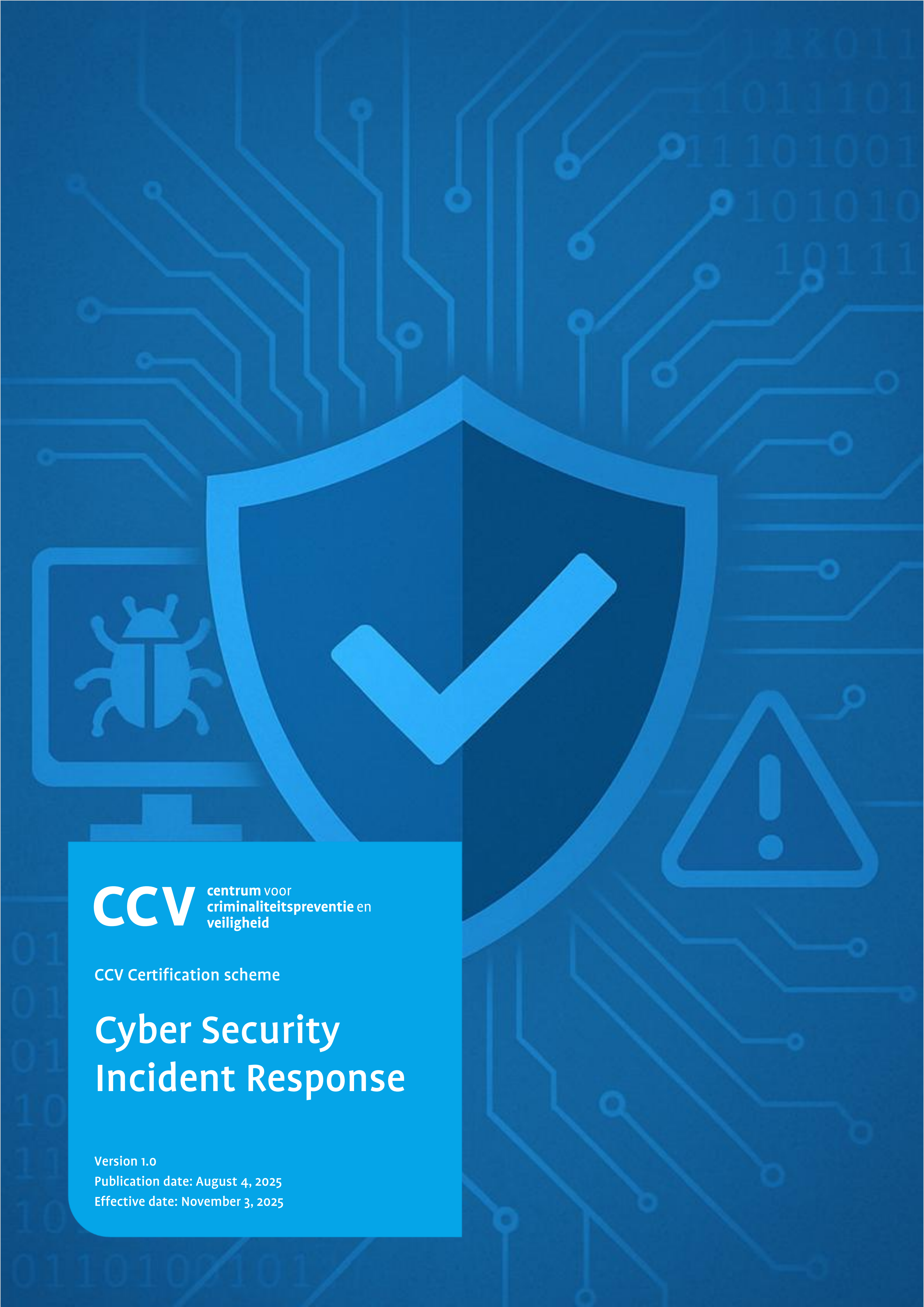


CCV centrum voor criminaliteitspreventie en veiligheid

CCV Certification scheme

Cyber Security Incident Response

Version 1.0
Publication date: August 4, 2025
Effective date: November 3, 2025

Foreword

This certification scheme is aimed at the certification of incident response services according to NEN-EN-ISO/IEC 17065.

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

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

1.1 General

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 an organisation 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. These security controls consist of a combination of technical, organisational and behavioural measures. An organisation that wants to protect itself against cybercrime needs this to be done properly, with safe products and installed or carried out by a professional. And in spite of these measures an organisation can still fall victim to cybercrime. When a cyber security incident does occur, the organisation needs a viable plan, process and capacity for appropriate incident response.

All of this can be difficult for an organisation to assess properly on its own. Certification schemes for cyber security services offer a good solution for this purpose. This applies first of all to preventative cyber security measures. But in case of an incident, an organisation can also require external assistance. This certification scheme focuses on incident response (IR).

1.1.1 Purpose

The service incident response is a structured response to a cyber security incident. It is an approach at various levels: operational, tactical and strategic. Incident Response can be seen as a kind of fire brigade that immediately takes action when something happens. An incident is defined as an event or action in which the security of hardware, software, information, a process or organisation may have been compromised or may have been (partly) breached. This can lead to serious threats to the organisation's primary processes and/or to its continuity. It can also lead to threats to the interests of third parties (individuals or organisations) with ties to the organisation where the incident takes place. Because of the possible consequences of an incident, incident response requires both urgency and capacity. Therefore, the incident response service must be carried out professionally. Government and private parties have a need for guaranteed quality of incident response. This assurance is possible with service certification of incident response.

The aim of the certification of the service is to reduce the costs of failure and risks for customers that may occur when the supposed quality of the service incident response is not up to an industry recognised standard. Certification allows clients to have legitimate confidence that the supplied service, 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 incident response and to describe the implementation of certification. This should lead to harmonised implementation. An additional goal is informing the market how certification of incident response is organised and carried out.

1.1.2 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. When a cyber security incident occurs, the organisation is responsible for an adequate response. An option to meet that responsibility is hiring an incident response party. In this certification scheme, the party requiring the service of incident response is referred to as "the client". When hiring an incident response party, the client is responsible for providing the incident responder with the required information and access.

