



RESPONSIBLE
JEWELLERY
COUNCIL

RJC CERTIFICATION PROCESS REQUIREMENTS FOR CERTIFICATION BODIES AND AUDITORS

V1.0 FEBRUARY 2025

CONTENTS

INTRODUCTION	2
A. About This Document	2
B. Status and Effective Date	2
C. Key Terms and Definitions	4
D. Purpose of This Document	5
E. Additional Supporting Documents	6
RJC CERTIFICATION PROCESS REQUIREMENTS	7
General – The RJC Standards	7
Overview of the RJC Certification Process	8
STEP 1 – PRE-CERTIFICATION ACTIVITIES	9
1. Application	9
2. Application Review	11
3. Certification Scope	13
4. Audit Programme and Audit Types	19
5. Determining Audit Time	22
6. Harmonise Efforts for Responsible Business Practices: Claims of Equivalency with RJC-Recognised Frameworks	27
7. Determining Audit Objectives and Scope	28
8. Multi-Site Sampling	29
9. COC Outsourced Contractors	35
10. Decide on On-Site or Remote Audit Methodology	36
11. Audit Team Selection and Assignment	37
12. Document and Communicate the Audit Plan	41
STEP 2 – EVALUATION	43
13. Initial Certification Evaluation Activities	43
Documentary Review	43
Initial Certification Audit	44
14. Conducting Audits	45
Meet to Open the Audit	45
Communicate During the Audit	45
Collect, Sample and Record Objective Evidence	46
Evaluate Findings	48
Grade Conformity	48
Document Nonconformities	51
Prepare Audit Conclusions	51
Meet to Close the Audit	52
15. Audit Report	54
16. Corrective Action Plans and Evidence – Submission and Verification	55
17. Audit Invalidation	58
STEP 3 – REPORT REVIEW AND CERTIFICATION DECISION	60
18. Technical Review	60
19. Certification Decision	61
20. Communication of Audit Report and Certification Decision	62
STEP 4 – CERTIFICATION	64
21. Certification Documentation	64
STEP 5 – SURVEILLANCE	66
22. Surveillance Audit Format and Scope	66

DURING THE CERTIFICATION CYCLE	69
23. Recertification	69
24. Semi-Announced Audit Format	70
25. Certification Grace Period	71
26. Transfer of Certification	72
27. Changes Affecting Certification	73
28. Reduction, Suspension, Withdrawal or Termination of Certification	74
29. Records	76
30. Complaints and Appeals	77

GOVERNANCE AND SUPPORT	80
A. RJC Ongoing Quality Checks	80
B. The RJC Complaints Mechanism	81
C. Disciplinary Proceedings	82
D. Data Confidentiality and Legal Advice	82
E. Training and Knowledge Exchange	83

REFERENCES	84
-------------------	----

LIST OF FIGURES & TABLES

FIGURES	
Figure 1. The RJC Assurance System	5
Figure 2. Steps in the RJC Audit and Certification Process	8
Figure 3. A Simple Structure Typical of Small and Medium-Sized Companies	16
Figure 4. A Multilayered, Complex Structure Typical of a Large Company	17
Figure 5. COP Versus COC Certification Scope for an Entity and its Parent Member	18
Figure 6. Member Types and Complexity Factors that Affect Auditing Times	22
Figure 7. The Seven Principles for Effective Auditing as Identified By ISO 19011	40
Figure 8. Certificate and Grace Period Example	72

TABLES	
Table 1. RJC Audit Types	20
Table 2. Guidelines for Audit Time Requirements for a Stand-Alone COP/LGMS Certification Audit, According to Company Size and Complexity	24
Table 3. Guidelines for Audit Time Requirements for a Stand-Alone RJC COC Certification Audit, According to Company Size and Complexity	24
Table 4. Guidelines for Audit Time Requirements for Subsequent COP/LGMS Audits	25
Table 5. Guidelines for Audit Time Requirements for Subsequent COC Audits	25
Table 6. Minimum Number of Entities/Facilities to Visit (Excluding the Central Office) for RJC Audits	31
Table 7. Criteria for Including Activities from Mining Exploration to Pre-Commissioned Stages in a COP Audit Scope	34
Table 8. Conformity Grading	49
Table 9. COP/LGMS Surveillance Format	67
Table 10. Extension (To Scope), Reduction, Suspension, Withdrawal or Termination of Certification	74
Table 11. Useful Timeframes	78

Our vision is a responsible worldwide supply chain that promotes trust in the global jewellery and watch industry.

