CERCOMS

Certification & Compliance Services

Certification Scheme

Generic for: ISO 27001 | NEN 7510 | ISO 9001

Document History

Version	Description	Status	By	Date	Changes
0.1	Initial document	Draft	Quartermaster	2025-01	
	Update	Draft	Quartermaster	2025-03	NCS 7510:2025 Ref. to def. document
1.0	Update	Final	Quartermaster	2025-03	
1.1	Update	Final	Operations Manager	2025-10	CIR58

Document Owner

Compliance Manager

Reference documents

IAF MD 25:2023 Issue 1, Version 2 – Criteria for evaluation of conformity assessment schemes
RvA-T033-NL versie 5, 20-02-2018
ISO 17021-1:2015
ISO 17021-3:2018
ISO 17030:2021
ISO 27006-1
NCS 7510:2018
NCS 7510:2025

For an overview of definitions included in standards, see CERCOMS Definitions (from the standards). CERCOMS Definitions (from the standards) is not consistently referred to in the text of this document

Contents

Introduction

This document, CERCOMS generic certification scheme, includes the process steps, requirements and guidelines for organisations seeking certification to ISO 27001, NEN 7510-1, and/or ISO 9001.

NEN 7510-1 certification is based on ISO 27001 and extended with specific healthcare sector requirements.

Definition: Certification scheme

Conformity assessment system related to management systems to which the same specified requirements, specific rules and procedures apply. (ISO 17021-1:2015 / 3.15)

Purpose and scope of the certification scheme

To explain the standardized processes for certification, audits, and competence management.
To demonstrate impartiality and credibility of CERCOMS management system certifications.

This scheme covers (references to) audit methodology, competence of personnel, decision-making processes, and more.

Certification Process

Application review

An application for certification will be reviewed. Assessments will include whether the applicant operates in an economic sector in which CERCOMS can carry out audits and whether CERCOMS can carry out the certification activities impartially.

The certification body shall require an authorized representative of the applicant organization to provide the necessary information to enable it to establish the following:

a) the desired scope of the certification;
b) relevant details of the applicant organization as required by the specific certification scheme, including its name and the address(es) of its site(s), its processes and operations, human and technical resources, functions, relationships and any relevant legal obligations;
c) identification of outsourced processes used by the organization that will affect conformity to requirements;
d) the standards or other requirements for which the applicant organization is seeking certification;
e) whether consultancy relating to the management system to be certified has been provided and, if so, by whom.

Reference documents:

- *CERCOMS Handbook General Principles*
- *CERCOMS Application for Certification*.

Proposal / Contract

If the certification services can be provided to the applicant, a proposal will be prepared. This proposal includes a commercial offer, conditions regarding, among other things, the use of logos and a reference to CERCOMS Algemene Voorwaarden (GT&C).

The commercial proposal will be specified for the 3-year audit cycle: initial audits (stage 1 and stage 2) in the first year and surveillance audits in the second and third year. The specification includes the number of calculated audit days per audit, any additional activities and the rates.

It also provides substantiated information on whether the calculation of the standard number of audit days has been adjusted upwards or downwards and on the basis of which criteria this was done. A calculation file is created for each applicant.

Multi-site audits, integrated management system audits and data centre audits are specified and explained.

The mutually signed proposal constitutes the contract between the parties.

Reference documents:
- ISO 17021-1;
- ISO 17030;
- ISO 17032;
- *CERCOMS Voorstel certificering [norm] 20xx-xx-xx template*
- *CERCOMS Algemene Voorwaarden (GT&C)*
- *CERCOMS Handbook Certification Issuing*
- *CERCOMS Process Audit Time Determination*
- *CERCOMS Process Multi-site Sampling*
- *CERCOMS Audit Time Calculator*

Stage 1 audit

During the stage 1 audit CERCOMS conducts a document review to check management system compliance. Key elements to be reviewed: policies & objectives, processes, internal audit & management review records, and risk & opportunity assessment.

Gaps in documentation and readiness for certification will be identified and recommendations for corrective actions will be provided. The findings are reported in writing.

Reference documents:
- ISO 19011
- *CERCOMS Handbook Certification Issuing*
- *CERCOMS Audit Report - template*

Stage 2 audit

Based on the established audit programme, a detailed schedule is drawn up for the stage 2 audit.

During this on-site audit CERCOMS assesses the implementation and effectiveness of the management system. The audit includes interviews with key personnel, records review, and process observation.
Major and minor non-conformities will be identified. The findings are reported in writing.

