# BCI Chain of Custody Standard Version Transition Document for Certification Bodies

## Title

BCI Chain of Custody Standard Version Transition Document for Certification Bodies

## Translation Accuracy

The official language of this document is English. In case of any inconsistency between versions due to translation, please refer to the English version. While translations to other languages may be provided, BCI assumes no liability for errors or misunderstandings due to translation.

## Disclaimer

The Better Cotton Initiative reserves the right to revise documents based on implementation, learnings and emerging good practice. Please visit https://bettercotton.org/document-library/ to verify that this document is the most recent version.

## Any Questions or Inputs?

Contact us at compliance@bettercotton.org

# Table of Contents

# About

The requirements set out in this document aim to provide consistent understanding and application of version transition across the Chain of Custody programme. This document shall be used in conjunction with the BCI Chain of Custody Monitoring and Certification Requirements.

## Introduction

BCI may publish revised versions of the BCI Chain of Custody Standard (CoC Standard) and associated normative documents as the programme develops. When a new version is published, it is important that all audits are conducted against a consistent version of the standard.

Without a defined transition approach, there is a risk of:

- Inconsistent audit application between Certification Bodies
- Supply chain organisations operating under outdated requirements for extended periods due to audit cycling

This document clarifies how standard version applicability is determined, how Certification Bodies shall manage the transition in practice, and how certification documentation shall be updated when a transition takes effect.

**Key principle:** The applicable version of the CoC Standard is determined by the audit start date relative to the defined transition deadline, not by the type of audit being conducted. The version of the CoC Standard referenced on the scope certificate is determined separately, in accordance with the audit type requirements set out in Section 3.

This document includes several audit types that fall within the broader category of surveillance audits. These include risk-triggered surveillance audits, NC-triggered surveillance audits, Multi-Site Scenario B annual surveillance audits, and scope extension audits. The requirements in this document apply across all surveillance audit types unless otherwise specified.

# 1. Key Transition Dates

The table below sets out the transition dates applicable to the move from CoC Standard v1.2:

| Version | Published | Status |
|---|---|---|
| CoC Standard v1.0 | 10 May 2023 | Superseded |
| CoC Standard v1.1 | 03 February 2025 | Published but never mandatory for all organisations – superseded by v1.2 before fully effective date |
| CoC Standard v1.2 | 06 January 2026 | **Current version — mandatory for all audits from January 2026** |

What this means in practice:

CoC Standard v1.1 was published in February 2025 with an intended effective date of January 2026. Prior to that effective date, a non-substantive revision was made to remove a single requirement that affected the scheme's alignment with ISO/IEC 17065. This revision was published as v1.2 in January 2026.

The applicable rule is therefore:

- All audits starting **before 06 January 2026** shall be conducted against CoC Standard v1.0/v1.1 depending on whether it was a Supplier/Manufacturer audit or a Brand audit
- Audits starting **on or after 06 January 2026** shall be conducted against CoC Standard v1.2

**Note**: The revision from v1.1 to v1.2 was non-substantive. The sole change was the removal of a membership requirement to ensure alignment with ISO/IEC 17065. No new requirements were introduced.

| Field | Information |
|---|---|
| **Document Title:** | BCI Chain of Custody Standard Version Transition Document for Certification Bodies |
| **Document ID:** | QMS_CB_PO_ 263_BCI Chain of Custody Standard Version Transition Document for Certification Bodies _v1.0 |
| **Document Type:** | Policy |
| **Standard/ Scope** | Chain of Custody Standard |
| **Work stream, team and function:** | Certification Body Management, Assurance |
| **Document Owner:** | Senior Assurance Coordinator |
| **Next Review Date:** | TBC |
| **Status:** | Active |

| Version | Date | Description of Change | Author / Editor |
|---|---|---|---|
| **1.0** | 24 March 2026 | Initial issue | Senior Assurance Coordinator |

# 2. Requirements for Certification Bodies (CBs)

| 2.1 | |
|---|---|
| From 06 January 2026, Certification Bodies shall audit their clients against CoC Standard v1.2 at the next scheduled audit, regardless of the type of audit being conducted (e.g. initial audit or surveillance audit). | **Guidance**: The applicable version of the CoC Standard is determined by the audit start date. Where an audit commenced prior to 06 January 2026, the version applicable at the time of the opening meeting shall apply for the duration of the audit process. |
| **2.2** | |
| Certification Bodies shall communicate the version of the standard to be applied at the audit to their clients in advance of the audit date. | **Guidance:** This should be done as part of pre-audit communications. As a minimum, the communication should include confirmation that v1.2 will be applied at the upcoming audit. However, the responsibility for implementing the revised requirements rests with organisation going for the audit. |
| **2.3** | |

