

Interface	RX bps	pps	%	TX bps	pps	%
ens33	0	0	0	0	0	0
ens33	0	0	0	0	0	0
ens33	0	0	0	0	0	0

```

lo
Interfaces:  RX bps  pps  %  TX bps  pps  %
lo           0      0  0    0      0  0
qdisc none (noqueue)
ens33       0      0  0    0      0  0
qdisc none (pfifo_fast)

(RX Bytes/second)
0.00 .....
0.00 .....
0.00 .....
0.00 .....
0.00 .....
0.00 .....
1      5     10    15    20    25    30    35    40    45    50    55    60

----- Press d to enable d
----- Press t to enable add

Thu Mar 16 10:09:39 2017

+myach-c0lon pe EXTBSV 26 T nt 10000:00/1000
) Golf-India ) ext file bus 610 director 0000:00/1000
Whiskey-yan y tool 'toolin tes, 1320 fl 4/pc
kee-alfa-cha y stall,instal Size: 0
rle-hotel-c lerActive 1' 0 Block
olon tined out /sys/power ks: 0
Kannogee (Ka ENOTRECOVERA disk 4096 dirc
mm-Op-ee) Kl BLE 131 Stat ze pn_async Device: 12h/
to-alfa-mke e not recove pn_free 18d Inod
-mike-Oscar rable stall,instal e: 14146
golf-echo-ec EPROTOTYPE 0 lerActive 10 pn_print Links: 3
ho 1 Protocol 0 times Access: (075
Odkovwalk (0 rong type fo + nv /opt/vm pn_test S/dmwr-xr-x
d-Kov-walk) r socket ware-toolst pn_trace 0/ root)
Oscar-delta ENSGSIZE 90 nstaller/tig dev_trace 0/ root)
Kilo-oscar-v Message too htdm.conf /e dev_match 0/ root)
ector-whiske y,alfa-ltna tc/inte pn_wakeu 0/ root)
kilo long ENOTBLK 15 B p,lrq reserved
nosladcau (N lock device + rm -rf /pp state
o-slad-cau) requtred /vmware-too installer
November-osc ENDSPC 28 No space left on device + /sbin/inte
ar-sterre-ll EALREADY 114 cll start tk wake_loc
no-alfa-delt operation progress wake_unl
fa-uniform GretEuph0a ( tready in pr /rcs.d/s0src ock
Gret-Euph-0a ) golf-romeo EISNAH 120 I local wakeup_c
echo-tango s a named ty + nv /etc/rc count
  
```

**CCV** centrum voor criminaliteitspreventie en veiligheid

CCV Certification Scheme

# Cyber Security Monitoring

Version 1.0  
 Publication date: 1 February 2026  
 Effective date: 1 May 2026



# Foreword

This certification scheme is aimed at the certification of security monitoring - 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.

© 2026. All rights reserved. No part of this publication may be reproduced, stored in a database or retrieval system, or published, in any form or by any means, electronically, mechanically, by print, photo print, microfilm or any other means without prior written permission from the publisher.

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.

Making copies of this publication is permitted on the basis of Article 16B of the Copyright Act 1912 in conjunction with the Decree of June 20, 1974, Dutch Bulletin of Acts and Decrees 351, as amended by the Decree of August 23, 1985, Dutch Bulletin of Acts and Decrees 471 and Article 17 of the Copyright Act 1912, the legally required fees must be paid to Stichting Reprorecht (PO Box 882, 1180 AW Amstelveen). The publisher must be contacted regarding the copying of part(s) of this publication for use in anthologies, readers and other compilation works (Article 16 of the Copyright Act 1912).

# Inhoud

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	General	5
1.1.1	Purpose	5
1.1.2	Responsibilities	6
1.1.3	Reading guide	6
1.2	Scope	6
1.2.1	Prerequisite certification	6
1.3	Relation to laws and regulations	7
1.4	Relationship chart	7
1.5	Transitional provisions	7
<b>2</b>	<b>Service requirements</b>	<b>8</b>
2.1	General	8
2.2	Assessment methods, requirements, approval and rejection	8
2.2.1	General	8
2.2.2	Monitoring plan	9
2.2.3	Monitoring process	12
2.2.4	Output: Reporting, Advice & Response	14
<b>3</b>	<b>Conditions for the service provider</b>	<b>21</b>
3.1	General	21
3.2	Quality system requirements	21
3.2.1	Organisation and responsibilities	22
3.2.2	Qualifications	22
3.2.3	Measuring means and equipment	25
3.2.4	Outsourcing	26
3.2.5	Contracting temporary or external personnel	26
3.2.6	Primary processes	26
3.2.7	Document management, registrations and archiving	28
3.2.8	Complaints	28
3.2.9	Recovery and corrective measures	29
3.2.10	Evaluation	29
3.3	Requirements for application and maintenance	29
3.3.1	Application data	29
3.3.2	Status during application	29
3.3.3	Access to information	30
3.3.4	Planning	30
3.3.5	Amendments	30
3.3.6	Limitation of scope	30
<b>4</b>	<b>Conditions for the certification body</b>	<b>31</b>
4.1	Requirements for the certification body	31
4.1.1	General	31
4.1.2	Qualifications	31
4.2	Process diagram	33
4.3	Handling of applications	34
4.4	Initial assessment	35
4.4.1	Implementation	35
4.4.2	Time spent and sample	35
4.4.3	Reporting, assessment and decision-making	37

4.4.4	Publication	37
4.5	Periodic assessment	37
4.5.1	Implementation	37
4.5.2	Frequency, time spent and sample	38
4.5.3	Reporting, assessment and decision-making	41
4.6	Additional review	41
4.7	Reduction of time spent based on other certificates	41
4.8	Nonconformities	42
4.8.1	Major - Quality System	42
4.8.2	Major – Service	42
4.8.3	Major – Consequences	42
4.8.4	Major - Assessment by the certification body	43
4.8.5	Minor - Quality System	43
4.8.6	Minor – Service	43
4.8.7	Minor – Consequences	43
4.8.8	Minor - Assessment by the certification body	44
4.9	Suspension	44
4.9.1	Suspension	44
4.9.2	Consequences of suspension	44
4.9.3	Lifting the suspension	45
4.10	Withdrawal	45
4.10.1	Withdrawal	45
4.10.2	Consequences of withdrawal	45
4.10.3	New application	45
<b>5</b>	<b>Certificate and certification mark</b>	<b>46</b>
5.1	Certification mark	46
5.1.1	Certification mark	46
5.1.2	Use of the mark	46
5.2	Service certificate	47
5.3	Periodic reports with certification mark	47
<b>6</b>	<b>References</b>	<b>49</b>
6.1	Terms and abbreviations	49
6.2	Standards and references	50

# 1 Introduction

Protecting digital systems and keeping them secure is important for every business. It only takes one vulnerability in a system for the damage to be extensive. It is up to the organisation to protect itself against attacks, vulnerabilities or other threats. Security controls consist of a combination of digital security and organisational measures. Cybersecurity services ensure that digital systems are properly secured, in line with the risk of a cyber incident. A company or other organisation that wants to protect itself against cybercrime needs this to be done properly, with safe products and services, installed or carried out by a professional. This is often difficult for the entrepreneur to assess properly on his or her own. Certification schemes for cybersecurity services offer a good solution for this purpose. This certification scheme focuses on security monitoring.

## 1.1 General

### 1.1.1 Purpose

The aim of this document, the certification scheme, is:

- increasing the quality of the security monitoring service;
- offering clients (public and private parties) certainty about the quality delivered by a supplier with a quality mark;
- limit the social costs of cybercrime, borne by organisations and citizens.

#### 1.1.1.1 Target audience

There are two target groups for the certification scheme:

- clients: companies, public and semi-public organisations that want to increase their cyber resilience by monitoring their digital systems for unusual and unwanted activities. They can consider acquiring the services of a managed security services provider (mssp).
- providers of the monitoring service: through certification and associated supervision, they are given an incentive to improve and maintain their own quality system, to properly guarantee the quality of the service provided and are given the opportunity to distinguish themselves in the market with the quality mark.

