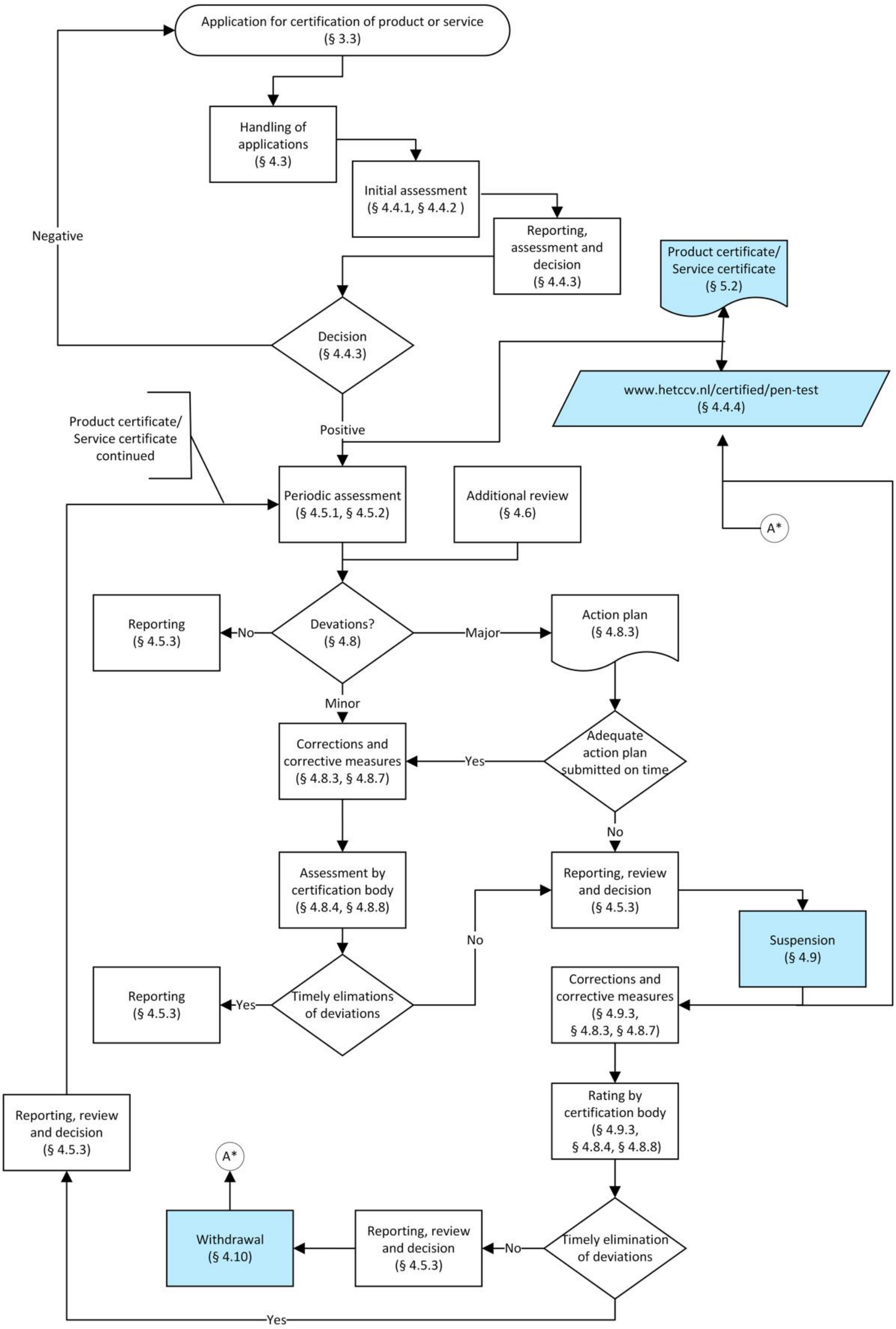
- have knowledge of performing pen tests.