| | |
|---|---|
| The Certification Body shall ensure that they use the audit report template that relates to the version of the standard that they are auditing against. | **Guidance**: From 06 January 2026, all audits should use the CoC Standard v1.2 audit report. The templates can be downloaded from the CoC Resource Centre. |
| **2.4** | |
| Where a surveillance audit was triggered by the nonconformity threshold raised under a previous version of the CoC Standard, the Certification Body shall assess the client has effectively implemented corrective actions against the equivalent requirement(s) in CoC Standard v1.2. | **Guidance**: The surveillance trigger is determined by the number of nonconformities raised at the preceding audit and is not affected by a subsequent revision to the standard. |
| **2.5** | |
| Where one or more nonconformities that triggered a surveillance audit related to a requirement that has been removed in CoC Standard v1.2, the Certification Body shall not evaluate conformity against that requirement. | **Guidance**: Where a requirement no longer exists in the current version of the Standard, it cannot form the basis of an ongoing surveillance obligation. |

# 3. Audit Scope and Certificate Update Rules

The following rules clarify how version transition and certificate updates shall be handled across different audit scenarios. Certification Bodies shall determine which scenario applies before planning an audit where a version transition is relevant.

| 3.1 | |
|---|---|
| When conducting annual surveillance audits for Multi-Site Scenario B clients, the Certification Body shall issue an updated scope certificate reflecting the updated version of the Standard. The expiry date on the scope certificate shall remain unchanged and shall only be updated upon completion of a full recertification audit, which occurs on a three-year cycle. | **Guidance**: The Certification Body is only required to issue an updated scope certificate when the audit has been conducted against a different version of the Standard that is listed on the organisation's existing scope certificate. Certification Bodies should carry forward the original expiry date from the initial certification audit but should update the version of the Standard mentioned on the scope certificate.<br><br>The Certification Body should note that annual surveillance audits are a requirement for organisations operating as Suppliers/Manufacturers only and not those operating as Brands/Traders/Sourcing Agents. The Certification Body may refer to Annex B in the BCI Chain of Custody Monitoring and Certification Requirements for further information. |
| **3.2** | |

| | |
|---|---|
| Where a surveillance audit is triggered, the Certification Body shall not update the standard version referenced on the existing certificate. This requirement applies to all surveillance audits with the exception of Multi-Site Scenario B annual surveillance audits (as outlined in 3.1). The scope certificate shall only be updated to reference a new version of the Standard upon completion of a full recertification audit. | **Guidance**: A surveillance audit verifies ongoing compliance against a subset of requirements only and does not constitute a full evaluation of the organisation's conformity with the standard. |

## Guidance – Table 1

Certification Bodies may use this table as a quick reference when planning audits where version transition may be relevant:

| Audit Scenario | Audit conducted against v1.2 from transition date? | Scope certificate updated to reflect scope change? | Scope certificate updated to reference v1.2? |
|---|---|---|---|
| Risk-triggered surveillance audit | Yes | No | No |
| NC-triggered surveillance | Yes | No | No |
| Multi-site Scenario B annual surveillance audit | Yes | No | Yes - version updated but expiry date unchanged until full recertification |
| Scope extension audit (e.g. additional processes or sites) | Yes | Yes | No – extension added but certificate retains existing standard until full recertification |
| Scope extension but no audit | No – audit n/a | Yes | No – extension added but certificate retains existing standard until full recertification |

# 4. INTACT Requirements

This section sets out how Certification Bodies shall record information into INTACT where a version transition is taking place. The purpose is to ensure that the v1.2 checklist is applied correctly and that the audit record accurately reflects which sites were assessed in a given cycle.

| 4.1 | |
|---|---|
| Where a surveillance audit is conducted against CoC Standard v1.2, the Certification Body shall create a new Audit Order (AO) in INTACT and record all audit findings against the v1.2 checklist. The AO shall only be updated to reflect a change to the organisation's certification status or scope certificate where the outcome of the audit requires it (see Table 1). | **Guidance**: A new AO must be created to ensure the correct v1.2 checklist is applied, as this is only available within a newly created AO. The Certification Body shall select the AO type that corresponds to the audit being conducted. Where the audit outcome does not require a change to the organisation's certification status or scope certificate, the AO may be closed without uploading an updated certificate. |
| **4.2** | |

| | |
|---|---|
| Where the outcome of an audit requires an updated scope certificate to be issued, the Certification Body shall upload the updated certificate in INTACT. | **Guidance**: The Certification Body may refer to Table 1 for more guidance. |