Reference documents:
- ISO 19011
- *CERCOMS Handbook Certification Issuing*
- *CERCOMS Audit Report - template*

Certification decision

Certification decision will be made by a competent and independent professional; the Manager Business Unit Certification Issuing or the Compliance Manager.

If non-conformities exist, the client must provide corrective actions within a defined timeframe.
If major non-conformities exist, a follow-up audit is required within 3 months before certification.

Upon successful audit, CERCOMS issues a certificate valid for 3 years.

The certificate will be issued and the relevant details will be communicated to Accreditation Body Raad voor Accreditatie, as set out in the contract.

Reference documents:
- *CERCOMS Handbook Certification Issuing;*
- *CERCOMS Process Review Certification Decision;*
- *CERCOMS Certification Issuance Policy;*
- *CERCOMS Handbook Business Office;*
- *CERCOMS Certificate template*.

Surveillance audits

Based on the established audit programme, a detailed schedule is drawn up for the surveillance audits.

These audits will be conducted annually to verify continued compliance. With a focus on key processes, corrective actions, and improvement initiatives.
It also discusses whether the number of FTEs involved in carrying out the activities within scope should be adjusted.
Major and minor non-conformities will be identified. The findings are reported in writing.

Toevoeging voor NEN 7510:
Focus op de zorgspecifieke maatregelen zoals het beheer van patiëntgegevens.

If non-conformities exist, the client must provide corrective actions within a defined timeframe.
If major non-conformities exist, a follow-up audit is required within 3 months.
Failure to maintain compliance can result in suspension of certification.

Reference documents:
- ISO 19011
- *CERCOMS Handbook Certification Issuing*
- *CERCOMS Audit Report – template.*

Recertification audit

Conducted every 3 years before certificate expiration. Includes a full system audit to ensure sustained compliance (comparable with the stage 2 audit).

A new proposal and audit programme will be prepared for the new cycle.
The new cycle will consist of a recertification audit and two surveillance audit. See also the specifications described for the stage 2 and the surveillance audits.

Reference documents:
- *CERCOMS Voorstel certificering [norm] 20xx-xx-xx template;*
- *CERCOMS Algemene Voorwaarden (GT&C);*
- *CERCOMS Handbook Certification Issuing;*
- *CERCOMS Certification Issuance Policy;*
- *CERCOMS Process Audit Time Determination;*
- *CERCOMS Process Multi-site Sampling;*
- *CERCOMS Audit Time Calculator.*

Multiple management systems

The ISMS audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to a Management System shall appear clearly and be readily identifiable in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits.
Where an organization has integrated the requirements of two or more management system standards into a single management system, the relevant requirements described in CERCOMS management system documentation may apply.

Transfer

Procedures for transfer audit are included in *CERCOMS Certification Issuance Policy.*

Scope extension and reduction

Procedures for transfer audit are included in *CERCOMS Certification Issuance Policy.*

Reports

Audit reports are reviewed by an independent reviewer before being handed over to the customer.
De rapporten worden opgesteld aan de hand van een template.

Reference documents:

- ISO 17021-1;
- *CERCOMS Handbook Certification Issuing*
- *CERCOMS Audit Report – template.*

Competence Requirements for Auditors / Audit teams

Standards that mandates CERCOMS must ensure auditor competency and impartiality:

- ISO 17021-1;
- ISO 17021-3;
- ISO 27006-1;
- NCS 7510.

Auditor qualifications

Audits are conducted exclusively by CERCOMS qualified auditors. This means, among other things, that the auditor holds a recognised Lead Auditor training certificate, has in-depth knowledge of the relevant standards, attends the Continual Professional Development Programme, meets the practice requirements set for an auditor and has gained knowledge of the relevant industry and customer's business processes. Additional requirements apply to a lead auditor.

If the audit is conducted by a team of auditors, the necessary knowledge will be present within the team.

Auditors are evaluated annually. Performance and customer feedback are included.

Reference documents:

- ISO 17021-1;
- ISO 17021-3;
- ISO 27006-1;
- NCS 7510;
- *CERCOMS Handbook Governance*;
- *CERCOMS Handbook Certification Issuing*;
- *CERCOMS Handbook Business Office*;
- *CERCOMS Selecting and Evaluating Auditors – template*;
- *CERCOMS Continual Professional Development Programme*.

Continual Professional Development Programme (CPD)

CERCOMS qualified auditors must attend the CPD programme, and will be evaluated yearly.