The organisation providing the service incident response - hereafter referred to as "the service provider" - is responsible for compliance with the certification scheme. It ensures that the incident response service to which the certification mark is applied (see section 5.1) meets all applicable requirements.

1.1.3 Reading guide

The certification scheme contains:

- requirements to be met by the service incident response and how this is assessed (chapter 2);
- conditions for the service provider to obtain and maintain the service certificate (chapter 3);
- harmonised methods and standards 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, as well as guidance on the correct use of the certification mark in reports issued by the service provider to the client (chapter 5).

1.2 Scope

The scope of the certification scheme is the execution of the service incident response, including reporting to the client.

This certification scheme has two sub-scopes: ‘Incident Response - 24/7’ and ‘Incident Response’.

Most of the criteria in this certification scheme apply to both sub-scopes. The sub-scope ‘Incident Response – 24/7’ includes one additional requirement: the service provider is continuously available (24/7), not only for existing clients (under retainer) but also for ad hoc clients. In other words, the provider is accessible for organisations that are facing a (potential) incident and do not yet have a contractual relationship. See paragraph 2.2.1 for details.

The rest of this paragraph applies to both sub-scopes.

A service provider can deliver incident response under certification and thus the certification mark. When a service provider delivers incident response under this certification scheme, all of his incident response services are delivered in accordance with the criteria in this scheme, fall under supervision of the certification body and are delivered with the CCV certification mark. This service consists of the following elements:

1. Incident Analysis
The thorough examination and assessment of security incidents to determine their nature, extent, and impact on the organisation's systems, networks, and data.

2. Incident Coordination (breach role)
A cyber security incident can lead to a broader crisis for a client. Therefore, if a service provider delivers incident response under this certification scheme, it is also required to inform the client about possible needed additional actions, for instance in communication and/or regarding legal aspects. This can lead to a client’s decision to attract external expertise in these domains. The service provider can also advise to use services of specific service providers. However, delivery of services in communication and legal matters is out of scope of this certification schema.

Prior or during the execution of elements mentioned in this paragraph, the service provider pays attention to the possibility of (future) forensic investigation. This includes taking the following steps:

(1) The service provider discusses the need for, or usefulness of, forensic investigation with the client, and

(2) Prior to the execution of steps required for incident response, the service provider
a. makes an explicit analysis of consequences for data that can be relevant as forensic evidence,
b. includes the client in relevant decision making and
c. makes copies of data relevant for forensic investigation, respecting the required chain of custody.

3. Incident Containment
The swift and decisive actions taken to prevent the further spread or escalation of a security incident, including (but not limited to) isolation of affected systems, network segmentation, and implementation of access controls.

4. Incident Eradication and Preventing Reoccurrence
The systematic removal of the root causes of security incidents, such as malware, points vulnerable to unauthorised access and other system vulnerabilities, to eliminate the risk of reoccurrence. The service provider also advises the client with the goal of preventing similar incidents in the future.

5. Recovery
The restoration of affected systems, applications and data to a secure and operational state following a security incident. In doing so, backups, system patches, data recovery procedures, and other recovery mechanisms are utilised.

6. Post-Incident Analysis and Report
The review and analysis of incident response actions taken.

Relation to forensic investigation
This certification scheme does not entail full forensic investigation execution or capabilities. For elements in scope, see under “incident coordination” above. For details, see chapter 2.

Relation to communication
Providing the service of in- or external (crisis) communication is out of scope. What is in scope however is (1) advising the client about taking communication actions and if necessary hiring an external party (see under “incident coordination” above), and (2) providing the client with information about the incident and the executed response, in a useful form and abstraction level, as input for in- or external communication.

Relation to legal advice
Providing legal services is out of scope. The incident response service provider is required to advise clients about the option of using legal services. (See under “incident coordination” above.)

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

For specific cases that are exempt from the ‘all incident response under certification’ rule, and the conditions under which such exceptions apply, see section 4.5.2.

In principle, incident response under these scheme can be provided by a provider that also provides cyber security monitoring services. Because of the required impartiality, the service provider for incident response cannot be a provider of the client’s infrastructure, general IT services or software.

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

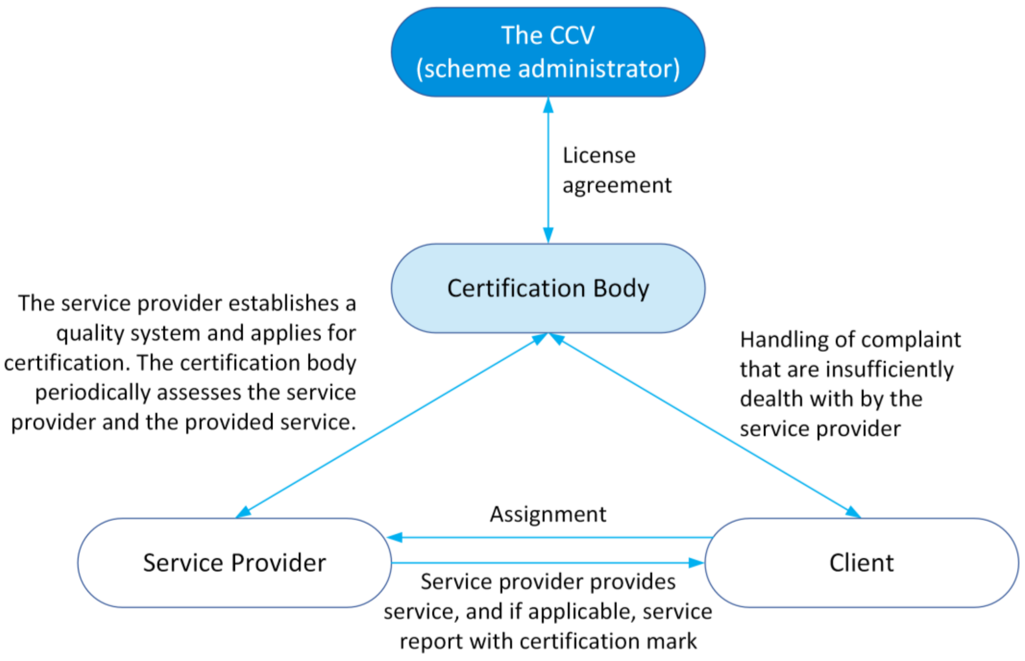

The CCV
(scheme administrator)
License
agreement
Certification Body
The service provider establishes a quality system and applies for certification. The certification body periodically assesses the service provider and the provided service.
Handling of complaint that are insufficiently dealth with by the service provider
Assignment
Service Provider
Client
Service provider provides service, and if applicable, service report with certification mark

Figure 1 - Overview of parties involved in service certification

1.5 Transitional provisions

This is version 1.0 of this certification scheme; no transitional provisions are required.