4.1.2.4 Facilities and equipment

The certification body does not have to have its own facilities or equipment for performing service-based assessments. The certification body may use the tooling of the service provider as referred to in section 3.2.3 (measuring means and equipment).

4.2 Process diagram

Figure 2 - Service certification process diagram NEN-EN-ISO/IEC17065


Application for certification of product or service (§ 3.3)
Handling of applications (§ 4.3)
Initial assessment (§ 4.4.1, § 4.4.2)
Reporting, assessment and decision (§ 4.4.3)
Negative
Product certificate/ Service certificate (§ 5.2)
Decision (§ 4.4.3)
www.hetccv.nl/certified/pen-test (§ 4.4.4)
Product certificate/ Service certificate continued
Positive
Periodic assessment (§ 4.5.1, § 4.5.2)
Additional review (§ 4.6)
A*
Reporting (§ 4.5.3)
No
Devations? (§ 4.8)
Major
Action plan (§ 4.8.3)
Minor
Corrections and corrective measures (§ 4.8.3, § 4.8.7)
Yes
Adequate action plan submitted on time
No
Assessment by certification body (§ 4.8.4, § 4.8.8)
Reporting, review and decision (§ 4.5.3)
No
Suspension (§ 4.9)
Reporting (§ 4.5.3)
Yes
Timely elimations of deviations
Corrections and corrective measures (§ 4.9.3, § 4.8.3, § 4.8.7)
Rating by certification body (§ 4.9.3, § 4.8.4, § 4.8.8)
Reporting, review and decision (§ 4.5.3)
A*
Withdrawal (§ 4.10)
Reporting, review and decision (§ 4.5.3)
No
Timely elimination of deviations
Yes

4.3 Handling of applications

The certification body considers each application and checks whether all details are complete and correct at the time of application.

The certification body handles the application of a certificate holder with a certification agreement with another certification body in accordance with the '*CCV-reglement beoordelen overstappende certificaathouder*' (CCV Regulations for Assessing Switching Certificate Holders).

The certification body requests additional data that are necessary to process the application and to draw up a budget and planning, such as:

- data requested in section 3.3.1;
- data requested in section 3.3.4;
- description of how the quality system has been set up;
- data that may lead to a reduction in the scope and depth of the initial assessment, such as other certificates present and available assessment reports. The certification body assesses the extent to which existing reports and certificates can be used;
- data for the correct assessment of a service provider with several branches. A service provider with several branches can be assessed in two ways:
    - each branch is considered a separate service provider with one service certificate per branch.
    - as a single service provider with multiple sites/branches. This is one service provider with one certification contract and one service certificate (multi-site assessment). The conditions for multi-site certification are:
        - the service provider has a head office and decentralised locations that all apply the same quality system managed from the head office;
        - the decentralised locations are managed hierarchically from the head office (it is not necessary for all locations to fall under the same legal entity);
        - the processes at all sites are substantially similar and the same methods and procedures are applied;
        - the head office handles complaints (see section 3.2.8);
        - Headquarters shall ensure that corrective measures (see section 3.2.9) are also implemented at all decentralised locations, where applicable;
        - headquarters also involves the decentralised sites in carrying out evaluations (see section 3.2.10).
- possible suspension (see section 4.9) or withdrawal (see section 4.10).

Based on the documented application for certification, the certification body draws up a budget and planning for carrying out the initial assessment and for performing periodic assessments.

The certification body uses the provisions in sections 4.4.2 and 4.5.2 for this. The calculated times are exclusive of travel and reporting time and exclusive of the time required for the assessment of shortcomings.

Variables in the calculation may include the organisational form of the service provider, the number of employees, geographical spread, variations in projects.

The budget shall be laid down and approved, including its substantiation.

The certification body informs the service provider about at least:

- an estimate of costs and time;
- the requirements and conditions of this scheme (including the certification mark regulations);
- whether the quote and following certification concerns one or more sites of the service provider;

- the contractual/regulatory conditions of the certification body itself.