The Responsible Jewellery Council (RJC) is a not-for-profit standard-setting organisation founded in 2005. The RJC plays a crucial role in promoting responsible practices and ethical standards within the jewellery and watch industry, bringing together member companies of all sizes, from mining to retail. Through the RJC Code of Practices (COP), the RJC Chain of Custody (COC) and the RJC Laboratory Grown Materials Standard (LGMS), hereinafter also collectively referred to as the RJC standards, and through third-party certification and collaborative initiatives, the RJC aims to build trust, transparency and sustainability across the entire jewellery and watch supply chain, ultimately benefiting consumers, communities and the environment.

The RJC's assurance system works to ensure a robust and credible evaluation process that supports members to implement and maintain the RJC standards as a pathway to addressing sustainability best practices, responsible sourcing and supply chain due diligence.

This is a version-controlled document and the RJC reserves the right to revise it based on implementation experience and emerging good practice. The official language of the RJC is English. Translations of various relevant RJC documents are available in a range of languages and are published on the [RJC website](#), as applicable. In the case of inconsistency between versions, reference shall default to the official-language version.

ENQUIRIES, FEEDBACK OR COMPLAINTS

If you have any enquiries or feedback on this document, please contact:

Email: assurance@responsiblejewellery.com. Telephone: +44 (0)20 7321 0992

Any complaints relating to this document can be submitted through the RJC Complaints Mechanism

<https://www.responsiblejewellery.com/contact-rjc/#complaints>

or by telephone: +44 (0)20 7321 0992.

DISCLAIMER

No guarantee, warranty or representation is made as to the accuracy or completeness of this document and other documents or information sources referenced in it. Use of this document is not intended to, nor does it, replace, contravene or otherwise alter the requirements of any applicable national, state or local governmental statutes, laws, regulations, ordinances or other requirements.

While this document should not be regarded as a complete and authoritative statement on any of the topics covered by it, the requirements enclosed herein are obligatory for certification bodies and their auditors when managing RJC audit and certification. Use of this document is neither intended to, nor does it, create, establish or recognise any legally enforceable obligations or rights against the RJC and/or its members or signatories.

RJC does not accept liability for any violations of applicable law or any infringement of third-party rights (each a breach) by other organisations, even where such a breach arises in relation to, or in reliance on, any RJC standard, document or other material, recommendation or directive issued by or on behalf of RJC. RJC gives no undertaking, representation or warranty that compliance with an RJC standard, document or other material, recommendation or directive issued by or on behalf of RJC will result in compliance with any applicable law or will prevent any breach from occurring.

The Responsible Jewellery Council is the trading name of the Council for Responsible Jewellery Practices Ltd, which is registered in England and Wales with company number 05449042.

© RJC 2025. All rights reserved.

Introduction

Learn about the key changes to the certification requirements and their effective date.

A ABOUT THIS DOCUMENT

The RJC Certification Process Requirements for Certification Bodies and Auditors, hereinafter called the 'RJC Certification Process Requirements', apply to all RJC certification bodies, their RJC auditors and relevant personnel under their control, who shall use it to understand and direct their activities and responsibilities associated with RJC audit and certification.

Specifically, this document sets out requirements, instruction and guidance for certification bodies and their auditors on how to:

- use the member self-assessment workbook.
- conduct independent third-party RJC audits, considering the principles for conducting effective audits to drive continual improvement.
- manage the RJC certification, including statement of conformity and certification decision, certificate issue, reduction, suspension, withdrawal and termination.