2 Service requirements

In service certification, the core focus lies on the defined requirements that the certified service must meet.

2.1 General

This chapter outlines all technical and administrative requirements that the certified incident response service must meet, as well as how compliance with these requirements is assessed. Failure to meet the requirements set out in this chapter results in 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 **Notes** ■ Assessment A1 and A2 can only be carried out if the documents are present ■ This method may require access to information from the service provider's systems.
(I) Interviews	Interviews, formal and/or informal[1], relating to the service and/or the quality system. **Note** ■ This method can be used by the certification body, in addition to the methods mentioned below, at the discretion of the certification body.

[1] The distinction in formal and informal interviews refers to different levels of formal structure these conversations with personnel of the service provider can have. In all cases it is clear that the conservations are part of the assessment by the certification body, and the certification body registers its preliminary findings.

2.2.1 General requirements

TABLE 2B - GENERAL REQUIREMENTS

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Response time	- The service provider is transparent towards (potential) clients how to reach him (for instance: by phone or e-mail) in urgent cases. - (Potential) client receives confirmation (by e-mail or phone and then confirmed by e-mail). This is within 30 minutes of receipt by the service provider of the first notification from the (potential) client. This confirmation includes a statement that triage can start within 2 hours from the moment the confirmation was given. - If confirmed by client, triage is in fact started within that timeframe. Timely execution is documented. - If a service provider at the moment of the incident does not have the required capacity available to start triage, it informs the party seeking assistance directly or as soon as possible, with a maximum of the above mentioned 30 minutes.	A2
Accessibility	Regarding the assessment aspect of response time (see above) all requirements are met not only for clients under retainer but also for new /ad hoc (potential) clients: - By all service providers working under this scheme during office hours, that is at least during weekdays (Monday to Friday), from 8:00 to 17:00 CET. - By service providers with the sub-scope “24/7”: all day, every day of the week.	A2

2.2.2 Incident Analysis (including intake)

TABLE 2C - INCIDENT ANALYSIS

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Transparency/ independence	Check on potential conflicts of interest, for instance in regard to other clients or business partners. Examples of potential conflicts of interest: - Providing support to a managed service provider during an incident affecting their hosting provider, while also being engaged by that same hosting provider to assist with investigation and recovery for the same incident. - A consultancy firm providing incident response to a company for which the consultancy firm is also the accountant.	A1

TABLE 2C - INCIDENT ANALYSIS

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Triage - Analysis	■ Analysis is based on understanding both of the client's systems and his business. Therefore, the service providers asks the client to provide input and documents aspects relevant for the analysis. ■ The analysis makes a clear distinction between: – in- and external impact – certain, likely and possible impact	A2
Triage – recommended follow up	Recommended follow up is proportional, in relation to solving the incident and possibly preventing comparable future incidents.	A2
Triage – Relevant regulatory frameworks	■ The service provider asks client about specific legal requirements that apply to the client and may be relevant in regard to the incident response service. ■ The service provider takes this input into account in its analysis and, if relevant, the further execution of the incident response.	A1
Report	A final report, with a written summary of the execution of the entire incident response, is a basic part of the service incident response. However, exceptional circumstances can arise in which a client does not want to receive a final report. In those specific cases, this is properly motivated by the client and documented by the service provider.	A2
Summary of root cause analysis	Summary of root cause analysis. Including limitations of applied method/available data.	A1

2.2.3 Incident coordination (breach role)

TABLE 2D - INCIDENT COORDINATION

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Designated employee	One person is active as coordinator for an incident; service provider makes clear to client who this is at the start of an incident. (Depending on context and intensity of the incident, the coordinator can have a substitute, about whom the client is informed.)	A1
Integrated role	■ A coordinator leads the intake process, and oversees it through to the resolution of the incident. ■ The coordinator explicitly plays a role in triage, making sure that an understanding of the client's business and systems is used to properly weigh the findings during triage.	A2

TABLE 2D - INCIDENT COORDINATION

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
	▪ If the role of coordinator is transferred to someone else, this is documented. ▪ At any given time, the client is informed about who is acting as coordinator.	
Monitoring development	The coordinator oversees the development of the incident and required measures. The coordinator adapts measures as needed, consistently applying awareness of the incident in its specific context.	A2
Information and advice	The coordinator keeps the client informed during the incident and advises on required actions by the client.	A2
Client-authorised changes	If the service provider makes substantial changes to the client's systems or data, or shuts down applications or systems, authorisation by the client is made explicit and is documented.	A2
Deciding on saving potentially relevant data / configurations	Prior to changes, an explicit choice is made, in agreement with the client, about whether or not to make copies of data and or configurations. This includes considering a need for forensic investigation at the later time.	A2
Threat actor communication	In some cases, threat actor communication is required as part of incident response. In such cases three options are available for the service provider under certification: ▪ The service provider's personnel provide this part of the service. (The service provider sees to it that relevant qualifications are set and upheld, see chapter 3.) ▪ This part of the service is outsourced by the service provider (see chapter 3). ▪ The service provider brings the client in contact with a reliable business partner, that can provide this service under an assignment directly from the client. ▪ If the situation requires it, the service provider offers at least one of those options to his client.	A2