4.4 Initial assessment

4.4.1 Implementation

The initial assessment consists of the following parts:

- Verification of information provided with the application.
- Verification of validity and scope of other certificates.
- Assessment of the implementation of the quality system, see section 3.2 with the topics mentioned therein (audit).
- Assessment of compliance with the conditions of the certification scheme, including use of the certification mark.
- Assessment of the primary processes.
- Assessment of technical provisions (if applicable).
- Assessment of the delivered/to be delivered pen test against the requirements formulated in section 2.2).
- Assessment of corrective measures and their demonstrability (if applicable).

4.4.2 Time spent and sample

A. INITIAL ASSESSMENT AUDIT	
Quality system assessment	The certification body makes, based on the available data, an audit plan(s) and an audit programme for all elements of the quality system mentioned in section 3.2. Preparation time 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 that justifies 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 pen tests, a large number of personnel is involved, the organization is complex and/or the way the quality system is organized makes the assessment more time-consuming. No maximum applies here. Full reporting (on quality system + service-oriented control[7]) takes 4 hours. At the end of the audit, 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 shall provide a fully documented foundation for the audit planning, the audit programme, the time expenditure and the

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

	adjustments to this for the purpose of harmonisation investigation by the CCV.

B INITIAL ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)	
Technical facilities	The use of tooling will be assessed during the service-specific assessment.
Evaluation pen test	The implementation of pen testing is evaluated against all requirements from the relevant section in chapter 2. Assessment of the pen test consists of: ■ assessing at least two different project files, to be selected by the certification body. Including verification of the report; ■ monitoring the implementation of the pen test and assessing whether it is carried out in accordance with chapter 2, possibly requesting clarification and explanation. In case of multi-site assessment, this applies to the main site. Per additional branch, one project is selected for file review and a pen test is assessed while it is executed. 2 hours are assumed for each pen test file to be examined. For assessing during (a) pen test(s) in progress, a total of 4 hours is assumed. For monitoring the implementation of pen tests the following principles apply: 1. The certification body asks one or two pen testers / employees of the service provider about the process followed in two pen test projects. 2. The certification body is present during the implementation of at least one project. Attendance at one or more parts of the performance of the pen test(s) is sufficient. 3. The project executed while the certification body is present may be a different project than the two projects of which the files including the pen test reports are assessed. 4. When asking questions about the two projects whose file is being assessed and/or the project in which the certification body is present, attention can be paid to the following subjects. These topics can be supplemented or replaced by other relevant topics at the discretion of the certification body. ■ What was the input /assignment/briefing/scope? ■ How is the team composed and who is in charge? ■ What are the do's and don'ts regarding the pen test? ■ What choices were subsequently made? ■ Which tooling is/will be used? ■ What manual interpretations have been performed? ■ Where are the reports located? ■ Who checked this? ■ How is the customer involved in the process? ■ How did the final report come about? ■ How was the project completed? ■ How has been ensured that no artifacts / remnants of the pen tests have been left behind?

	- Has there been a final review?
File	The project file of the projects assessed (see above) is reviewed to provide a complete and representative picture of the entire process (available starting information, consent of all owners of systems in scope, test plan, procedures, documentation).

4.4.3 Reporting, assessment and decision-making

Each initial assessment shall be accompanied by a report containing all findings on the points listed in section 4.4.1.

The certification body reviews the report for at least the completeness of the assessment, the execution by qualified certifying staff and a correct process flow.

Based on this review, the certification body makes a written recommendation for decision-making by the certification body. All non-conformities found during the initial assessment must be demonstrably removed before the certification body can take a positive decision.

4.4.4 Publication

After a positive decision, the certification body publishes the details of the service provider for the relevant certification scheme on www.hetccv.nl/certified/pen-test. This website is owned and managed by the CCV.

4.5 Periodic assessment

4.5.1 Implementation

The periodic assessment consists of the following components:

- Assessment of effective implementation of the quality system, see section 3.2 with the topics listed therein (audit);
- assessment of continued compliance with the conditions of this certification scheme, including use of the certification mark;
- Assessment of primary processes;
- assessment of technical provisions (if any);
- Assessment of the delivered/to be delivered pen test against the requirements as formulated in section 2.2;
- Assessment of corrective action and its demonstrability (if applicable).