B STATUS AND EFFECTIVE DATE

The RJC Certification Process Requirements (version 1.0 February 2025) was approved by the RJC Board on 29 January 2025 and published on 19 February 2025. This version comes into effect on 1 July 2025 and supersedes all the certification process requirements previously detailed in the RJC Assessment Manual. This document is part of a suite of documents supporting the RJC standards.

This version is effective for:

- any RJC audits conducted against any RJC standards as of 1 July 2025, except COP 2019 mid-term reviews, COC 2017 surveillance audits, extensions to scope or provenance claim bolt-on audits conducted under a pre-existing COP/COC certificate. Any audits conducted as part of a pre-existing certificate shall follow the requirements in Assessment Manual version 1.3 December 2020, as the assessment methodology.
- any certificates issued as of 1 July 2025, regardless of whether the audit took place before or after 1 July 2025. The certificates shall be issued by the certification bodies as of this date. Any updates to pre-existing COP 2019/COC 2017 certificates following any audit type associated with them (mid-term reviews, surveillance audits, extensions to scope, etc.) shall be completed by the RJC, until these certificates expire.

Introduction

RJC Certification Process Requirements	
Document version	1.0
Date of publication	19 February 2025
Date of implementation	1 July 2025
Changes	<p>First version.</p> <p>Key differences compared to certification process requirements previously detailed in the RJC Assessment Manual:</p> <ul style="list-style-type: none"> • Intended for certification bodies and auditors. • Elimination of one-year COP certificates and COP transition audits. • Corrective action implementation and verification for major nonconformities before certificate issue. • Correction implementation and verification for all nonconformities before certificate issue. • Recommendation for semi-announced audits under specific limited conditions. • Audit invalidation. • Implementation of one mandatory COP/LGMS surveillance audit per certification cycle, at 12-18 months from certificate start date. • Certification to be managed by certification bodies, including certificate issue, reduction, suspension, withdrawal and termination, complaints and appeals. • Initial certification audit to take place within one and a half years of joining, to support achieving certification within two years. • Six-month timeframe before the certificate expiry date to complete the audit. • Mandatory submission of the member self-assessment workbook one month before the audit. • A new, separate mandatory documentary review stage for initial certification audits (absorbed within the audit planning and preparation time), to assess the member's preparedness for the audit and to communicate any areas of concern. • Remote audit elements as regular assessment tools and force majeure, subject to eligibility criteria. • Three months to address critical breaches, the same as major nonconformities. • Introduction of a three-month grace period after certificate expiry date, subject to conditions. • Certificate to be issued by the certification body within 10 working days of receipt of the member's signed audit report declaration, subject to conditions. • A provisional audit date to be booked at the closing meeting of the current audit, for the subsequent mandatory audit.

Introduction

C KEY TERMS AND DEFINITIONS

- '(RJC) members' refers to companies who have joined the RJC as commercial members and are seeking certification against the RJC standards.
- '(RJC) certification bodies' refers to the independent third-party certification bodies that have applied for and obtained approval to conduct RJC evaluation activities and manage RJC certification.
- '(RJC) auditor(s)' refers to the individual auditors under their control who have been approved to conduct RJC audits.
- '(RJC) audits' refers to evaluation activities including documentation review, interviews, observation, sampling and audits against the RJC standards' requirements, unless otherwise specified.

The following definitions, aligned with the International Organization for Standardization (ISO), apply in understanding how to implement this document:

- 'Shall' indicates a requirement.
- 'Should' indicates a recommendation.
- 'May' is used to indicate that something is permitted.
- 'Can' is used to indicate that something is possible, e.g. that a company or individual is able to do something.