2.2.4 Incident Containment

TABLE 2E - INCIDENT CONTAINMENT

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Deciding on continuous monitoring during incident	The service provider makes an informed decision on whether or not to apply real-time monitoring of relevant events during the incident. If required, the client is informed about this and the reasons behind it.	A2

TABLE 2E - INCIDENT CONTAINMENT

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Performing continuous monitoring during incident	If applicable, the service provider can deliver adequate monitoring services during the incident and can demonstrate the use of proficient tools.	A2
Advising on isolation	The service provider advises on isolation, also considering business operation interests.	A1
Performing isolation	The service provider has the capabilities to isolate (parts of) systems. Executing isolation is done by the service provider, if requested by the client. **Notes** 1 Performing isolation can be executed by the client himself, a third party as preferred by the client, or by the service provider (incident responder). 2 If the service provider is requested to perform isolation, this can be provided only if the client, or a third party assigned by the client, provides proper additional authorisation and information to the service provider. 3 The need for authorisation provided by the client is addressed in the contract, both for retainer and ad hoc clients. 4 Especially for ad hoc clients, timely isolation by the service provider can be hampered by the required step of providing authorisation, especially if third parties are required for this step.	A2

2.2.5 Incident Eradication and Preventing Reoccurrence

TABLE 2F - INCIDENT ERADICATION AND PREVENTING REOCCURRENCE

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Removal of malicious elements	■ Malicious elements are removed from all known affected systems. This includes systems that are/will be restored from backups. This is done by the service provider, by the client or a third party as preferred by the client. ■ A test is done to check if all is removed. Automated tooling can be applied for this. In case this test is not executed by the service provider, the service provider has insight in both the method and the test results. Based on this, the service provider is able to give its expert opinion on whether or not the environment is deemed 'safe' or 'clean'.	A1
Preventing misuse and unauthorized access	The service provider identifies actions required to prevent abuse of compromised elements such as credentials and certificates.	A2

TABLE 2F - INCIDENT ERADICATION AND PREVENTING REOCCURRENCE

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
	The service provider executes these actions on behalf of the client or advises the client to take these actions.	
Preventing reoccurrence	The service provider advises the client with the goal of preventing a similar incident in the future. The service provider executes these actions on behalf of the client or advises the client to take these actions. The advice is documented.	A2

2.2.6 Recovery

TABLE 2G - RECOVERY

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Prioritised asset list	■ The service provider helps set up a prioritised asset list that translates the business priorities to the specific applications and systems needed to for this. The service provider helps maintain this list and ensures the list is adjusted when priorities change. ■ Confirmation by both parties of this list is documented.	A1

In some cases, the client may opt to perform the recovery themselves or delegate it to a preferred (contracted) third party. This is acceptable within this certification scheme if this point is made explicit in the agreement with the client, along with the required division of work and responsibilities between the client and the service provider.

2.2.7 Post-Incident Analysis and Final report

TABLE 2H - POST INCIDENT ANALYSIS AND FINAL REPORT

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Language	Report is written in language as agreed with client (English or Dutch).	A2
Root cause	■ A summary of the root cause analysis is shared with the client. ■ The summary includes limitations of the analysis if applicable.	A2
Recovery strategy and implementation	Description of recovery strategy and implementation; summary of work done in different process steps, to recover and to prevent reoccurrence, as defined in this chapter.	A2

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 is able to continuously demonstrate to the certification body 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. This is regardless of other certifications already obtained such as ISO.

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 continuously securing the quality of incident response executed under certification. The following subsections elaborate on the requirements of the quality system.

3.2.1 Organisation and responsibilities

The service provider has an overview of all employees involved in delivering the service, including those in supporting or indirect roles. Tasks, responsibilities and authority of these employees, as well as their hierarchical relationships, are recorded.

The employees are aware of and apply the quality system, and are informed about changes.

Incident response under this scheme can be provided by a provider that also provides other cyber security services, including monitoring services.

Because of the required impartiality in incident response, the following requires special attention: Has the service provider provided the client with infrastructure, general IT services or software? Or is the service provider part of a larger company that has done so? As part of its quality system, the incident response service provider verifies impartiality prior to accepting new clients or assignments for incident response. If products or services delivered by the same company may come in scope of the incident response, the client is notified about this at the start of the assignment. This is also the case if such possible dependencies become clear to the service provider during the handling of an incident.

3.2.1.1 Working under supervision

Employees who are not (yet) demonstrably qualified, only work under the supervision of qualified employees. When providing the incident response service, a qualified employee can be responsible for a maximum of two non-qualified employees. The qualified employees are ultimately responsible for the execution of the service and the reports delivered and have provided at least 50% of the total time used for the incident response.

3.2.1.2 Continuity

In order to guarantee continuity of operations, the service provider ensures replacement of experts if applicable. External experts not employed by the service provider can 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 doing 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 are deployed for the tasks mentioned. Qualifications are kept up to date and are documented. Annual evaluations are carried out to establish whether or not qualification requirements are met.

The person within the service provider who is responsible for qualification of employees (table 3A) decides on whether personnel is qualified for incident response based on the criteria in this scheme. This includes practical certificates (table 3B and appendix).

TABLE 3A - RESPONSIBLE FOR EMPLOYEE QUALIFICATIONS	
Qualification for person being responsible for employee qualification	Set by the Executive Board
Level	Work and thinking skills at HBO[2] level
Knowledge of and ability to work with	This certification scheme

Incident response teams need a mix of knowledge and skills relating to subareas. This means not all criteria in this scheme and further qualifications as set by the service provider need to be met by every individual team member. It is the service provider's responsibility to describe in its quality system the qualifications needed for teams as a whole, as teams are assigned to clients. The service provider is responsible for seeing to it that that minimum level of qualifications is maintained.

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

TABLE 3B - INCIDENT RESPONSE PROFESSIONAL	
Qualification A:	Set by person responsible for employee qualifications, including at least: *1. For all personnel working on an incident:* Analytical skills Communication skills, both written and oral *2. Additionally, for analysts:* Able to work methodically, structured and focussed. Proper knowledge of and skills in operating systems and networks. *3. Additionally, for coordinator and others with direct contact with clients and client's organisation/personnel:* Understanding the main aspects of technical issues Able to translate between clients' business, IT/OT and cyber security Able to perform under pressure, in a turbulent environment.