#### Note

The “provider of the monitoring service” in many cases is a service provider with several external clients, in an open market. However, this certification scheme can also be used to certify an “in-house” monitoring service, where an internal department of an organisation provides cyber security monitoring. This means the organisation itself is the only or main client. In this case certification and associated supervision also gives an incentive to improve and maintain the internal quality system, to properly guarantee the quality of the service provided. In addition, the organisation can use certification of its internal cyber security monitoring to demonstrate control over this aspect of cyber security, in its communication with clients, stakeholders or supervising bodies. A monitoring division can have as primary client the organisation it is part of and have external clients. In such cases, both the internally and externally delivered services are subject to the criteria of this certification scheme.

### 1.1.2 Responsibilities

Companies and other private and public organisations have to take measures to increase their cyber resilience. It is essential that they can engage reliable cybersecurity companies that provide professional services of demonstrable, high quality.

The organisation providing security monitoring - hereafter referred to as "the service provider" - is responsible for compliance with the certification scheme. It must ensure that the monitoring 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 security monitoring service and how this is assessed (chapter 2);
- conditions for the service provider to obtain and maintain the service certificate (chapter 3);
- harmonised 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, 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 cyber security monitoring, including reporting. When we refer to monitoring in this certification scheme, it concerns security monitoring.

Security monitoring is defined as 'continuous monitoring of a computer or digital infrastructure with the aim of detecting suspicious and/or anomalous events or patterns which could harm the business of the organisation'. It concerns both information and operation technology (IT and OT). Continuous means security monitoring by triggers and/or 24/7 attention. Detection will lead to a reaction in the form of reporting, advise and/or possible mitigating actions (see 2.2.5.4).

This certification schema is focused on cyber security. Thus, the following is **not** in scope:

- Availability and performance monitoring, when not directly linked to security.
- Network Operation Centre
- Compliance monitoring

When a service provider provides cyber security monitoring under the certification scheme, all of his monitoring 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.

For specific cases that may be exempt from the 'all monitoring under certification' rule, and the conditions under which such exceptions apply, see section 4.5.2.

### 1.2.1 Prerequisite certification

Certification under this scheme requires certification under ISO/IEC 27001 by an accredited certification body. See section 3.2.12 for motivation and application.

### 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

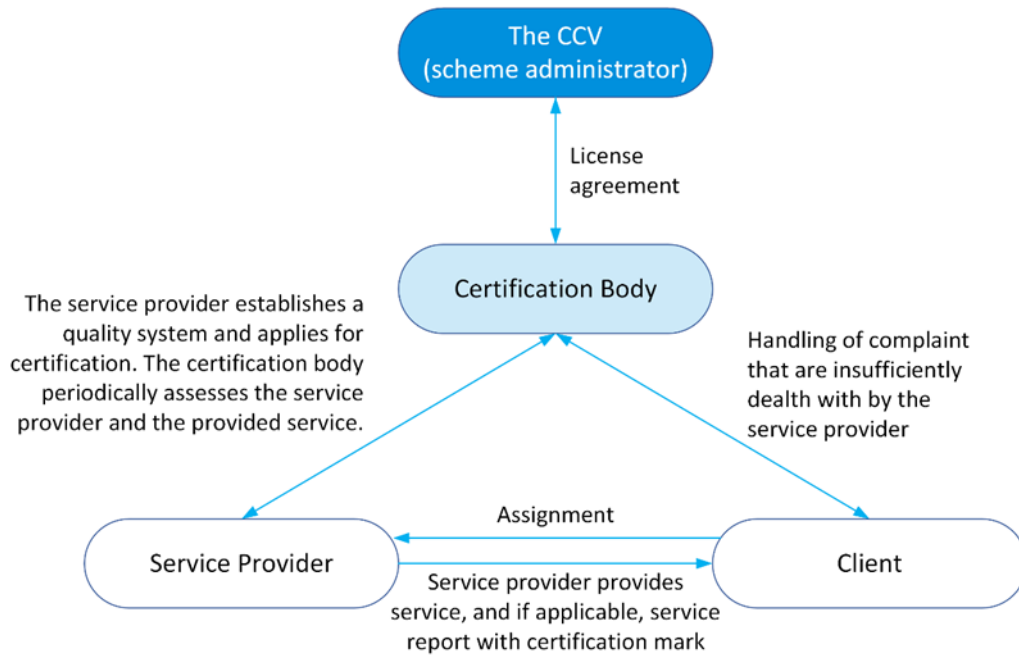


Figure 1 - Overview of parties involved in service certification

### 1.5 Transitional provisions

No transitional arrangement is necessary; the certification scheme is a new scheme and has no predecessor.

## 2 Service requirements

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

### 2.1 General

All technical and administrative requirements with which cyber security monitoring supplied under certificate must comply, and the way in which this is assessed, are included in this chapter. Failure to meet the requirements set out in this chapter will result in rejection.

### 2.2 Assessment methods, requirements, approval and rejection

#### 2.2.1 General

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

TABLE 2A ASSESSMENT METHODS	
METHODOLOGY	DESCRIPTION
(A) Administrative	<p>Assessment of administrative documents such as design documents, certificates and reports</p> <p>A1: Assessment of completeness: checking that required documents or records are complete.</p> <p>A2: Assessment of correctness: checking that the content and implementation meet the requirements and correspond with evidence observed in practice.</p> <p>Note: <i>Assessment A1 and A2 can only be carried out if the documents are present</i></p>
(I)	<p>Interviews, formal and/or informal, relating to the service and/or the quality system.</p> <p>Note: <i>This method can be used by the certification body, in addition to the methods A1 and A2 as mentioned in the following paragraphs, at the discretion of the certification body.</i></p>

The service monitoring at least consist of the elements monitoring plan (2.2.2), monitoring process (2.2.3) and reporting, recommendations & response (2.2.4).

**2.2.2 Monitoring plan**

**2.2.2.1 Starting the intake - choosing categories and components**

Monitoring requires ingestion of signals across one or more categories/components. The following table provides a matrix overview of the categories and components covered by cyber security monitoring.

In its proposal to a client, the service provider presents the entire matrix below (table 2b), indicating which components it offers, from the full range of cyber security monitoring options.

In addition, the plan clarifies which components are not part of the plan, and why this is the case/what the consequences are. The service provider maps out with the client which components need to be connected to provide an acceptable degree of coverage relating to the risks. As part of this process, the client is made aware that selecting specific monitoring components involves making conscious choices. A client can choose to obtain only one component of monitoring from a service provider. A single component of monitoring is delivered only when both parties agree that this is desirable.

TABLE 2B: OPTIONAL CATEGORIES AND COMPONENTS		
CATEGORY	COMPONENT	ENTAILS (EXAMPLES)
Network	Firewall	Traffic logs & Security alerts
	DNS	Query logs
	VPN	VPN logs
	Switches/routers	Span ports, net flow
Compute	Servers	Application logs, os logs, file activity monitoring, file system logs, file integrity, IDS/IPS, Vulnerability scanning logs, patch management logging
	Database	database activity monitoring, database logs
	"serverless" platforms	Function invocation logs
Platform (configuration perspective)	IaaS	platform / cloud (config) logs
	SaaS	platform / cloud (config) logs
	PaaS	platform / cloud (config) logs
End-user device	Laptops	endpoint detection, EDR logs, Anti-malware logs, File integrity, IDS/IPS, Vulnerability scanning logs, patch management logging
	Desktops	endpoint detection, EDR logs, Anti-malware logs, File integrity, IDS/IPS, Vulnerability scanning logs, patch management logging
	Mobile devices	endpoint detection, EDR logs, Anti-malware logs, File integrity, IDS/IPS, Vulnerability scanning logs, patch management logging
	Phones	Phone logs
E-mail/Collaboration	Phishing filtering	Email logs
	Spam filtering	Email logs
	Links	Email logs

**TABLE 2B: OPTIONAL CATEGORIES AND COMPONENTS**

CATEGORY	COMPONENT	ENTAILS (EXAMPLES)
Identity	AD	MFA, SSO, LDAP/AD logging, UEBA
	Other identity stores	MFA, SSO, LDAP/AD logging, UEBA
Applications		User behaviour analytics, application logs
Enrichment	Honeypots, Threat intelligence	Attack logs
	Canary Tokens	Alert logs
	Vulnerability management	Vulnerability scanning logs, patch management logging

2.2.2.2 Monitoring Process - scope/outline

The monitoring process is an essential part of the monitoring service and must be formally established and documented to ensure consistency and verifiability. The process covers, at a minimum, the activities described in section 2.2.3 (including detection, triage, analysis, and possible response coordination).