Internal trainings are available to gain competencies, the personal attributes or behaviours which result in effective or superior performance in a job.

To gain competences, external trainings will be attended as much as possible at recognised training institutes, such as the Security Academy in the Netherlands.

Reference documents:

- ISO 17021-1;
- ISO 17021-3;
- ISO 27006-1;
- NCS 7510
- *CERCOMS Handbook Governance*;
- *CERCOMS Handbook Business Office*;
- *CERCOMS Selecting and Evaluating Auditors – template*;
- *CERCOMS Continual Professional Development Programme*.

Conflict of Interest Management

CERCOMS pays close attention to auditor independence and conflict of interest.

This means, among other things, that auditors are not allowed to perform audits for a certain period of time if they have carried out consultancy work on the management system at the organisation concerned, certification decisions must be made by independent personnel and complaint handling can only be carried out by independent persons (externally hired if necessary).

Reference documents:
- ISO 17021-1;
- *CERCOMS Handbook Governance*;
- *CERCOMS Handbook Business Office*;
- *CERCOMS Selecting and Evaluating Auditors – template*;
- *CERCOMS Process Complaints and Appeals Management*.

Management system Requirements & Compliance

Organisations must demonstrate compliance with the relevant standard, including the following components:

Leadership & planning

Top management must be actively involved in management system implementation & review.

Policies (ISMS, QMS) & objectives must be established, communicated and maintained.

Process approach & risk-based thinking

Organizations must define and document core processes, must conduct risk assessments to identify and mitigate related risks and must implement risk mitigation strategies for threats.
NEN 7510-1 certification requires focusing on a risk assessment on patient data and IT systems.
ISO 9001 certification requires focusing on high, medium and low risk activities.

Customer focus & continual improvement

Monitor customer satisfaction & feedback mechanisms. This section applies specifically to a QMS.

Implement corrective actions & performance improvement plans.

Access control & data protection

Strong authentication mechanisms, e.g. MFA, role-based access controls and encryption of sensitive data at rest and in transit are required.

NEN 7510-1 certification requires focusing on logging & monitoring of access to patient records.

Incident response & business continuity

Procedures for incident response and testing.
Procedures for data breaches.

Business continuity plan, including disaster recovery plans, shall be available.
Backup restore tests and DRP tests shall be performed according to a test plan.

Impartiality & Independence

CERCOMS pays close attention to impartiality and independence. Hierbij wordt voldaan aan de voorwaarden van relevante normen en regelgevingen.

This means, among other things, that auditors are not allowed to perform audits for a certain period of time if they have carried out consultancy work on the management system at the organisation concerned, certification decisions must be made by independent personnel and complaint handling can only be carried out by independent persons (externally hired if necessary).

Certification decisions are free from financial or commercial influence.

The risk analysis includes potential impartiality risks.

Reference documents:
- ISO 17021-1;
- ISO 17021-3;
- NCS 7510;
- Relevant IAF documentation;
- *CERCOMS Handbook Governance*;
- *CERCOMS Handbook Business Office*;
- *CERCOMS Selecting and Evaluating Auditors – template*;
- *CERCOMS Process Complaints and Appeals Management*;
- *CERCOMS Process Review Certification Decision*;
- *CERCOMS Risk Identification Analysis and Treatment*.

Complaints & Appeals Process

All complaints and appeals are handled zoals beschreven in het process, respecting the timelines described. The independence of practitioners is guaranteed herein.

Reference documents:
- ISO 17021-1;
- NCS 7510;
- *CERCOMS Handbook Business Office*;
- *CERCOMS Process Complaints and Appeals Management*.

Accreditation & Oversight

CERCOMS is accredited by Accreditation Body Raad voor Accreditatie to issue certificates, as a Certification Body, for ISO 27001, NEN 7510 and ISO 9001.

CERCOMS is regularly assessed by Raad voor Accreditatie to ensure CERCOMS compliancy with compliance with ISO 17021-1, ISO 17021-3, ISO 27006-1 and NCS 7510. Non-compliance may result in suspension or withdrawal of accreditation.

Van de uitwisseling van gegevens met Raad voor Accreditatie is melding gemaakt in het contract met de klanten.