[2] HBO: higher education level in the Netherlands; universities of applied sciences.

	4. Additionally, analysts and coordinators have knowledge and skills relating to different subareas. The service provider documents which subareas it considers most important for their incident response service and periodically checks the relevant knowledge and skills of their personnel, recording the results.
Qualification B ; Practical certificate	*For all personnel working on an incident:* Specific qualifications for incident response, as demonstrated with personal certificates. The service provider determines which certificates are relevant, meet the required level and are considered reliable, and can justify these choices for the incident response team(s).
Experience	At least 1 year of experience in ICT services and incident response. Experience as an intern does not qualify.
Knowledge of and ability to work with	This certification scheme. For verbal and textual communication with client (including the report): Dutch language on level C1 and/or English language on level C1.[3]
Maintaining qualification	According to the service provider's training and evaluation plan

Note
Qualifications A and B assume incident response with teams consisting of a coordinator and one or more analysts. If on smaller incidents only one person is designated, this requires:
The service provider to register this choice, including a short motivation, in the project files/its internal administration.
The service provider needs to make sure that the one person designated meets the above mentioned qualification requirements for both roles; analyst and coordinator.

All employees involved in the incident response process and/or who have access to information concerning the service (permanent staff or external contractors) 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 is not older than three years. In case of personnel not based or registered in the Netherlands, other comparable national certificates or declarations by or on behalf of a national government can apply. Whether these are acceptable is at the discretion of the certification body.

3.2.3 Measuring means and equipment

The service provider can provide an overview of tooling that is deployed in the context of delivering incident response under certification. The service provider declares that all tooling used is acquired and used in a legal manner and that it has licenses for all commercial software used. In case of doubt the service provider can provide the certification body with evidence.

3.2.4 Outsourcing

The service provider may subcontract work to another incident response service provider. Full outsourcing of incident response assignments is not acceptable.

In addition, the following applies here:

[3] Information on language levels: https://www.coe.int/en/web/common-european-framework-reference-languages/table-2-cefr-3.3-common-reference-levels-self-assessment-grid.

The service provider assesses 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 incident response it provides.

If the service provider to whom the incident response is outsourced carries out the work under valid service certification in accordance with the CCV Certification Scheme Cyber Security Incident Response, 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 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 incident response is secured.

Security policy

The service provider has a security policy that covers, as a minimum, the systems it uses in incident response, as well as the data obtained from clients in the context of the incident response. This policy includes, at a minimum:

- concrete technical security measures to protect customer information;
- concrete time limits for the storage and cleansing of raw data concerning clients, with a minimum storage time of one year[4], 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.

Initial information and consent

The service provider has procedures in place for the acceptance of monitoring assignments. The initial information forms part of the intake process (see 2.2.2). In addition to the initial information, the consent of all owners of systems in scope is necessary.

Integrated in this procedure is providing clarification per client on what party executes isolation if an incident requires it; the client itself, a third party assigned by the client, or the service provider. In the latter case, arrangements are made for proper additional information and information as needed by the service provider. This can be part of the contract, for both retainer and ad hoc clients. In the case of ad hoc clients, the working procedure of the service provider aims at clarifying this point in the intake process, (Also 2.2.4, under “performing isolation”).

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

Methodologies
For all aspects described in chapter 2, the service provider applies internally documented standard methodologies. These (high level) protocols are part of the service providers quality management.

Triage (and follow-up)
The quality management system determines the process steps to follow in order to deliver triage, in line with the definitions of and requirements for triage as defined in chapter 2. Additionally, the service provider records all triages performed. The service provider can provide an overview of both:

- Reported issues or incident leading to triage <u>with</u> follow-up by the incident responder (such as Containment, Eradication, and Recovery);
- Reported issues or incidents leading to triage <u>without</u> further follow-up by the incident responder. For the latter category, the incident response provider can provide documentation leading to the decision not to take further incident response actions.

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

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

Registrations
The service provider has the following registrations:

- overview of employees[5], their duties, powers and responsibilities and 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 incident response performed.

The data of the service provider is kept for a period of at least one year[6]. This refers to data regarding the quality system itself, but also to data regarding delivered incident response (see 3.2.6) and incident response reports.

3.2.8 Complaints

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

The service provider confirms the receipt of a complaint in writing to the complaining party within a maximum of two weeks. The service provider settles the complaint within at most two months and sends a written message to the complaining party. In the written message the service provider states

[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.

whether the complaint is justified and indicates what measures have been or will be taken. If the complaint is not justified, the service provider explains why this is the case.

3.2.9 Recovery and corrective measures

The service provider has a written procedure in place for recovery and corrective action. In case of errors and deviations found, the service provider takes 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;
- testing the activities of operational staff against the prescribed working methods;
- 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.

3.3 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[7];
- a declaration by an authorised person that the service provider complies with the requirements, conditions and obligations stated in the certification scheme;
- the possible presence of several branches, which provide incident response.

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 service provider has access to all relevant information.

3.3.4 Planning

< Not applicable in this certification scheme; as incident response assignments cannot be planned, and thus the certification body cannot by advance be informed about clients and dates.>

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

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 incident response;
  - quality assurance of the incident response;
  - 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 >

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.

The certification body verifies if the requirements in chapters 2 and 3 are met by the service provider. The certification body does so by a combination of administrative verification, including a sample of incident response project files, and interviews that can relate to all these requirements.

Due to the nature of Incident Response, including the lack of plannability, witnessing the execution of the actual work during an incident is not automatically part of assessments by the certification body. However, the certification body has the possibility to add that method for specific certification decisions. Reasons can be the certifications own preliminary findings or concerns raised by other parties. Whether or not to use this option is at the certification body's own discretion. This can apply both to initial and periodic assessments or can be part of additional review (4.6).

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[8] 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 implements the necessary details. The certification body informs the scheme manager of this by submitting the subject for harmonisation.