2.2.2.3 Monitoring plan

As part of the intake and assignment process for monitoring, the service provider explains and documents how the security monitoring of the identified signals will be delivered. This includes how the signals are covered within the defined service modules and tiers. (Part of this can be done in request for proposal and request for information phases). This contributes to a plan agreed between the service provider and client, in line with the following criteria.

The monitoring plan is established in the context of the monitoring process described in section 2.2.3. The plan defines which components are in scope and how they are delivered. The requirements in table 2c therefore are applied to assess the monitoring plan against the intended scope and process.

**TABLE 2C: MONITORING PLAN**

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Language of reporting is acceptable for each client	The quote or plan clarifies whether the reporting will be written in Dutch or English or provides the client a choice between those languages.	A1
Summary of service to be provided	The plan describes at least the following elements of monitoring: use of threat intel, monitoring of log sources, use of tooling, detection and possible response, providing recommendations and reporting.	A1
Choice of components of service is clear	The quote or plan adheres to 2.2.1.1 This includes sharing with the client the full matrix of options in the field of monitoring.	A1

TABLE 2C: MONITORING PLAN		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Risk based choices and its background are documented	<p>The plan documents:</p> <ol style="list-style-type: none"> <li>1. What to monitor (what are core or prime assets?);</li> <li>2. Legal/regulatory requirements relevant to the client;</li> <li>3. Presence of relevant data to build use cases.</li> </ol> <p>This information is either:</p> <ol style="list-style-type: none"> <li>a. provided by the client, or</li> <li>b. presented by the service provider and explicitly confirmed by the client.</li> </ol>	A1
Conditions for client	The plan clarifies conditions to be met by the client for monitoring by the service provider <sup>1</sup>	A1
Log source specification	The monitoring plan describes the technical delivery of log data for each log source and explicitly states whether any log aggregation/clustering is used (i.e., where one defined log source represents multiple underlying sources or where multiple sources are combined before ingestion by the monitoring tool).	A1
Concrete description of the infrastructure/environment to be monitored	The quote and/or monitoring plan provides a concrete description of the infrastructure or environment that will be monitored. This includes relevant systems, networks, and applications that fall within the agreed monitoring scope.	A1
Use of Threat Intelligence	The monitoring plan clarifies how threat intelligence is used to support detection and analysis. This includes describing which sources or types of threat intelligence are integrated (e.g., commercial feeds, sectoral sharing platforms, open-source intelligence) and how these are applied to improve detection rules, correlation, and reporting.	A1
Designated team and/or contact person	A specific team works on monitoring for the specific client, and/or a specific first contact person is or will be made available for this client.	A1

<sup>1</sup> For instance, logging managed by the client and necessary for monitoring needs to stay operational.

**TABLE 2C: MONITORING PLAN**

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
	This contact person is familiar with the client's specific concerns and his infrastructure.	
Responsibilities over infrastructures	The plan clarifies which infrastructure is under which responsibility (e.g. which infrastructure is the responsibility of the service provider and which infrastructure is the responsibility of the client). And who is responsible for the back-up of that infrastructure (e.g. gateway server). An infrastructure drawing is added for clarification.	A1
Mitigating response	Clarification that agreeing on the plan also includes agreement on whether, and if so to what extend, mitigating responses are part of the service.	A1

**2.2.3 Monitoring process**

The monitoring process, introduced in section 2.2.2.2, must be formally established and documented to ensure consistency and verifiability. The requirement below specifies the minimum expectation.

**TABLE 2D: MONITORING PROCESS**

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Documented monitoring process	A documented and implemented monitoring process is in place, covering the activities described in section 2.2.3 (including detection, triage, analysis, and response coordination).	A2

To deliver the components of the monitoring service as described in 2.2.1, the service provider applies key process steps as listed in the following outline:

- Coordinating threat information, offering a perspective for action.
- Identity Detection and Response (ITDR)
- Security orchestration, automation and response (SOAR) services.
- Connection of tooling and sources. As part of this the service provider performs regular checks on the availability and integrity of log sources. These checks include, at a minimum:
  - verification that all agreed log sources deliver the expected data;
  - validation of timestamp and time zone accuracy, as well as consistency of log formats;
  - verification that the time difference between event occurrence (as registered at the source) and event ingestion at the monitoring system is within acceptable limits, and that deviations are periodically reviewed and corrected if necessary;
  - detection of interruptions, gaps, or abnormal deviations in the volume of logs received;
  - signalling when a log source fails or becomes inactive;

- verification that any aggregated or clustered log sources are reviewed for the availability and integrity of all underlying sub-sources.

All issues relating to availability and integrity of log sources are documented, and corrective measures are initiated accordingly.

- Setting up detection rules and use cases
- Linking with threat intel sources
- Monitoring, analysis and follow-up of events (triage)
- Provide mitigation advice / propose operational measures
- Incident response (for scope of incident response as part of monitoring, see 2.2.5.4)
- Maintaining threat intelligence sources
- Develop new use cases
- Advice on tactical and strategic measures
- Malware or Artifact analysis (this can be limited to providing relevant information to a third party, for instance an incident response party).
- Periodic testing and maintenance of existing use cases

The monitoring processes are aligned with internationally recognised best practices for incident detection and response, including guidance from NIST SP 800-61. It should be noted that the NIST framework is primarily written from the perspective of an internal organisation, whereas this certification scheme addresses monitoring as a service delivered by an external provider.

As a result, the ultimate effectiveness of monitoring is also dependent on factors beyond the direct control of the service provider, such as the contractual scope, the maturity of the client organisation, and the availability and quality of log sources.

### 2.2.3.1 Analysis

For the analysis phase of the monitoring process, the following criteria apply. (These criteria are inspired by recommendations from NIST SP 800-61 R3).

TABLE 2E: ANALYSIS		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
<b>DE.AE</b> (Adverse Event Analysis)	<p>Anomalies, indicators of compromise, and other potentially adverse events are analysed to characterize the events and detect cybersecurity incidents</p> <p>The service provider can rely on technical solutions that filter large event datasets down to a subset that is suitable for human viewing and analysis.</p> <p>The service provider strives to find incidents earlier in the attack life cycle and take a proactive approach to incident detection and response.</p>	A2
<b>DE.AE-02</b>	<p>Potentially adverse events are analysed to better understand associated activities</p> <p>Tools (e.g., SIEM, SOAR) are used to continuously monitor log events for known malicious and suspicious activity and to generate reports on their findings.</p> <p>Up-to-date cyber threat intelligence is utilized in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise.</p> <p>Manual reviews of log events are conducted for technologies that cannot be sufficiently monitored through automation.</p>	A2

TABLE 2E: ANALYSIS		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
DE.AE-03	Information is correlated from multiple sources Constantly transfer log data generated by other sources to a relatively small number of log servers. Event correlation technology (e.g., SIEM, SOAR) is used to gather pieces of related data captured by multiple sources. Cyber threat intelligence is utilized to help correlate events among log sources.	A2
DE.AE-04	The estimated impact and scope of adverse events are understood The impact and scope of adverse events are estimated through automated (e.g., SIEM, SOAR) and/or manual means, and review and refine the estimates.	A2
DE.AE-06	Information on adverse events is provided to authorized staff and tools Alerts are generated, and provided to cybersecurity and incident response tools and staff (e.g., the SOC and incident responders). Log analysis findings are made accessible to incident responders and other authorized personnel at all times. (In addition, the option is considered to automatically creating and assigning tickets in the organization's ticketing system when certain types of alerts occur.)	A2
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis Up-to-date CTI and other contextual information (e.g., asset inventories) are integrated into adverse event analysis to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. Vulnerability disclosures are rapidly acquired and analysed for the organization's technologies from suppliers, vendors, and third-party security advisories.	A2
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria Incident criteria are applied to known and assumed characteristics of analysed activity, and known false positives are considered to determine whether an incident should be declared.	A2

#### 2.2.4 Output: Reporting, Advice & Response

Monitoring can lead to four forms of output or actions: ad hoc or incident driven reporting, periodic reporting, giving recommendations and executing mitigating response. The following paragraphs provide minimal requirements for these forms of output or action.