Reference documents:
- ISO 17021-1;
- ISO 17021-3;
- ISO 27006-1;
- NCS 7510;
- RvA-SAP-C000-NL;
- RvA-SAP-C010-UK;
- RvA-T040-NL v3, Schaduwonderzoeken
- *CERCOMS Voorstel certificering [norm] 20xx-xx-xx.*

Certification Mark & Public register

Organizations awarded certification can use CERCOMS relevant **certification mark**.

Certification status is publicly available on CERCOMS online register.

The use of this the certification logo and entry in the register are included in the contract.

Reference documents:
- ISO 17021-1;
- ISO 17030;
- NCS 7510;
- *CERCOMS Voorstel certificering [norm] 20xx-xx-xx;*
- *CERCOMS Certificate Register.*

Annex: Requirements certification schemes

ISO 17021-1:2015

9.1.1 Application

The certification body shall require an authorized representative of the applicant organization to provide the necessary information to enable it to establish the following:

a) the desired scope of the certification;
b) relevant details of the applicant organization as required by the specific certification scheme, including its name and the address(es) of its site(s), its processes and operations, human and technical resources, functions, relationships and any relevant legal obligations;
c) identification of outsourced processes used by the organization that will affect conformity to requirements;
d) the standards or other requirements for which the applicant organization is seeking certification;
e) whether consultancy relating to the management system to be certified has been provided and, if so, by whom.

IAF MD25:2023

CERCOMS has reviewed the following requirements for a CAS (Conformity Assessment Scheme), regarding the completeness of its own certification schemes.

Requirements for the Scheme owner

Art.	Requirement	Implementation CERCOMS
3.2	The SO shall make a general description of the CAS publicly available without request. The scheme documents, including the criteria and process to be used in assessing conformity shall be publicly available.	CERCOMS Certification Scheme is available on request. The website will provide information of the processes.
3.3	The SO should demonstrate that the CAS has been validated. The validation should be documented and include the following aspects: i. A description of the purpose of the CAS; ii. A description of the requirements of the CAS; iii. An analysis of the appropriateness of the established requirements for fulfilling the defined purpose of the CAS; iv. A description of the methods to be used for determining fulfilment of the requirements; v. An analysis showing that the described methods to be used for determining fulfilment of the requirements are appropriate; vi. The decision on the conformity assessment activity to be used (including identification of the applicable conformity assessment standard); and vii. An analysis showing that the selected conformity assessment activity is appropriate.	All components included.
3.6	The SO shall have a procedure for dealing with complaints relating to the CAS, ensuring that complaints processes of CABs' clients, CABs and ABs are not affected. Investigation and decision on complaints shall not result in any discriminatory actions	CERCOMS Process Complaints and Appeals
3.9	The SO should have a process for a periodic review of the CAS taking into account the experience gained and the feedback received from parties interested in the CAS.	CERCOMS Operational Plan

Requirements for a CAS

Art.	Requirement	Implementation CERCOMS
4.1	The CAS should cover the following elements: i. Selection of the object(s) of conformity assessment, including selecting specified requirements to be assessed and planning information collection and sampling activities; ii. Determination, including the use of one or more determination methods (e.g. test, audit and/or examination) to develop complete information regarding fulfilment of the specified requirements by the object of conformity assessment or its sample; iii. Review, decision and attestation, including the review of evidence from the determination stage. Conclusion based on the results of the review as to whether fulfilment of specified requirements has been demonstrated and a subsequent attestation that the object of conformity assessment has been reliably demonstrated to fulfil the specified requirements, and any subsequent marking or licensing and their related controls, where applicable; and iv. iv) Surveillance and recertification, as applicable, systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity.	Included in the handbooks
4.2	A CAS shall include the following: i. The objectives of the scheme for the specific industry or user group; ii. The object of conformity assessment, e.g. product or process or person or claim; iii. The requirements against which conformity is to be assessed; iv. The conformity assessment process used in order to determine conformity of the object. This process shall fall under the scope of one of the IAF MLA Level 3 standards without any contradictions or exclusions; v. Any specific applications or explanations of ISO/IEC 17011 (e.g. specific competence criteria for assessors/technical experts/assessment teams, assessment criteria, specific details in the assessment reports), if applicable; and vi. Any specific application or explanation of accreditation standard at Level 3, e.g. ISO/IEC 17021-1, ISO/IEC 17065, ISO/IEC 17024/ ISO/IEC 17029 (e.g. specific competence criteria for auditors/evaluators/inspectors/technical experts/audit teams, audit/evaluation/inspection criteria, specific details in the audit/evaluation/inspection reports), if applicable.	Included in this document
4.6	The CAS should describe the method used to monitor that the certificate or attestation or statement holder continues to comply with the requirements, if applicable.	Included in this document and in CERCOMS Handbook certification Issuing
4.9	Where the CAS provides for the use of certificates, marks or other statements of conformity, there should be a license and/or rules or another form of enforceable agreement to control such use. Licenses can include provisions relating to the use of the certificate, mark or other statement of conformity in communications about the object of conformity assessment, and requirements to be fulfilled when the certification is no longer valid.	CERCOMS Voorstel certificering [norm]