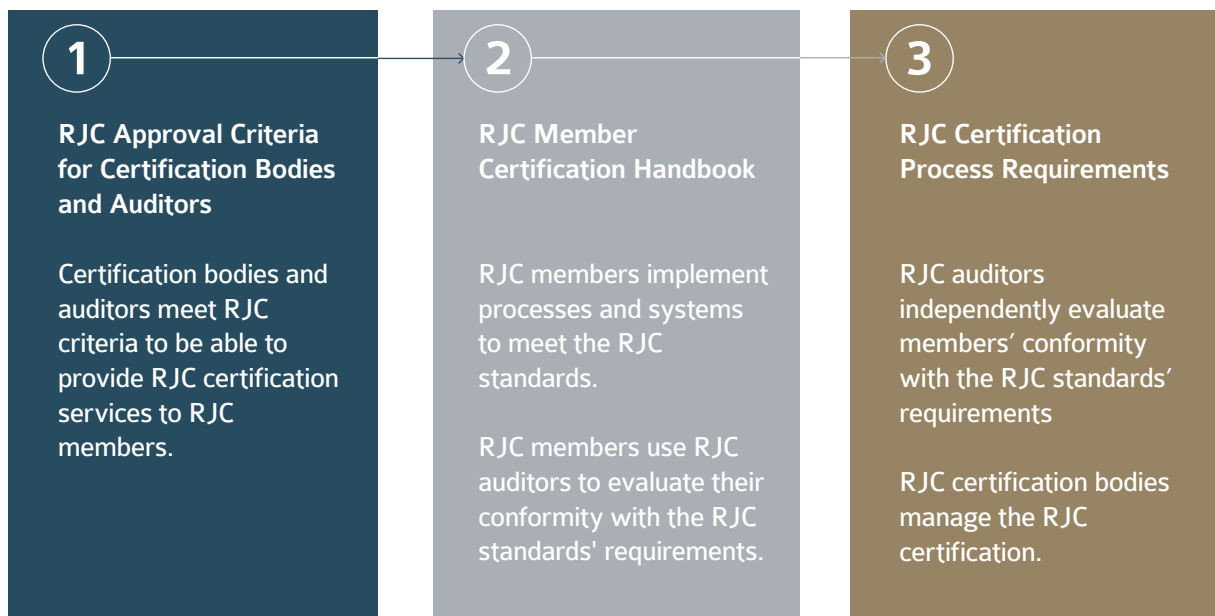


Introduction

D PURPOSE OF THIS DOCUMENT

The purpose of the RJC Certification Process Requirements is to set out the principles, procedures and objectives of the RJC assurance system that supports the independent third-party certification process for RJC members. This document covers the third element of the assurance system, as illustrated in Figure 1, below.

FIGURE 1: : THE RJC ASSURANCE SYSTEM



The RJC assurance system aligns with the principles outlined in the ISEAL Alliance Code of Good Practice for Sustainability Systems (version 1.0)¹. Drawing from this code, the desired outcomes from implementing the RJC Certification Process Requirements are the following:

- The RJC assurance system promotes accurate evaluation of conformity.
- The effectiveness and efficiency of the RJC assurance system are improved over time.
- The RJC assurance system is accessible and adds value to RJC members.

The implementation of the RJC Certification Process Requirements is subject to the RJC Oversight Mechanism, which is the umbrella term for a range of procedures to assess, review and improve the competency, accuracy, effectiveness and efficiency of the RJC assurance system.

¹ ISEAL's Code of Good Practice for Sustainability Systems (the 'ISEAL Code') provides a globally recognised framework, defining practices for effective and credible sustainability systems: <https://www.isealalliance.org/defining-credible-practice/iseal-code-good-practice>.

Introduction

E. ADDITIONAL SUPPORTING DOCUMENTS

The following documents provide normative and/or supporting information to assist certification bodies and auditors with the implementation of the requirements in this document:

- RJC standards, associated guidance, member self-assessment tools.
- [RJC Approval Criteria for Certification Bodies and Auditors](#) and [RJC Member Certification Handbook](#).

Further supporting documents, appendices, specialist toolkits and references to assist with implementation of the requirements in this document can be found on the [RJC website](#) and on the [Auditor Portal](#), while common terms and acronyms can be found in the [glossary](#) (see also Appendix 1, Supporting Documents).

Note that additional toolkits and templates are available to members only via the RJC Member Portal.

The RJC may periodically update, revise or develop any of these supporting documents, for example to reflect emerging best practice. If this happens, the RJC commits to:

- clearly specifying the timescales for members and certification bodies to implement, comply with and, where required, be assessed against the revised document;
- giving members and certification bodies advance warning of any amendment; and
- providing a summary of changes, where applicable.