2.2.4.1 Ad hoc or incident driven reporting

Minimum data requirements, both for internal registration and for reporting incidents to clients (form and content of messages or reports) are provided in the following table.

TABLE 2F: DATA REQUIREMENTS - REPORTING ATTRIBUTES INCIDENTS		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Available data in reports	Reporting includes at least the following attributes:	
	<b>Attribute</b>	<b>Explanation</b>
	Incident ID	Unique identifier assigned to the incident for tracking and reference purposes.
	Date/time of incident	Time of occurrence / detection.
	Date/time of reporting	If applicable: Time that the customer is informed.
	Priority	Need for response or action in a certain customer or supplier standard. This is described in the "Service Handbook" , SLA, e.g.
	Reported by	If applicable: Internal identifier of the analyst
	Customer Asset reference	Customer Configuration Item Number, Asset name, or equivalent. If no customer asset reference is available, the service provider records alternative identifiers such as IP address, hostname, MAC address, device type, or detection ID.
	Title	Brief description of the incident
	Summary	Short description
	Incident Category	Incident grouping
	Technical details / Indicators Of Compromise (IOC)	As much technical details that is necessary to understand the incident. Depends on type of incident.
	Consequence	An explanation of the type of incident to assist the customer to determine the possible loss or damage.
Recommended actions	Advise in how to handle the incident and how to proceed.	
Attachments	Possible reference documents	
Timelines and prioritisation of incident reporting	The reporting procedure defines how incidents are prioritised and within which agreed timeframes notifications are provided to the client, depending on the severity and potential impact.	A1

2.2.4.2 Periodic reporting

For periodic reporting, the data requirements from 2.2.5.1 apply. In addition, the following requirements apply.

TABLE 2G: PERIODIC REPORTS		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Frequency	<p>Periodic reports are produced every three months at least, and at a higher frequency if the client finds this useful.</p> <p>Note: <i>A real-time dashboard where the client has a complete insight in their security posture and in any actions taken can also fulfil this requirement.</i></p>	A2
Language	The report is written in English or Dutch, as agreed in the intake process.	A2
Content categories	<p>Reports consist of <u>at least</u> the following topics:</p> <ul style="list-style-type: none"> <li>■ Overview of the managed services that are provided. Including the log sources that provide the required information.</li> <li>■ KPI's and their status                             <ul style="list-style-type: none"> <li>– Total amount of cases handled.</li> <li>– Escalated events (events reported to the client, in line with agreed escalation criteria)</li> <li>– Verdicts of escalated cases, including prioritisation and the ratio of True Positives to False Positives (overview of detections indicating the proportion of valid alerts versus false alarms<sup>2</sup>)</li> <li>– SLA status</li> <li>– Health status of the services</li> <li>– Health status of the required log sources</li> </ul> </li> <li>■ Executive summary</li> </ul>	A1
Advice to client	When relevant, the service provider gives the client advice on how to lessen the chance of problematic incidents.	A1.
Evaluation of use cases	Includes an evaluation and if relevant modification of use cases. Evaluation outcomes are shared with the client at an appropriate level of detail, considering confidentiality of detection logic and third-party content.	A2
Recommendations to the client	<p>The service provider provides recommendations based on detected threats or incidents.</p> <p>At minimum, recommendations address identified monitoring coverage gaps (e.g. missing log sources or insufficient detection capabilities).</p>	A2

<sup>2</sup> In many cases, a conclusion “false alarm” can only be drawn in hindsight, partly because often contextual information from the client is required.

TABLE 2G: PERIODIC REPORTS		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
	Additional recommendations can concern infrastructure, preventive or organisational improvements. Recommendations are evidence-based and documented, and their relevance and feasibility are evaluated before sharing with the client.	
Certification mark on report	The report bears the mark referred to in 5.1 of the certification scheme, indicating that monitoring has been conducted correctly by a correctly equipped service provider with qualified personnel, compliant with the CCV certification scheme cyber security monitoring.	A2
Personal presentation and clarification	These reports can be clarified and discussed in a on premises or online meeting. Such a meeting is held at least once every three months.	A1
Systematic feedback from client	At least once a year the client is explicitly invited to give the service provider feedback on both the monitoring itself and on the reporting. The service provider uses the feedback in line with his quality management system (chapter 3).	A2

### 2.2.4.3 Follow up of detection

After triage (see 2.2.2), follow up of positive detection has three aspects; (a) a possible mitigating response, (b) effective communication with the client and (c) efficiently providing required access. This paragraph provides criteria relating to those aspects:

#### a Mitigating response

A possible minor mitigating response by the monitoring service provider, in line with the monitoring plan and contract between the service provider and the client, can be part of the monitoring service as provided. For example, putting a device in quarantine or disabling a user account to prevent spread of unwanted activities and being able to consult the client for further actions.

Actual execution of these response services is *not* part of this certification scheme for monitoring.

The relevant criteria under this scheme relating to response are aimed only at clear agreements; what a client can and cannot expect from the party providing monitoring, in case of an incident, in terms of response or mitigating measures.

TABLE 2H: MITIGATING RESPONSES		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Documented agreement	A written agreement, separately or as part of the general agreement or contract, clarifies what the client can and cannot expect from the party providing monitoring, in case of an incident, in terms of response or mitigating measures.	A2
Prioritised, appropriate signals	If the security incident requires immediate action in order to resolve the incident, the monitoring service provider reaches out to the client, or a third party acting on behalf of the client, via a phone call and shares both a description	A2

TABLE 2H: MITIGATING RESPONSES		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
	and the involved entities to mitigate and/or limit the threat as soon as possible. If resolving the incident can wait, the monitoring service provider will send its findings via a ticket.	
Providing adequate information for response	The client is provided with all relevant information in order to execute a required response. If the security incident requires a mitigating response in order to be resolved, the monitoring service provider reports its findings to the client or a third party acting on behalf of the client.  (Depending on the classification of the security incident, the way of responding might vary.)	A2
Follow-up actions	The follow-up actions are in line with the service provider's standardised processes. Additions or adjustments of monitoring for the client are documented.	A2

**b Communication, focused on cases of escalation**

Incident response requires efficient and effective reporting to, communication with and providing of data to the client or a third party acting on behalf of the client, in case of an incident.

**Note**

For communication and reporting under this certification scheme, the service provider shall ensure proficiency in Dutch and/or English, in line with what is agreed in the monitoring plan. These are the default languages under this scheme. However, agreements between the service provider and the client on the use of languages other than English or Dutch are permitted. Where this is the case, the service provider must ensure that documentation and evidence relevant for certification are available in English or Dutch, or otherwise made understandable for the auditor. See chapter 3 for criteria regarding language skills.