Certification bodies can, 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 case of a conflict regarding implementation in which the same objective is pursued, the certification scheme is not binding. Such cases are 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 is qualified based on the required competences. Competences are based on demonstrable "knowing" and "ability".

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

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 sets up a training programme for newly qualified certifying staff, aimed at achieving the required competencies.

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

Certification staff directly involved in certification assessments (auditors, inspectors) are 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 details 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 ISO 27001, including the necessary knowledge, experience, and certifications to carry out the audit in an adequate and compliant manner.
- 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 nonconformity;
- being able to explain and communicate findings and nonconformities to the service provider;
- being able to report the findings and nonconformities, including an assessment of their significance, in clear and unambiguous terms in 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 incident response service against the requirements set in chapter 2 of the certification scheme;
- being able to assess and weigh the possible effects of an observed nonconformity;
- being able to explain and communicate findings and nonconformities to the service provider;
- being able to report the findings and non-conformities, including an assessment of their significance, in clear and unambiguous terms in writing;
- qualified for auditing management systems in accordance with ISO/IEC 27001;
- have knowledge of and can work with the certification scheme;
- have knowledge of the process of an incident response service.

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

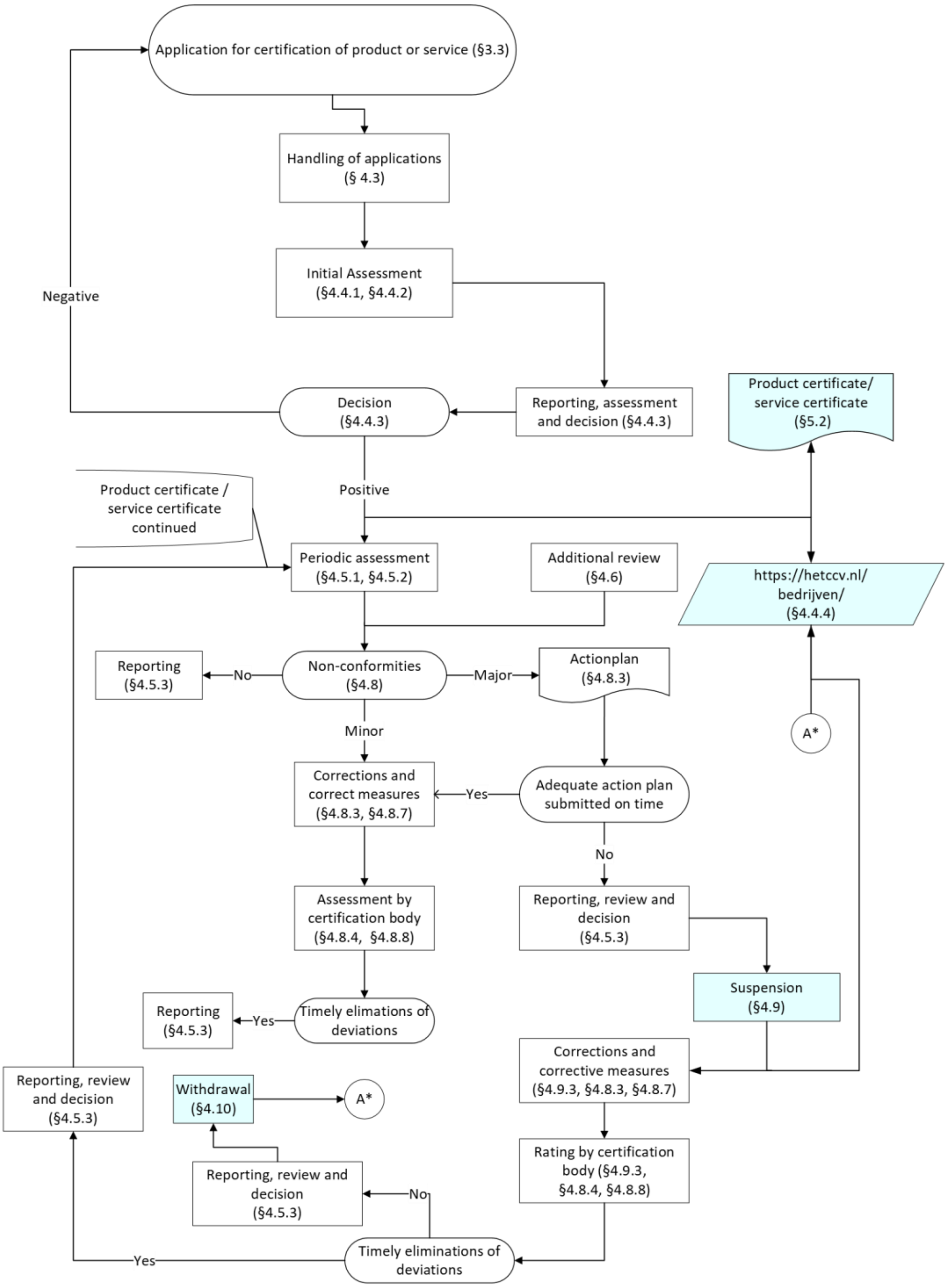

Application for certification of product or service (§3.3)
Handling of applications (§ 4.3)
Initial Assessment (§4.4.1, §4.4.2)
Negative
Decision (§4.4.3)
Reporting, assessment and decision (§4.4.3)
Product certificate/ service certificate (§5.2)
Positive
Product certificate / service certificate continued
Periodic assessment (§4.5.1, §4.5.2)
Additional review (§4.6)
https://hetccv.nl/ bedrijven/ (§4.4.4)
Reporting (§4.5.3)
No
Non-conformities (§4.8)
Major
Actionplan (§4.8.3)
Minor
A*
Corrections and correct 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)
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)
Reporting, review and decision (§4.5.3)
Withdrawal (§4.10)
A*
Rating by certification body (§4.9.3, §4.8.4, §4.8.8)
Reporting, review and decision (§4.5.3)
No
Yes
Timely eliminations of deviations

Figure 2 – Product and service certification process diagram NEN-EN-ISO/IEC17065

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 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 corrective measures and their demonstrability.