In all cases, amended documents supersede any previous versions unless otherwise specified. Please see [RJC website](#) for the latest versions of supporting documents.



RJC Certification Process Requirements

Learn what the RJC Certification Process Requirements are for independent third-party audits against the RJC standards. RJC members may also find this section useful in understanding in detail what to expect from their RJC certification.

GENERAL – THE RJC STANDARDS

The RJC has developed standards that promote responsible business practices throughout the jewellery and watch supply chain, for the materials in RJC scope, against which commercial members shall undergo independent third-party audits by RJC auditors, to achieve a three-year certification.

The RJC standards set the requirements against which members are evaluated. The standards are supported by definitions and rules in the normative documents, such as the RJC standards' guidance, glossary and appendices.

The applicability of the RJC standard provisions may vary according to the business activities undertaken by the member and its place in the supply chain (see relevant standards and standard guidance).

The RJC Code of Practices (COP) and Laboratory Grown Materials Standard (LGMS) are mandatory standards that define the responsible ethical, human rights, social and environmental practices that all certified RJC members must adhere to, within the jewellery and watch industry.

Audit and certification against the COP/LGMS are mandatory for RJC members that handle materials in scope. Members are expected to undergo their initial certification audit against the requirements of the COP/LGMS within one and a half years of joining and achieve certification against the same within two years of joining the RJC, to demonstrate responsible business practices.

Members are certified as a whole and for all materials in the RJC COP/LGMS scope, rather than by entity/facility and/or material. Once certification against the RJC mandatory standard(s) is achieved, maintaining it is required to retain RJC membership (see [RJC membership](#) for more information).

The RJC Chain of Custody (COC) is a voluntary standard available for precious metals only. The COC defines the requirements for creating a chain of custody of precious metals that are responsibly sourced, produced, processed (fully segregated and traceable) and traded.

Audit and certification against the COC standard is voluntary for members (or entities under their control), and therefore not a requirement of RJC membership.

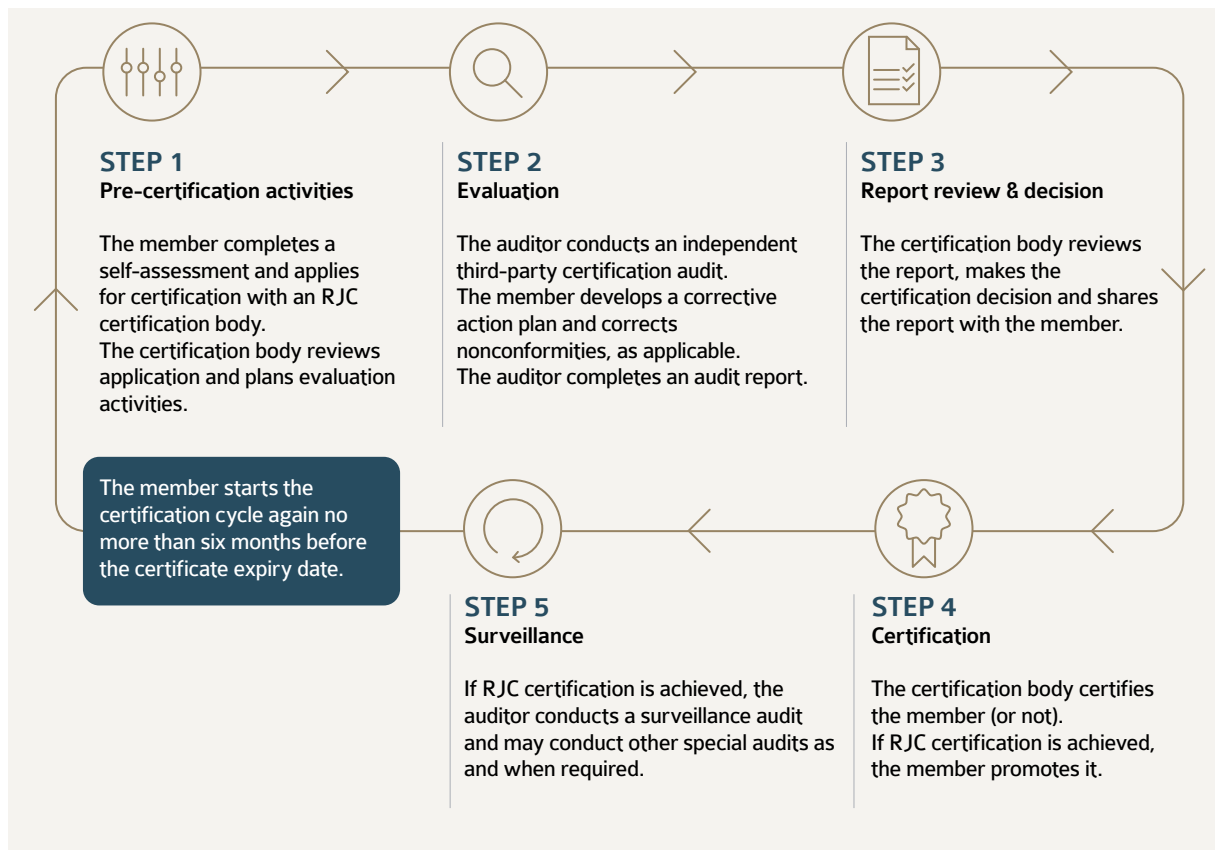
Certification bodies can only certify against the COC those RJC members (or entities under the control of an RJC member) that are already COP-certified or are evaluated in a combined COP/COC audit to achieve simultaneous certification.