TABLE 2I: COMMUNICATION CONCERNING RESPONSE		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Client- dedicated personnel	Client facing personnel is set and fixed; a limited subset of staff has this role towards the specific client.  Note: <i>This to ensure a thorough understanding of the customer and IT environment, to anchor the services in personnel.</i>	A2

TABLE 2I: COMMUNICATION CONCERNING RESPONSE		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Application of engagement model	<ul style="list-style-type: none"> <li>■ A detailed engagement model across all entities / parties is applied.</li> <li>■ This includes meeting cadence, meeting purpose and related reporting.</li> <li>■ The engagement model specifies the levels within the client’s organisation to which escalation and communication apply, in line with agreements made with the client.</li> </ul> <p>Note: <i>This assessment aspect ensures that escalation is anchored in the governance structure, rather than an ad hoc measure.</i></p>	A2

**c Providing access to data managed by the service provider for follow up**

When a client has outsourced monitoring, the client has provided access to his logs for monitoring. In such scenario’s the client has access to his own logs and can provide that access to third parties without help of the monitoring service provider. However, the client may also want to use the service provider’s SIEM/monitoring tool. Providing access to monitoring data depends on the service model and ownership of the SIEM or monitoring tool.

Where the client owns or contractually has rights to the relevant tool, timely access must be arranged.

Where the tool is owned and operated solely by the service provider, access may be limited, but the provider shall ensure that the client receives all relevant data required for incident follow-up through agreed reporting or secure data exchange.

The following assessment aspect apply:

TABLE 2J: PROVIDING ACCESS		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Providing access to gathered data	<p>The service includes clear arrangements to ensure timely access to relevant data in the event of an incident, in line with agreed response and escalation procedures.</p> <p>This can entail:</p> <ul style="list-style-type: none"> <li>■ Service provider provides the client or a third party on behalf of the client access to his monitoring tool, when requested.</li> <li>■ In case of hybrid monitoring (customer and service provider have a role), the client can already have default access to the SIEM/supplier monitoring. In that case the requirement is that the client’s right</li> </ul>	A2

**TABLE 2J: PROVIDING ACCESS**

ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
	to provide third parties with that access is documented.	

## 3 Conditions for the service provider

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

### 3.1 General

The service provider must be 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).

The following general requirements apply to all service providers seeking certification under this scheme.

TABLE 3A: GENERAL REQUIREMENTS		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
ISO/IEC 27001 certification	The service provider holds a valid ISO/IEC 27001 certification issued by an accredited certification body. The scope of this certification includes the monitoring services provided under this scheme.	A1

### 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 the monitoring service executed under certification. In the following sub sections the requirements of the quality system are elaborated.

Certification under this scheme requires the service provider to be certified under ISO/IEC 27001 by an accredited certification body. The scope of this certificate explicitly includes the monitoring services provided under this certification scheme, as defined in the corresponding Statement of Applicability of the service provider's ISO/IEC 27001 certification. ISO/IEC 27001 certification is considered a minimum requirement, as it ensures that the service provider has a functioning Information Security Management System (ISMS) in place. This ISMS provides the foundation for secure delivery of monitoring services. Obtaining and maintaining ISO/IEC 27001 certification is therefore a prerequisite for certification under the CCV Certification Scheme Cyber Security Monitoring. ISO 27001 certification is obtained either prior to or parallel with certification under this scheme.

### 3.2.1 Organisation and responsibilities

The service provider has an overview of the employees whose work influences the quality of the monitoring service to be delivered. Tasks, responsibilities and authority of these employees and their hierarchical relationships are recorded. This overview includes, at minimum:

- the employee's name or unique identifier
- function or role (e.g. SOC analyst, monitoring engineer, service manager)
- corresponding tasks and responsibilities in relation to the monitoring service
- reporting line and supervising manager

The overview is part of the quality system documentation and is available for review by the certification body during audits. Changes in personnel or responsibilities are recorded without undue delay. The employees are made aware of the quality system, kept informed of any changes, and are responsible for applying it correctly in their daily work.

#### 3.2.1.1 Working under supervision

Employees performing operational monitoring activities who are not (yet) demonstrably qualified may only work under the supervision of qualified employees. The supervision and oversight requirements apply to the monitoring service as a whole. The service provider ensures that each non-qualified employee operates within a defined development path towards qualification, and that qualified employees maintain direct oversight and final responsibility for the execution of the service and the reports delivered.

#### 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

#### *Introduction*

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 members of personnel are deployed for the tasks mentioned. Qualifications are kept up to date and documented.

#### *Setting qualification requirements*

The service provider defines what knowledge, experience, and personal exams or certifications are required to deliver the monitoring service and to operate the specific tooling in use. This is laid down by the service provider in a documented policy and in the provider's training and evaluation plan. In this policy with required qualifications, the service provider can differentiate between specific roles or functions amongst monitoring professionals.

Demonstrable competence may be evidenced through a combination of education, professional experience, and relevant practical certificates. Practical certificates that include a laboratory or hands-on examination are considered strong evidence of competence, provided that they are relevant to the work performed and the tooling applied. Entry-level certificates may be accepted if the service provider can demonstrate, through its training and evaluation plan, that additional internal training and supervision ensure the required competence level. The certification scheme does not prescribe specific commercial certificates; the service provider determines which qualifications are appropriate, taking into account the complexity of monitoring activities and technologies used.

Qualifications for validation of tooling and automated monitoring processes is one of the specific topics that needs to be addressed in the service provider's qualification policy. (Concerning monitoring professionals who are responsible for reviewing and confirming that the automated processes and their results are reliable and suitable for the required monitoring activities, as mentioned in 3.2.3.1).

The service provider demonstrates annually that qualification requirements remain appropriate to the scope of the service, the technological environment, and the monitoring objectives.

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

TABLE 3B - RESPONSIBLE FOR EMPLOYEE QUALIFICATIONS	
Qualification for person being responsible for employee qualification	Set by the Executive Board
Level	Work and thinking skills at HBO <sup>3</sup> level
Knowledge of and ability to work with:	This certification scheme

TABLE 3C – MONITORING PROFESSIONAL	
Qualification of monitoring professional	<p>Set by the service provider (executive board, or if mandated, person responsible for employee qualifications).</p> <p>Includes qualification requirements for reviewing automatic findings from tooling.</p> <p>In addition, specifically for analysts: demonstrable in-depth knowledge and skills concerning cybersecurity monitoring solutions, detection techniques, and the relevant technologies used within the certified service. Evidence is provided through the qualification policy and annual evaluations.</p>
Practical certificate(s)	<p>Set by the service provider (executive board, or if mandated, person responsible for employee qualifications).</p> <p>Includes qualification requirements for reviewing automatic findings from tooling.</p> <p>In addition, specifically for analysts: at least one relevant, practice-oriented personal certificate or equivalent demonstrable competence, aligned with the monitoring technologies and tasks performed. The service provider substantiates in its qualification policy which certificates (or</p>

<sup>3</sup> HBO: higher education level in the Netherlands; universities of applied sciences.

TABLE 3C – MONITORING PROFESSIONAL	
	equivalent internal assessments) meet the required level and why.
Experience	At least 1 year of experience in ICT services and performing security monitoring.  Note: <i>Experience as an intern does not qualify.</i>
Knowledge of and ability to work with	This certification scheme
Language and communication skills	<u>Analysts:</u> Fluent in Dutch language (C1 level) <sup>4</sup> for Dutch speaking clients and/or fluent in English (C1 level) for services delivered in English. Both written communication (reporting) and verbal communication meets this level.  Monitoring team's <u>first contact persons</u> for a client: In addition to requirements for analysts: communication skills, sensitive to perceptions by the client and the client's staff, persuasiveness.
Maintaining qualification	According to the service provider's training and evaluation plan
Qualification of senior monitoring professional	Within the organisation, at least one individual holds overall responsibility for the content and quality of the monitoring service.  All criteria for monitoring professional apply, plus a minimum of <b>five years</b> of demonstrable professional experience in the field of cybersecurity monitoring, security operations, or equivalent activities.  The service provider documents this experience and the person's role within the organisation's quality system.  This requirement ensures that the service provider has sufficient senior expertise to oversee and continuously improve the monitoring processes.

All employees involved in the monitoring process and/or who have access to information related to monitoring (permanent 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 may not be older than three years. In case of personnel not based or

<sup>4</sup> 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>.

registered in the Netherlands, other comparable national certificates or declarations by or on behalf of a national government may apply. Whether these are acceptable is at the discretion of the certification body.