Beoordeling eigen schema – indienen bij aanvraag accreditatie (RvA-T033-NL v5, 2018)

Dit toelichtend document (RvA-T033, verder T033 genoemd) beschrijft de criteria die relevant zijn voor een eigen beoordeling van een schema. In het proces van het beoordelen van een aanvraag voor (uitbreiding van) accreditatie (zie RvA-BR002) evalueert de RvA vervolgens het schema op basis van de door de CBI verstrekte gegevens. Deze evaluatie moet antwoord geven op de vraag of de CBI die het schema gebruikt hiermee aan de accreditatievereisten kan voldoen.

De werkwijze bij het evalueren van schema's door de RvA is uiteengezet in beleidsregel RvA-BR012.

Art. T033		Implementatie CERCOMS
2.1	Schema voor conformiteitsbeoordeling Onder een conformiteitsbeoordelingsschema wordt verstaan een gedocumenteerd en publiek verkrijgbare set aan eisen die het volgende regelen:	
	1. het wat van de conformiteitsbeoordeling in de vorm van: • identificatie van het onderwerp van de conformiteitsbeoordeling, zoals product, proces, dienst, systeem, competentie van een persoon, installatie, monster, partij of (emissie-) gegevens; • de vastgelegde eisen2, inclusief eventuele interpretaties daarvan, waartegen de toetsing van het onderwerp plaatsvindt, zoals de certificatienorm, product-, systeemof processpecificaties, wettelijke eisen, officiële norm3, andere normatieve documenten, klantenspecificaties, branchenormen, etc. Eisen zijn beschreven op een heldere, directe en nauwkeurige wijze en resulteren in een nauwkeurige en uniforme interpretatie, zodat partijen die gebruik maken van het schema aan de inhoud van het document een gemeenschappelijk begrip van de betekenis en opzet ervan kunnen afleiden. Eisen worden geschreven in termen van resultaten of uitkomsten, samen met grenswaarden en toleranties, indien relevant. Eisen worden ondubbelzinnig beschreven, met gebruik van woorden die objectief, logisch, valide en specifiek zijn;	
	2. het hoe van de conformiteitsbeoordeling, inhoudende: • de wijze waarop de CBI de conformiteit vaststelt. Hierbij worden de termen gebruikt zoals beschreven in EN ISO/IEC 17011 (testen, inspectie, audit, certificatie etc.). Het schema bevat ook een uitwerking van de methoden en procedures voor deze activiteiten, zoals audit- of verificatiemethode, keuringsprotocol, test- of onderzoeksmethode, inspectievoorschrift, of examenmethode, en de daarbij benodigde proces- of procedurebeschrijvingen; • indien van toepassing de wijze waarop toezicht door de CBI plaatsvindt in termen van bijvoorbeeld controlefrequenties en inhoud en omvang van controles en van hercertificatie;	
	3. het wie, waarmee de soort CBI wordt bedoeld die de conformiteitsbeoordelingsactiviteiten uitvoert, in de vorm van: • benoeming van de soort CBI in de vorm van bijvoorbeeld: testlaboratorium, inspectieinstelling of certificatie-instelling; • de eisen die op de CBI van toepassing zijn, en eventuele specifieke toepassingsregels of interpretaties daarvan; • de eventuele aanvullende eisen, bijvoorbeeld uit wetgeving of branchespecifieke eisen;	

	• eventuele specifieke toepassingsregels of interpretaties van EN ISO/IEC 17011.	

Ten behoeve van het vaststellen of een eigen beoordeling van het schema met behulp van T033 van belang is voor de accreditatie-aanvraag onderscheidt de RvA drie typen schema's, w.o.:

eigen schema

- Bij ISO/IEC 17021-1 wordt T033 gebruikt, tenzij […]. Dus T033 wordt bijvoorbeeld niet toegepast bij certificatie tegen ISO 9001 waarvoor IAF onder andere mandatory documents gepubliceerd heeft.