RJC Certification Process Requirements

OVERVIEW OF THE RJC CERTIFICATION PROCESS

The RJC certification process is broadly made up of five steps (see Figure 2, below), which are further broken down over the following sections to specify requirements for certification bodies and auditors. For more general guidelines on how to conduct effective audits, including how to listen, question and observe effectively, see Appendix 8, Guidelines for Auditors: Conducting Effective Audits.

FIGURE 2: STEPS IN THE RJC AUDIT AND CERTIFICATION PROCESS



Step 1 – Pre-Certification Activities



1. APPLICATION

The first step in the certification process is for members and certification bodies to make contact to discuss and confirm details about the certification and audit scope, including the logistics involved in carrying out the audit, access to documentation and the desired audit date.

- 1.1. Once contact is initiated, the certification body shall respond to the member within five working days to ensure timely communication is maintained at all stages of the process.
- 1.2. For an initial certification audit, the certification body shall obtain all the necessary information to complete the certification process and document the information gathered, as per mandatory and supplementary information under 1.3. For any other type of audit, depending on whether the certification body has changed or not, the information below shall be either newly obtained or as an update to information already obtained for the initial certification audit. A variety of media and mechanisms can be used to collect and record this information at various times, including an application form set by the certification body, the RJC self-assessment workbook or an equivalent format of the member's choice. Such information gathering can be in conjunction with, or separate from, the completion of a legally binding agreement (the certification agreement) between the certification body and the member.
- 1.3. Mandatory member information to obtain:
 - a) Contact details for key staff including the authorised member representative for communicating with the certification body and the RJC.
 - b) The RJC standard(s) against which certification is sought.
 - c) Member name and address details.
 - d) Member forum (i.e. mining, refining, retail, etc.), as assigned by the RJC on membership application and approval process (see [RJC applications guidance](#)).