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

The budget is set out 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 incident response service 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 of the entire assessment takes 2 hours. Regarding the assessment of the quality system, the starting point for the initial assessment is 6 hours. If the service provider already has other relevant certificates that justify a less extensive assessment of the quality system, this can be reduced in the following scenario's: ■ When the service provider is certified for ISO 27001 under accreditation with a relevant scope, the audit duration can be reduced to a limit of 3 hours. ■ Certificates under other CCV cyber security certification schemes can lead to a reduced audit time of 3 hours. Alternatively, when the service provider is audited for two CCV cybersecurity certification schemes simultaneously and the quality management systems for both services are integrated or directly related, the audit duration for the quality management system can be reduced to 6 hours, distributed across both files. The number of hours can also be increased, if it concerns a service provider that carries out many incident response services, a large number of personnel is involved, the organisation is complex and/or the way the quality system is organized makes the assessment more time-consuming. No maximum of hours applies here.

	Full reporting (on quality system + service-oriented control[9]) 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 harmonisation investigation by the CCV.

B INITIAL ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)	
Technical facilities	The use of tooling is assessed during the service-specific assessment.
Evaluation of the incident response service	The implementation of the incident response service is evaluated against all requirements from the relevant section in chapter 2. Assessment of the incident response service consists of: ■ assessing two different incident response files, to be selected by the certification body. This includes verification of the report. ■ monitoring the implementation of the incident response service 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. 1,5 hours are assumed for each incident response file to be examined. For monitoring the implementation of incident response services, the following principles apply: ■ The certification body asks one or two employees of the service provider about the process followed in two incident response projects. ■ When assessing the two incident response projects, the certification body can ask questions relating to the following topics. These may be supplemented or replaced with 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 incident response service? – 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?

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

	– How is the customer involved in the process? – How did the final report come about? – How was the project completed? – How has it been ensured that no artifacts / remnants of the incident response service are left behind? – Has there been a final review?
File	The project file of the incident response 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, procedures, documentation).

4.4.3 Reporting, assessment and decision-making

Each initial assessment is 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 are 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 in the search engine with qualified companies (www.hetccv.nl/companies). 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 incident response service 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 for the entire assessment takes 2 hours. Regarding the assessment of the quality system, the starting point for the periodic assessment is 4 hours. If the service provider already holds other relevant certificates, such as ISO 27001 under accreditation with an appropriate scope or certificates under other CCV cyber security schemes, the audit duration (assessment of the quality system) can be reduced to a minimum of 3 hours.. When the service provider is audited for two CCV cybersecurity certification schemes simultaneously, the total audit duration for the management system can be reduced to 6 hours, distributed across both files. The number of hours can also be increased if it concerns a company that carries out many incident response services, 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 of hours applies here. Full reporting (on quality system + service-oriented control[10]) 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 incident response services	The implementation of incident response services is evaluated against all requirements from the relevant section in chapter 2. Assessment of the incident response service 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;

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

B. PERIODIC ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)

- monitoring the implementation of the incident response service and assessing whether it is carried out in accordance with chapter 2, possibly requesting clarification and explanation.

1,5 hours are assumed for each incident response service file to be examined.

Deliveries of incident response services in a 12-month period are assessed by the certification body according to the table below:

NUMBER OF INCIDENT RESPONSE SERVICES	NUMBER OF PROJECT FILES FOR ASSESSMENT
0	-[11]
1 or 2	1
3 to 15	2
16 to 50	3
51 to 100	5
101 to 200	7
201 and more	9

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

At least 95% of the executed incident response services 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 explains 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 is divided as much as possible (spread over types of incident response services, staff, customers), but can also extended, if this is necessary for the representative picture. The checks are preferably and where possible, spread over the year, so that a representative picture emerges with regard to the quality of the incident response service provided.

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

[11] If less than one incident response service referred to in Chapter 2 is delivered per calendar year, the certification body makes further agreements with the service provider under which condition the service certificate issued by the certification body remains valid. If the service provider does not provide certified incident response services according to this certification scheme for two consecutive years, the certification body will suspend the certificate.

B. PERIODIC ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)	
	For monitoring the implementation of incident response services the following principles apply: 1. The certification body asks one or two employees of the service provider about the process followed in incident response 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 incident response service(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 incident response reports are assessed. 4. When asking questions about the two projects whose file is being assessed, 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 incident response service? – 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 incident response service are left behind? – Has there been a final review?
File (during audit)	The project file of the reviewed incident response services (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 immediately informs the certification body about this, so that the certification body is enabled to carry out an interim audit of this incident response service 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 nonconformities. If the nonconformities are resolved within the time limits specified for this purpose, the report contains a positive conclusion on the conformity found so that the certified status can be maintained without any decision being taken.

If nonconformities 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 can 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.

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

See table A in section 4.4.2 and section 4.5.2.

4.8 Nonconformities

A situation which is not in accordance with the requirements is considered a nonconformity. Nonconformities may relate to the incident response service delivered under certificate and/or to the quality system. Nonconformities can be classified as major or minor.

The certification body communicates nonconformities 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), nonconformities 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 incident response service that meet the requirements set, or
- The same nonconformity 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 incident response service supplied under certificate does not meet the requirements set, because:

- dangerous or unsafe situations (may) arise, or
- the digital system on which the incident response service 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 nonconformities, the service provider 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 action plan consists at least of:

- an analysis focused on the root cause and/or root causes of the nonconformity. This analysis includes in any case (but not be limited to) the possible causes in the process of producing the incident response service and the possible causes in the failure of control processes;
- the actions to be taken immediately to prevent further non-compliant incident response services from being delivered with the certification mark;
- An analysis focused on the incident response services 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 incident response services 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 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 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 , 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 can 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 incident response service 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 – Services

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

4.8.7 Minor – Consequences

The service provider is given a period of three months to take corrective action. The corrective measures include at least:

- an analysis focused on the root cause and/or root causes of the nonconformity. This analysis includes in any case (but not be limited to) the possible causes in the process of producing the incident response service and the possible causes in the failure of control processes;
- an analysis focused on the scope of incident response service 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 incident response services 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 fully documents 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 is carried out for verification.