4.5.2 Frequency, time spent and sample

The periodic assessment is carried out at least once a year.

Audits can be combined, but also performed separately. The sample should preferably be spread over the entire period until the next periodic audit.

A. PERIODIC ASSESSMENT – AUDIT	
Quality system assessment	The certification body carries out the audit in accordance with the audit plan(s) and audit programme drawn up and updated, see section 4.4.2. 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 carries out many pen tests, 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[8]) takes 4 hours. At the end of the audit, 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 the harmonisation investigation by the CCV.

B. PERIODIC ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)	
Technical facilities	The use of tooling is assessed during the service-specific assessment.
Evaluation pen test	The implementation of pen testing is evaluated against all requirements from the relevant section in chapter 2. Assessment of the pen test consists of: ▪ assessing project files, number of checks according to the table below, to be selected by the certification body. Including verification of the report; ▪ monitoring the implementation of the pen test and assessing whether it is carried out in accordance with chapter 2, possibly requesting clarification and explanation. 2 hours are assumed for each pen test file to be examined. For assessing during (a) pen test(s) in progress, a total of 4 hours is assumed. Deliveries of pen test in a 12-month period are checked by the certification body according to the table below:

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

NUMBER OF PEN TEST	NUMBER OF CHECKS
0	–[9]
1	1
2	2
3 to 50	3
51 to 100	5
101 to 150	7
151 to 300	9
301 to 500	11
501 and more	13

The service provider provides a list of all executed pen test projects. The certification body determines the sample.

At least 95% of the executed pen tests must be transparent and accessible to the certification body. Projects that are strictly confidential can be excluded from the certification mark and from assessment by the certification body. If this applies, the service provider must explain the sensitive nature of these projects to the auditor from the certification body. It is at the discretion of the certification body at what level of detail to document this conversation.

The sample will be divided as much as possible (spread over types of pen tests, pen testers, customers, but can also extended, if this is necessary for the representative picture. The checks shall, preferably and where possible, be spread over the year, so that a representative picture emerges with regard to the quality of the pen tests provided.

In case of multi-site assessment, the total sample size is determined based on the number of pen tests delivered by the entire organisation. The certification body ensures that every site is part of the selection of projects.

For monitoring the implementation of pen tests the following principles apply:

1. The certification body asks one or two pen testers / employees of the service provider about the process followed in two pen test projects.
2. The certification body is present during the implementation of at least one project. Attendance at one or more parts of the performance of the pen test(s) is sufficient.
3. The project executed while the certification body is present may be a different project than the two projects of which the files including the pen test reports are assessed.
4. When asking questions about the two projects whose file is being assessed and/or the project in which the certification body is present, attention can be paid to the following subjects. These topics can be supplemented or replaced by other relevant topics / at the discretion of the certification body.

   - What was the input /assignment/briefing/scope?
   - How is the team composed and who is in charge?
   - What are the do's and don'ts regarding the pen test?
   - What choices were subsequently made?

	- Which tooling is/will be used? - What manual interpretations have been performed? - Where are the reports located? - Who checked this? - How is the customer involved in this process? - How did the final report come about? - How was the project completed? - How has it been ensured that no artifacts / remnants of the pen tests have been left behind? - Has there been a final review?
File (during audit)	The project file of the reviewed pen tests (see above) is reviewed, so that a representative picture of the entire process is obtained (available starting information, consent of all owners of systems in scope, test plan, procedures, documentation). The service provider may deviate from the retention period (see section 3.2.6) at the explicit request of the customer. The service provider must immediately inform the certification body about this, so that the certification body is enabled to carry out an interim audit of this pen test if desired.