*Applying qualification requirements*

The person within the service provider who is responsible for qualification of employees (table 3B) decides whether personnel is qualified for monitoring based on the general criteria in this scheme and the specific qualification requirements as set in the service provider’s policy. This includes relevant and practice-oriented professional certificates that demonstrate competence in security monitoring or related fields.

The assessment required for this decision is based on:

- evidence that employees possess up-to-date practical knowledge and skills appropriate to their role;
- relevant practical certificates where applicable and aligned with technology in use;
- outcomes of the internal training and evaluation plan.

Annual evaluations are carried out to establish whether or not qualification requirements are met.

**3.2.3 Measuring means and equipment**

Monitoring is partially executed in an automated manner, via tooling. The following criteria apply:

- Findings from such tooling must be verifiable and, where relevant, are reviewed by a monitoring professional.
- The service provider has an overview of tooling that is deployed in the context of delivering monitoring under certification.
- The service provider declares that all tooling used is acquired and used in a lawful manner and that it has licenses for all commercial software used. In case of doubt the service provider can provide the certification body with proof.
- The service provider manages a process to make selections of tooling for detection and/or demonstration of possible issues or incidents in line with the monitoring plan for specific clients. The selected tooling is demonstrably appropriate for the intended monitoring activities.
- The service provider demonstrates that the tools in use are suitable for carrying out the whole of the required monitoring activities.

The service provider periodically tests his monitoring capabilities to verify the correct operation and coverage of the applied tooling. This includes validating the correct implementation and effectiveness of client-specific use cases within the monitoring environment.

TABLE 3D VALIDATION OF AUTOMATED MONITORING		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Tooling overview		A1
Legal use and licensing	The service provider declares that all tooling is lawfully acquired and licensed; proof can be provided to the certification body upon request.	A1

TABLE 3D VALIDATION OF AUTOMATED MONITORING		
ASSESSMENT ASPECT	REQUIREMENT	METHOD OF ASSESSMENT
Suitability of tooling	The service provider demonstrates that the selected tooling is suitable for the monitoring activities and client use cases.	A2
Automated detection	Automated monitoring processes are subject to regular review and validation by a qualified monitoring professional.	A2
Periodic capability testing	The service provider periodically tests and validates monitoring capabilities, including applied use cases.	A2

### 3.2.4 Outsourcing

The service provider may subcontract work to another monitoring service provider. Fully outsourcing a large part of a monitoring assignment 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 monitoring service it provides.
- If the service provider to whom part of the outsourced monitoring service carries out the work under valid service certification in accordance with the CCV Certification Scheme Cyber Security Monitoring, 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 Contracting temporary or external personnel

The service provider may contract temporary/external personnel to carry out the work. All requirements for personnel regularly employed by the service provider (staff) as stated in chapter 3, also apply to temporary/external 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 monitoring service is secured.

### 3.2.6.1 Security policy

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

- in addition to the requirements of ISO/IEC 27001, concrete time limits for the storage and deletion of monitoring-related data. A minimum retention period of one year<sup>5</sup> applies to records and evidence of monitoring activities (such as incidents, alerts, reports, tickets, and client communications), to enable service-oriented assessment by the certification body;
- description of the means the service provider offers to exchange encrypted confidential data - such as reports - with the client, so that confidential data is never stored unencrypted, and never sent via public networks;
- policy relating to the use of a confidentiality agreement to be concluded with employees and subcontractor who have access to data and information of the customer.

### 3.2.6.2 Starting information and consent

The service provider has procedures in place for the acceptance of monitoring assignments. For this purpose, at least the following starting information is available:

- the scope of the assignment in terms of categories and components in 2.2.1.1;
- concrete technical limitation of the object(s) to be monitored;
- project documentation.

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

### 3.2.6.3 Processes for triage, follow-up actions, and the periodic evaluation and updating of use cases.

For the effective delivery of monitoring to its client, the service provider demonstrably maintains processes for triage, detection, follow-up actions, and the periodic evaluation and updating of use cases. These processes reflect the principles set out in NIST SP 800-61 (Rev. 3), while being translated into a service delivery model that is appropriate for Managed Security Services.

- Detection of a possible incident leads to the process of triage: The first response on a detection is an (automated) analyses and triage resulting in a verdict. To determine the right verdict, the definition of these verdicts needs to be clearly described and standardized within the monitoring service. Triage outcomes should at minimum distinguish between events that require follow-up and those that do not. This can include labels such as “requires further investigation”, “benign”, or “confirmed malicious”. Based on such outcome, a standard follow-up action should be described. The follow-up actions can vary in multiple ways based on agreements with the client.
- The service provider maintains and applies a documented process for triage. This process describes how different types of events are categorised, describes possible outcomes and how the appropriate follow-up is determined, in line with the monitoring plan and contractual agreements. As part of this, the process clarifies:
  - how triage verdicts are reached and documented;
  - how events are escalated when required;
  - how follow-up actions are selected, standardised and communicated to the client

---

<sup>5</sup> Par. 4.5.2 offers an alternative approach for a limited subset of projects/clients, in case of special concerns regarding security.

The process includes a mechanism for periodic review and improvement, ensuring that follow-up actions remain effective and aligned with the monitoring service, the client's requirements, and evolving threats.

- The follow-up actions are standardised within processes and additions or adjustments of monitoring per client level are documented accordingly.
- If an event is labelled as an incident, several (external) parties can play a role. When Standard Operation Procedures are no longer suited, the monitoring service provider needs to be able to escalate. The quality system holds a documented operational escalation process, showing both flexibility and the capability to stay in control.
- The service provider can demonstrate it is able to provide access to a third party quickly in case of an incident, for client-cases where this is required (see 2.2.4 C).

### 3.2.7 Document management, registrations and archiving

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

#### *Registrations*

The service provider has the following registrations:

- overview of employees<sup>6</sup>, 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 monitoring service performed.

The data of the service provider must be kept for a period of at least one year<sup>7</sup>. This refers to data regarding the quality system itself, but also to data regarding performed monitoring services (see 3.2.6) and monitoring 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 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

---

<sup>6</sup> This also includes hired personnel (see section 3.2.5) and personnel carrying out evaluation (section 3.2.10)

<sup>7</sup> Due to legislation, longer retention periods may apply to certain documents.

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

### 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 the service provider) and chapter 2 (requirements for service) are permanently fulfilled. To this end, the service provider makes an annual analysis, including the following elements:

- the complaints received and the way in which they are dealt with;
- checking to what extent feedback received, while discussing periodic reports with clients (chapter 2), led to improvements in the monitoring service;
- periodically testing the activities of operational staff against the prescribed working methods;
- periodically testing the quality system for effective implementation;

In 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<sup>8</sup>;
- 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 monitoring.

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 can be made to this application.

---

<sup>8</sup> In the Netherlands, this is registration in the Trade Register of the Chamber of Commerce. Online consultation of the Trade Register is permitted.

### 3.3.3 Access to information

The service provider ensures that personnel of or on behalf of the certification body and the national accreditation 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 monitoring service.

### 3.3.4 Planning

The service provider provides the certification body with all information about all provided monitoring services (for instance when, which customer, what kind of infrastructure, which team/personnel members) 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 monitoring;
  - quality assurance of the monitoring;
  - 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

*This paragraph is not applicable.*

Clarification:

- When a service provider provides cyber security monitoring under the certification scheme, all his monitoring services are delivered in accordance with the criteria in this scheme and are delivered with the CCV certification mark.
- Chapter 2 requires the service provider to clarify to his (potential) clients what subset of aspects of monitoring he will deliver.

## 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 with the CCV<sup>9</sup>.

This certification scheme is not yet implemented under accreditation.

This certification scheme assumes harmonised implementation under NEN-EN-ISO/IEC 17065. Documents published by the national accreditation body relating to the use of ISO 17065 also apply.