The certification body can 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 an action plan on time when determining a major nonconformity (see section 4.8.3), or;
- If the action plan that does not sufficiently guarantee that corrections are carried out and/or the action plan 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 nonconformities have not led to the elimination of the nonconformity or nonconformities 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 incident response services 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 documents the assessor's advice, the review and decision-making process and the decision in full, including the substantiation.

The certification body informs 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/bedrijven. From the moment of suspension, the service provider cannot use the certification mark. Nor can the service provider refer to the certified status of the incident response service to be delivered. The service provider remains responsible for remedying defects in the incident response service 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 is lifted. The certification body informs the service 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 is permitted again.

A suspension lasts a maximum of six months.

4.10 Withdrawal

4.10.1 Withdrawal

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

The certification body informs 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 cannot use the certification mark or refer to the certified status of the incident response service to be delivered. The certification body removes the data of the service provider from the certification scheme concerned on www.hetccv.nl/bedrijven.

The service provider remains responsible for remedying defects in the incident response service 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, can again apply for an initial assessment in accordance with the certification scheme (see section 4.4).

5 Certificate and certification mark

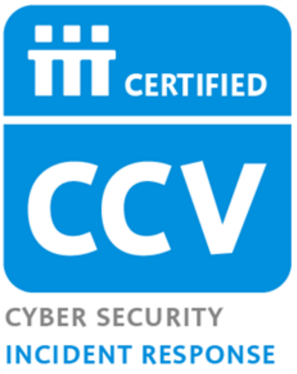
5.1 Certification mark

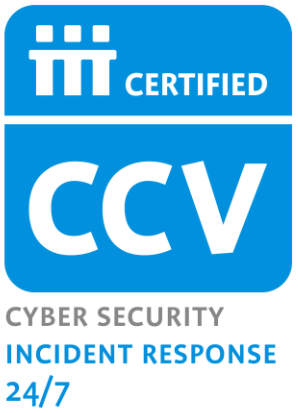
The certification mark, further called ‘the mark’, is the proof for buyers that the certification body has a justified confidence that the service provider who delivers an incident response service complies with the requirements set in the certification scheme (as described in chapter 2) and that the 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 marks

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





The certification mark affixed to the report indicates legitimate confidence in the quality of the incident response service.

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 is permitted under certain conditions.

The service provider places the mark on the final report, see section 5.3. The use of the mark is mandatory. In addition to this paragraph, the regulations stated in ‘CCV Reglement Kwaliteitslogo’ apply to the use of the certification mark. 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 is drawn up in the house style of the certification body. The service provider may advertise itself as "Registered to provide certified incident response services".

The service certificate contains at least the following data:

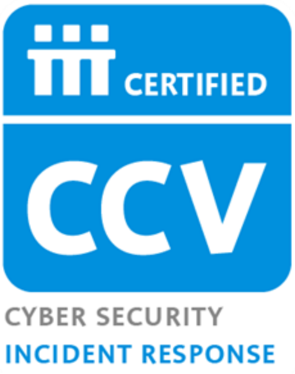
- name and address of the certificate holder (correspondence address);
- the texts and certification mark

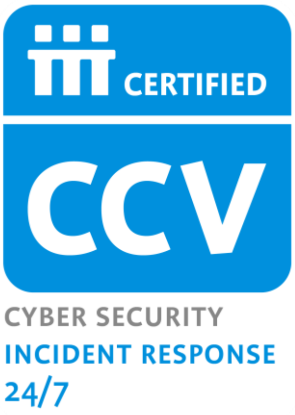
  "<Certification body> declares that, based on the assessments by <Certification body>, confidence is justified that the incident response service carried out by the service provider, including the final report, complies with the requirements set out in the CCV certification scheme – Cyber Security – Incident Response, version 1.0>."

  When applicable with the addition: "This includes the sub-scope 24/7."

  "<Certification body> licenses the certification mark shown here to <the service provider> for the incident response service delivered under the certification scheme."

[Depending on sub-scope one of the following]





- 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:

  "Incident Responders and third parties can check the status of a valid service certificate with <certification body> or on <reference to www.hetccv.nl/incident-response> "

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

5.3 Final report with certification mark

The service provider provides a final report with the certification mark, upon delivery of the incident response service.

The service provider places the certification mark on the definitive version of the final report for the client. The layout of the document is such that it is clear that it concerns a final report of an incident response service. The report explicitly states that the certification mark is about the quality of the incident response service.

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

6 References

6.1 Terms and abbreviations

Assessment	Implementation of this certification scheme by the certification body at the service provider.
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 incident response service provided.
Certification mark	Word or figurative mark used to indicate conformity to requirements
Certification scheme	System of rules, procedures and management aspects for performing certification assessments.
Committee of Interested Parties	The committee within the CCV that determines the support for the scheme and advises the CCV on (amendments to) the certification scheme. Interested and involved parties are represented in this committee.
Customer	Person or organisation that purchases the incident response service.
Incident Response*	Responding to a cyber incident. It is a (structured) approach at all levels: operational, tactical, and strategic. Incident response can be seen as a kind of fire brigade for a cyber incident.
Initial assessment	Assessment leading to a decision on certification and, in the event of a positive decision, issue of the service certificate.
ISO	International Organisation for Standardization. An ISO standard is an international standard issued by ISO.
Multi-site certification	Certification for organisations with multiple locations operating under a shared quality system. One certificate covers all sites if they meet the criteria for central management and consistent implementation.
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.
Retainer	A contractual agreement ensuring availability of a service provider for incident response during the contract period.
Root cause analysis (RCA)	A structured method to determine the fundamental cause(s) of an incident.
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 incident response service.
Service-oriented assessment	Assessment of the incident response service by the certification body, including the final report.
Service provider	The organisation providing the incident response service.
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.
Triage	The process of assessing and categorizing the severity and impact of an incident to prioritize response actions.
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 apply as indicated herein. A certification body possesses all normative standards and documents. The service provider has at least those standards and documents marked with an * at his disposal.

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**

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

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

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