4.5.3 Reporting, assessment and decision-making

The report of a periodical assessment or an additional assessment should contain all findings of the assessment, including the assessment of corrective actions for identified deficiencies. If the deficiencies are resolved within the time limits specified for this purpose, the report must contain a positive conclusion on the conformity found so that the certified status can be maintained without any decision being taken.

If shortcomings are not remedied within the time limits set for this, an interim report is drawn up, which includes advice for suspension of (part) of the scope.

The report with the recommendation for suspension is assessed for, among other things, completeness of the assessment, execution by qualified certifying staff and correct process execution.

4.6 Additional review

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 service to which the certification mark has been applied 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.

[9] If less than one pen test 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 certified pen tests according to this certification scheme for two consecutive years, the certification body must suspend the certificate.

Implementation, reporting, review, decision making and possible sanctions are subject to the same provisions as for the periodic assessment.

4.7 Reduction of time spent on other certificates

Not applicable, see table A in section 4.4.2 respectively section 4.5.2.

4.8 Deviations

A situation which is not in accordance with the requirements is considered as a deviation. Deviations may relate to the pen test delivered under certificate and/or to the quality system. Deviations can be classified as major or minor.

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

In the case of a service provider with multiple sites who opts for multi-site assessment (see section 4.3), deviations and their consequences concern the entire organisation of the service provider.

4.8.1 Major - Quality System

- One or more requirements from the certification scheme have not been implemented, or there is a situation that, based on objective observations, raises significant doubt as to whether the quality system provides sufficient support for the service provider to deliver the pen tests 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.

4.8.2 Major – Service

The pen test supplied under certificate does not meet the requirements set, because of which:

- dangerous or unsafe situations (may) arise, or
- the digital system on which the pen test was carried out does not function or no longer functions, or malfunctions/situations have arisen which increase the risk of vulnerabilities.

4.8.3 Major – Consequences

In the event of major deviations, the service provider shall present an action plan within a period to be determined by the certification body, not exceeding seven working days.

Errors made shall be 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 shall in any case (but not be limited to) include the possible causes in the process of producing the pen test and the possible causes in the failure of control processes;
- the actions to be taken immediately to prevent further non-compliant pen tests from being delivered with the certification mark;
- An analysis focused on the pen test delivered since the last assessment by the certification body that may not meet the set requirements and on the extent to which the root causes analysed have led to (previously) identified nonconformities;
- actions to be taken to repair or remedy any delivered pen tests that do not meet the requirements;
- solutions aimed at preventing recurrence and securing them;

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

The service provider shall fully document 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 shall be at most three months.

4.8.4 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.

The certification body assesses the implementation of the corrections and the implementation of the corrective measures within four months after the nonconformity has been established[10], to establish that the nonconformity has been removed. The manner of assessment depends on the nature of the nonconformities and is based on the elements mentioned in section 4.5.1. If necessary, an additional assessment is carried out for verification.

The certification body may extend the period for corrections and corrective actions once, with substantiation, by a period of three months.

4.8.5 Minor - Quality System

- A situation which, based on objective observations, raises doubts about the quality assurance of the pen test supplied under certificate, or
- 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 nonconformity, 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).

4.8.6 Minor – Service

- The pen test delivered under certificate does not meet the set requirements, which has not resulted in a major deviation, or
- A situation which, based on objective observations, casts doubt on the quality of the pen test delivered under certificate.

4.8.7 Minor – Consequences

The service provider shall be given a period of three 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 shall in any case (but not be limited to) include the possible causes in the process of producing the pen test and the possible causes in the failure of control processes;
- An analysis focused on the scope of pen test delivered since the last assessment by the certification body that may not comply with the set requirements, and the extent to which the root causes analysed have led to (previously) identified nonconformities;
- action to be taken in order to repair and/or remedy all delivered pen tests that do not meet the requirements;
- solutions aimed at preventing recurrence and securing them;

[10] This three-month period is the same for major deviations as for minor deviations (see section 4.8.6). If there is a suspension, it is recommended that the assessment not be carried out at the same time but split up so that the suspension can be lifted as soon as possible.