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 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 "knowledge" and "ability". More specifically this includes demonstrable knowledge of security operations processes and managed security service providers.

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.

---

<sup>9</sup> The model agreement for certification bodies is published on the CCV website: [www.hetccv.nl](http://www.hetccv.nl).

The certification body has and maintains 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 shall be 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 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) and ISO 27001;
- 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 monitoring 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 nonconformity 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;
- have knowledge of and can work with the certification scheme;
- have knowledge of performing cyber security monitoring.

## 4.2 Process diagram

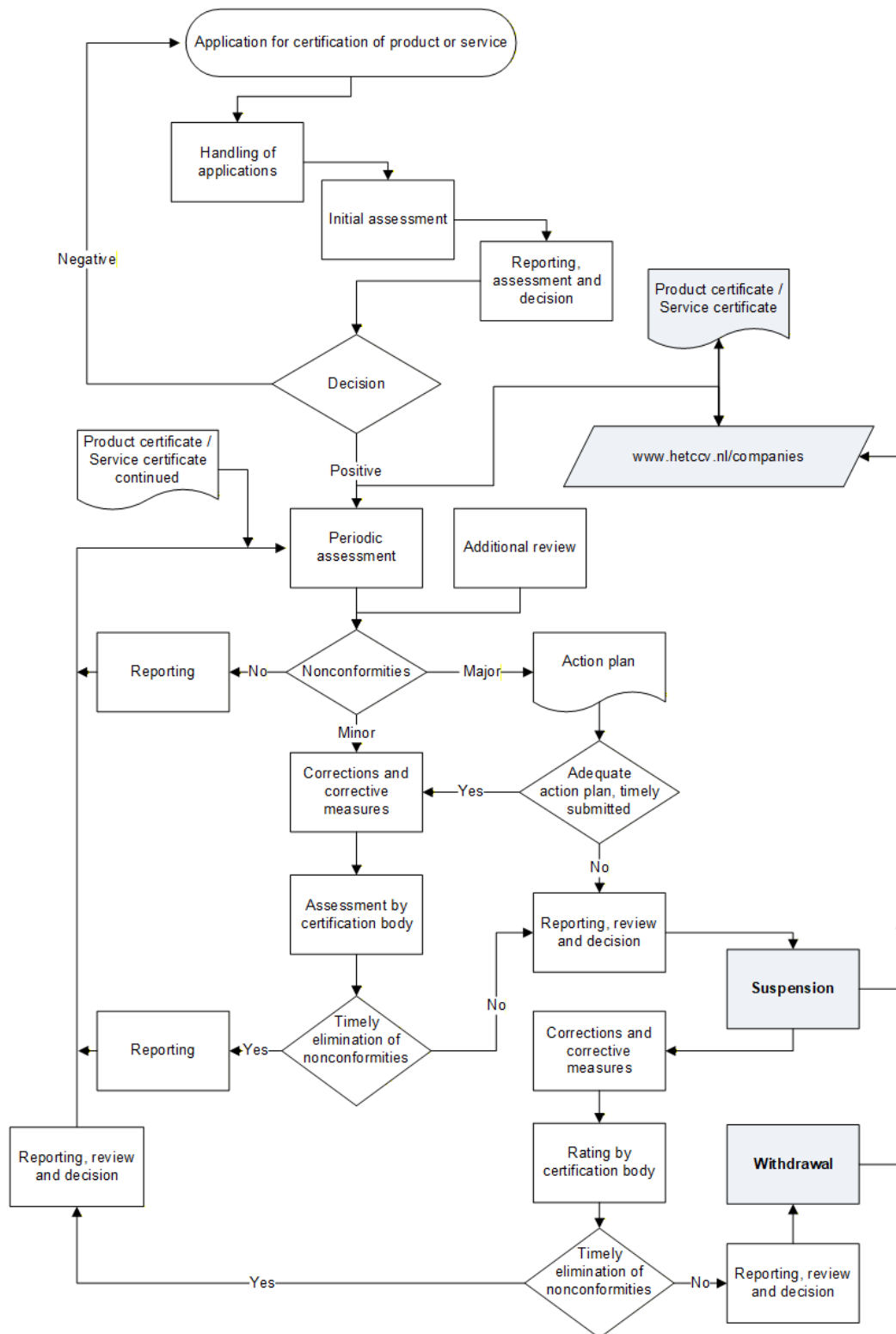


Figure 2 - Service certification process diagram NEN-EN-ISO/IEC17065

### 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 ensures 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 include preparation and reporting time, but exclude travel time and 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, including its substantiation, shall be laid down and approved.

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 monitoring services 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	<p>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.</p> <p>Preparation of the entire assessment takes 2 hours.</p> <p>Regarding the assessment of the quality system, the starting point for the initial assessment is 4 hours.</p> <p>ISO 27001 certification with a relevant scope is a prerequisite under this scheme. If the service provider holds other CCV cybersecurity certificates or other relevant certificates that justify a less extensive assessment of the quality system the audit duration can be reduced to 3 hours as a minimum at initial assessment.</p> <p>The number of hours can also be increased if it concerns a service provider that carries out many monitoring 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.</p> <p>Full reporting (on quality system + service-oriented control<sup>10</sup>) takes 4 hours.</p> <p>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.</p>

<sup>10</sup> For time indicated for service orientated assessment, see table B.

**A. INITIAL ASSESSMENT AUDIT**

	The certification body shall provide 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 will be assessed during the service-specific assessment.
Evaluation of monitoring service	<p>The implementation of monitoring is evaluated against all requirements from the relevant section in chapter 2. Assessment of monitoring consists of:</p> <ul style="list-style-type: none"> <li>■ assessing at least two different project files, to be selected by the certification body. Including verification of the periodic reports;</li> <li>■ monitoring the implementation of monitoring and assessing whether it is carried out in accordance with chapter 2, possibly requesting clarification and explanation.</li> </ul> <p>In case of multi-site assessment, this applies to the main site. Per additional branch, one project is selected for file review and a project is assessed while it is executed.</p> <p>The indicative time per monitoring <i>file</i> is 2 hours.</p> <p>In addition, for assessing during monitoring in <i>progress</i>, 2 hours is indicated.</p> <p>For monitoring the implementation of monitoring, the following principles apply:</p> <ol style="list-style-type: none"> <li>1. The certification body asks one or two analysts/ employees of the service provider about the process followed in two monitoring projects.</li> <li>2. The certification body is present during the implementation of at least one project.</li> <li>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 periodic reports are assessed.</li> <li>4. When asking questions about the two projects of which the 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.</li> </ol> <ul style="list-style-type: none"> <li>■ What was the input /assignment/briefing/scope?</li> <li>■ How is the team composed and who is in charge?</li> <li>■ What are the do's and don'ts regarding the project?</li> <li>■ What choices were subsequently made?</li> </ul>

B INITIAL ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)	
	<ul style="list-style-type: none"> <li>■ Which tooling is/will be used for this particular client, why, and how was this/were these useful for correctly delivering the assigned service?</li> <li>■ What manual interpretations have been performed?</li> <li>■ Where are the reports located?</li> <li>■ Who checked this?</li> <li>■ How is the customer involved in the process?</li> <li>■ How did the final reports come about?</li> <li>■ Has there been a final review?</li> </ul>
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, monitoring 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 <https://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 monitoring 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.

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

A. PERIODIC ASSESSMENT – AUDIT	
Quality system assessment	<p>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.</p> <p>Preparation for the entire assessment takes 2 hours.</p> <p>Regarding the assessment of the quality system, the starting point for the periodic assessment is 3 hours.</p> <p>If the service provider already has CCV cyber security or other relevant certificates that justify a less extensive assessment of the quality system, this can be reduced to a minimum of 2 hours at periodic assessment.</p> <p>The number of hours can also be increased if it concerns an organisation that carries out many monitoring assignments, 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.</p> <p>Full reporting (on quality system + service-oriented control<sup>11</sup>) takes 4 hours.</p> <p>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.</p> <p>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.</p>

B. PERIODIC ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)	
Technical facilities	The use of tooling is assessed during the service-specific assessment.

<sup>11</sup> For time indicated for service orientated assessment, see table B.

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

Evaluation of monitoring service

The implementation of monitoring is evaluated against all requirements from the relevant section in chapter 2. Assessment of monitoring 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 monitoring service and assessing whether it is carried out in accordance with chapter 2, possibly requesting clarification and explanation.

2 hours are indicated for each project *file* to be examined, for sample sizes of three files per year. In addition, for the fourth and each subsequent file, a time allocation of 1 hour per file applies.

In addition, for assessing during monitoring *in progress*, 2 hours is indicated.

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

NUMBER OF MONITORING PROJECTS	NUMBER OF PROJECT FILES FOR ASSESMENT
0	<sup>12</sup>
1 or 2	1
3 to 15	2
16 to 50	3
51 to 100	5
101 to 200	7
201 to 400	9
401 and more	11

<sup>12</sup> 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.

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

	<p>The service provider provides a list of all executed monitoring projects. The certification body determines the sample.</p> <p>The monitoring services for at least 95% of the clients of the service provider must be transparent and accessible to the certification body. Projects for specific clients 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.</p> <p>The sample will be divided as much as possible (spread over types monitoring assignments, analysts, clients). The sample can also be 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 monitoring provided.</p> <p>In case of multi-site assessment, the total sample size is determined based on the number of projects delivered by the entire organisation. The certification body ensures that every site is part of the selection of projects.</p> <p>For monitoring the implementation of monitoring the following principles apply:</p> <ol style="list-style-type: none"> <li>1. The certification body asks one or two analysts/ employees of the service provider about the process followed in two projects.</li> <li>2. The certification body is present during the implementation of at least one project.</li> <li>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 periodic reports are assessed.</li> <li>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.</li> </ol> <ul style="list-style-type: none"> <li>■ What was the input /assignment/briefing/scope?</li> <li>■ How is the team composed and who is in charge?</li> <li>■ What are the do's and don'ts regarding the project?</li> <li>■ What choices were subsequently made?</li> <li>■ Which tooling is/will be used for this particular client, why, and how was this/were these useful for correctly delivering the assigned service?</li> <li>■ What manual interpretations have been performed?</li> <li>■ Where are the reports located?</li> <li>■ Who checked this?</li> <li>■ How is the customer involved in this process?</li> <li>■ How did the final report come about?</li> </ul>
--	--

B. PERIODIC ASSESSMENT - SERVICE ORIENTED ASSESSMENT (PER BRANCH)	
	<ul style="list-style-type: none"> <li>■ Has there been a final review?</li> </ul>
File	<p>The project file of the reviewed monitoring project (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).</p> <p>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 interim assessments if desired.</p>

#### 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.

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 based 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 monitoring 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 that 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 monitoring 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 monitoring service supplied under certificate does not meet the requirements set, because:

- dangerous or unsafe situations (may) arise, or
- the digital system on which the monitoring 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 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 nonconformity. This analysis shall in any case (but not be limited to) include the possible causes in the process of producing the monitoring service and the possible causes in the failure of control processes;
- the actions to be taken immediately to prevent further non-compliant monitoring services from being delivered with the certification mark;
- An analysis focused on the monitoring service 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 monitoring 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 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 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<sup>13</sup>, 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 doubt about the quality assurance of the monitoring 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 – Service

- The monitoring 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 monitoring service 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 nonconformity. This analysis shall in any case (but not be limited to) include the possible causes in the process of producing the monitoring service and the possible causes in the failure of control processes;
- an analysis focused on the scope of monitoring 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 monitoring services that do not meet the requirements;
- solutions aimed at preventing recurrence and securing them;

---

<sup>13</sup> This three-month period is the same for major nonconformities as for minor nonconformities (see section 4.8.6). If there is a suspension, it is recommended that the assessment of nonconformities 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 nonconformity (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 nonconformities have not led to the elimination of the nonconformity(/ies) 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 monitoring services for a period of two 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 <https://hetccv.nl/schorsingen/>. From the moment of suspension, the service provider is no longer allowed to use the certification mark. Nor is the service provider allowed to refer to the certified status of the monitoring service to be delivered. The service provider remains responsible for remedying defects in the monitoring 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 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 is 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 monitoring service to be delivered. The certification body removes the data of the service provider from the certification scheme concerned on <https://hetccv.nl/companies>.

The service provider remains responsible for remedying defects in the monitoring 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 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 clients that the certification body has justified confidence that the service provider who delivers cyber security monitoring services 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 logo shown below is attached to this certification scheme.



Figure 3 Example of a certification mark

The certification mark affixed to monitoring reports indicates legitimate confidence in the quality of the monitoring.

#### 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.

Illustrative use on letterheads, website, folders and other publicity material with references to the certification scheme by the *service provider* is permitted under certain conditions.<sup>14</sup>

The service provider places the certification mark on (periodic) monitoring reports, see section 5.3. This use of the mark is mandatory.

In addition, for both certification bodies and service providers, the *CCV Reglement Kwaliteitslogo*, as published at <https://hetccv.nl/> applies.

## 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 cyber security monitoring services".

The service certificate contains at least the following data<sup>15</sup>:

- 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 monitoring service carried out by the service provider, including reporting to the client, complies with the requirements set out in the CCV certification scheme – Cyber Security – Monitoring, version <number>."*

*"<Certification body> licenses the certification mark shown here to <the service provider> for monitoring services 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:

*"Monitoring providers and third parties can check the status of a valid service certificate with <certification body> or on <reference to <https://hetccv.nl/companies>> "*

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

## 5.3 Periodic reports with certification mark

The service provider provides periodic reports for its clients with the certification mark.

---

<sup>14</sup> "See CCV Reglement Kwaliteitslogo", as published at [www.hetCCV.nl](http://www.hetCCV.nl).

The service provider shall place the mark on the definitive version of the report for the client. The layout of the document is such that it is clear that it concerns findings from cyber security monitoring. The report explicitly states that the certification mark is about the quality of the monitoring service, not that of the monitored object or environment.

The service provider is not allowed to place the mark of the certification body on its monitoring reports.

## 6 References

### 6.1 Terms and abbreviations

Assessment	Implementation of this certification scheme by the certification body at the service provider of the monitoring service.
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 monitoring 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 / Client	Person or organisation that purchases the monitoring service and orders the service provider to carry out the monitoring.
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.
Monitoring Professional	A person directly involved in performing or validating cybersecurity monitoring activities, such as detection analysis, triage, use case maintenance or reporting, under the scope of the certified monitoring service. This includes analysts, engineers and other staff whose work directly affects the quality and reliability of monitoring outcomes.
NEN	Foundation Royal Dutch Standardisation Institute. The NEN publishes the Dutch standards.

Periodic assessment	Assessment aimed at confirmation that the requirements and conditions are still met, thereby maintaining certification.
Standard	Document in which the parties involved set down agreements with the aim of keeping to them.
Service certificate	Document prepared by the certification body, listing the service provider as the supplier of the certified monitoring service.
Service-oriented assessment	Assessment of the monitoring service by the certification body, including monitoring reports.
Service provider	The organisation providing the monitoring service.
Security monitoring	The continuous monitoring of a computer or digital infrastructure with the aim of detecting suspicious and/or anomalous events or patterns which could harm the business of the organisation.
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 the monitoring service.
VOG	Verklaring Omtrent Gedrag, Certificate of Conduct.

## 6.2 Standards and references

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

STANDARD	TOPIC	AVAILABLE
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
NIST SP 800-61r3	Incident response recommendations and considerations for cybersecurity risk management	National Institute of Standards and Technology, US Department of Commerce
CCV Reglement Kwaliteitslogo*	CCV rules quality mark	CCV, Utrecht



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

T (030) 751 6700  
E [info@hetccv.nl](mailto:info@hetccv.nl)  
I [www.hetccv.nl](http://www.hetccv.nl)