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

The service provider shall fully document the corrective actions to be implemented, so that they are verifiable by the certification body.

4.8.8 Minor - Assessment by the certification body

In order to ascertain that the nonconformity has been rectified, the certification body assesses the implementation of the corrections and the implementation of the corrective measures within four months of establishing the nonconformity. The method of assessment depends on the nature of the nonconformities and is based on the elements mentioned in section 4.5.1. If necessary, an additional assessment shall be carried out for verification.

The certification body may extend the period for corrections and corrective actions once, with substantiation, by a period of three months.

4.9 Suspension

4.9.1 Suspension

The service provider is suspended:

- when failing to provide a plan of action on time when determining a major deviation (see section 4.8.3), 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 4.8.3 and 4.8.7), or;
- if the corrective actions for both major and minor deviations have not led to the elimination of the deviation(s) within the set (extended) timeframe (see sections 4.8.3 and 4.8.7), 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 service provider has not provided pen tests over a period of up to three years, or;
- if the service provider damages the interests and image of the certification scheme, the certification body and/or the CCV.

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

The certification body shall inform the service provider of the suspension by registered letter or by e-mail with confirmation of receipt.

4.9.2 Consequences of suspension

The certification body publishes the suspension on www.hetccv.nl/certified/pen-test. From the moment of suspension, the service provider may not use the certification mark. Nor may the service provider refer to the certified status of the pen test to be delivered. The service provider remains responsible for remedying defects in the pen test to which the certification mark has been applied.

4.9.3 Lifting the suspension

If the certification body establishes that all nonconformities have been removed, the suspension shall be lifted. The certification body shall inform the service provider in writing of this and shall cancel 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.

4.10 Withdrawal

4.10.1 Withdrawal

The certificate shall be revoked if the service provider is unable to remedy the nonconformities found within the period of suspension.

The certification body shall inform the service provider of the withdrawal by registered letter or by e-mail with acknowledgement of receipt.

4.10.2 Consequences of withdrawal

From the moment of withdrawal the service provider may not use the certification mark or refer to the certified status of the pen test to be delivered. The certification body removes the data of the service provider from the certification scheme concerned on www.hetccv.nl/certified/pen-test.

The service provider remains responsible for remedying defects in the pen test in which the certification mark was applied. The certification body has the authority - if the service provider is negligent in this - to take corrective measures, such as informing clients. The costs of this may be charged to the service provider whose service certificate has been withdrawn.

4.10.3 New application

A service provider whose certificate has been revoked may again apply for an initial assessment in accordance with the certification scheme (see section 4.4).

5. Certificate and certification mark

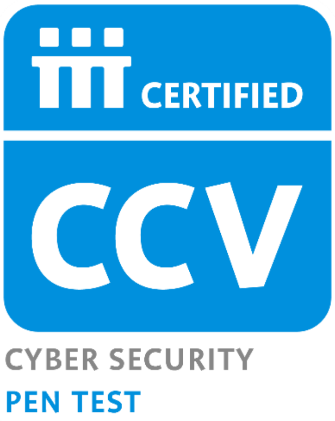
5.1 Certification mark

The certification mark, further called ‘the mark’, is the proof for buyers that the certification body has a justified confidence that the service provider who delivers a pen test complies with the requirements set in the certification scheme (as described in chapter 2) 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 mark shown below is associated with this certification scheme.



The certification mark affixed to the pen test report indicates legitimate confidence in the quality of the pen test.

5.1.2 Use of the mark

The main conditions for the use of the certification mark are:

- The certification body has a valid license with the CCV.
- The service provider has a valid certification contract and has not been suspended.
- The service provider has ascertained that the service meets the requirements set.

Illustrative use on letterheads, website, folders and other publicity material with references to the certification scheme by the certification body is permitted under certain conditions.

The service provider shall place the mark on the final test report, see section 5.3. The use of the mark is mandatory. In addition to this paragraph, for use of the certification mark the regulations stated in ‘*CCV Reglement Kwaliteitslogo’* apply. This document is published on the CCV website: www.hetccv.nl.

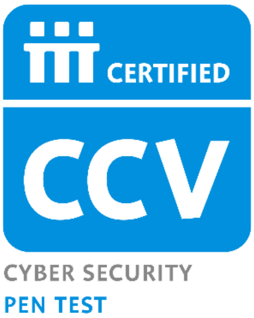
5.2 Service certificate

The certification body provides a service certificate to the service provider. This service certificate shall be drawn up in the house style of the certification body. The service provider may advertise itself as "Registered to provide certified pen tests".

The service certificate contains at least the following data:

- Name and address of the certification body;
- name and address of the certificate holder (correspondence address);
- the texts and certification mark

> *"<Certification body> declares that, based on the assessments by <Certification body>, confidence is justified that the pen test carried out by the service provider, including the pen test report, complies with the requirements set out in the CCV certification scheme – Cyber Security - Pen Test, version 2.0>."*
>
> *"<Certification body> licenses the certification mark shown here to <the service provider> for the pen test delivered under the certification scheme."*



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

> *"Pen testers and third parties can check the status of a valid service certificate with <certification body> or on <reference to www.hetccv.nl/pentest> "*
>
> *"This certificate remains the property of <certification body>."*

5.3 Test report with certification mark

The service provider provides a test report with the certification mark, upon delivery of the pen test.

The service provider shall place the mark on the definitive version of the test report for the client. The layout of the document is such that it is clear that it concerns a test report - pen testing. The report explicitly states that the certification mark is about the quality of the pen test and not that of the tested object or environment.

The service provider is not allowed to place the mark of the certification body on the test report.

6. References

6.1 Terms and abbreviations

Assessment	Implementation of this certification scheme by the certification body at the service provider of the pen test.
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
CCV	Centrum voor Criminaliteitspreventie en Veiligheid (Centre for Crime Prevention and Safety)
Certificate	Document prepared by the service provider containing a statement regarding the pen testing 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.
Customer	Person or organisation that purchases the pen test and orders the service provider to carry out the pen test.
Initial assessment	Assessment leading to a decision on certification and, in the event of a positive decision, issue of the service 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.
Pen test*	A manual check that seeks to penetrate as deeply as possible into a system to find weaknesses and know the consequences. One uses the weaknesses to get a little deeper into the system. The goal of the test is not to find as many vulnerabilities as possible. That does happen with a vulnerability scan.
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.
Service certificate	Document prepared by the certification body, listing the service provider as the supplier of the certified pen test.
Service-oriented assessment	Assessment of the pen test by the certification body, including the test report.
Service provider	The organisation providing the pen test or vulnerability assessment.
Tooling	Tooling is a term used for utilities that make certain actions easier for a user or take over completely. It is an aid, a tool. Tooling is not leading in the execution of a pen test.
VOG	Verklaring Omtrent Gedrag, Certificate of Conduct.

Vulnerability assessment*	The vulnerability assessment is a manual check to find weak spots in a system. It is determined in advance how this is done. With a vulnerability assessment, one tries to find all weak spots in a small area. This is different from a penetration test where one tries to get as deep as possible into a system.
Vulnerability scan*	An automated check that detects weaknesses in a system. Only if it is a false alarm, it is removed manually.

* Source: Cybersecurity Dictionary, Cyberveilig Nederland

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 shall apply as indicated herein. A certification body possesses all normative standards and documents. The service provider shall have at his disposal at least those standards and documents marked with an *.

STANDARD	TOPIC	AVAILABLE
NEN-EN ISO/IEC 17065	Conformity assessment - Requirements for certification bodies awarding certificates to products, processes and services	NEN, Delft
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
	Rules CCV certification mark: *CCV Reglement Kwaliteitslogo* *	CCV, Utrecht

CCV centrum voor criminaliteitspreventie en veiligheid

(Centre for Crime Prevention and Safety)

Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht
T +31 (0)30 751 6700
E info@hetccv.nl
I www.hetccv.nl