Step 1 – Pre-Certification Activities

- e) Any relevant legal obligations.
- f) The certification scope, as identified, proposed and documented by the member – namely, a written summary of significant aspects of its processes, services, operations and business activities to be certified, owned or controlled, that contribute to the jewellery and watch supply chain, whether or not these are situated at the member's entities/facilities (see Section 3, Certification Scope, for more information, including any exclusions).
- g) Identification of outsourced processes used by the member that will affect conformity with the RJC standards' requirements.
- h) Organisational charts outlining member structure (organogram including all entities/facilities and share percentages), responsibilities and authorities, human and technical resources, functions and relationships. The member structure organogram should be certified by a notary or independent qualified accountant.
- i) The activities or functions to be audited and the availability of key personnel for interview, wherever possible. It is not uncommon, however, to have to exercise flexibility here if, for example, information is not available off-site.
- j) Information about each entity/facility within the certification scope, including the headquarters, such as:
 - name.
 - address.
 - whether a virtual business and, if so, whether any processes are executed in a physical environment.
 - type, infrastructure, facilities and equipment (such as retail store, workshop, etc.).
 - working hours and shifts, associated activities and any downtime periods.
 - number of employees and contractors; if it is impractical to record this per entity/facility (e.g. if the member is a large retailer with an international network of shops), the member can document number of employees and contractors at a country level and in total.
 - nature of activity, namely processes conducted and materials in RJC scope – members that own or control multiple entities/facilities doing the same type of activity can group their descriptions here.
- k) Any on-site contractors and details of their activities.
- l) If the application is for COC, any outsourced contractors, details of outsourced activities and the risk level.
- m) Any claims the member is making or intends to make, including provenance claims.
- n) The full reports of previous RJC audits and corrective action plans and associated documentation (where performed by another certification body).
- o) Information about any changes to the certification scope anticipated in the next three years, such as expansions, acquisitions, divestments, etc. (see Section 27, Changes Affecting Certification).

Supplementary member information and documents, where applicable, to review include the following:

- p) A completed RJC self-assessment workbook, or any other equivalent tool, if it is already available but no older than six months, including details of any self-assessed nonconformities and how these are being addressed.

Step 1 – Pre-Certification Activities

- q) Whether the audit will be combined, integrated or joint.²
- r) Whether the member has any RJC-recognised certifications (see Section 6, Harmonise Efforts for Responsible Business Practices: Claims of Equivalency with RJC-Recognised Frameworks).
- s) Whether the member will require the auditor to sign a confidentiality agreement. Note that this will not apply to information that it is necessary to share with the RJC as per this document, including critical breaches.
- t) Details of any contractors (other than those covered in 1.3(k) and (l)), business partners or other related companies out of the member's control, to help put the certification scope in context. This includes identifying where members are part of a broader corporate group.
- u) Any available reports from local regulators and required corrective actions and plans.
- v) Relevant organisational performance data (e.g. key performance indicator data).
- w) Whether consultancy relating to compliance with the RJC standard(s) has been provided and, if so, by whom.
- x) Reports or briefings on relevant issues, for example:
 - a list of interested parties, including neighbours and other stakeholders and any concerns.
 - a risk profile outlining ethical, environmental and workplace health and safety issues.
 - a summary of any complaints received by the certification body or the RJC about the member and requiring review during the audit.

2. APPLICATION REVIEW

- 2.1. To get as much understanding of the member's business as possible, the certification body shall review the member's mandatory and supplementary information and any other useful details in this phase, as per internal processes, to ensure that:
- a) the information about the member and its systems, processes, services and activities is sufficient to develop an audit programme and conduct the certification process.
 - b) any known difference in understanding between the certification body and the member is resolved.
 - c) the RJC certification scope sought is clearly and accurately defined, as per Section 3, Certification Scope.
 - d) the member's entities/facilities, the time required to complete the audits and any other points influencing the certification activity are taken into account (language, safety conditions, threats to impartiality, etc.).
 - e) the certification body has the means, competence and capability to perform the audit and certification activity.

² 'Combined audit' refers to one single audit where the company is evaluated against two or more standards/schemes. If requirements from multiple standards/schemes have been integrated into a single, cohesive system within a company, then this is considered an integrated audit. A joint audit is conducted when two or more certification or conformity assessment bodies collaborate to audit a single company together.

Step 1 – Pre-Certification Activities

- 2.2. Following the review of the application, and depending on whether the certification body has the means, competence and capability to undertake the relevant audit and certification activities, it shall either accept or decline an application for certification, by documenting its decision, including the justification for accepting or reason for declining an application.
- 2.3. On application acceptance (and certification agreement with the member), the certification body shall ensure that all audits of any type are recorded on the RJC Auditor Portal under Booked Audits so that the RJC has timely visibility of all upcoming (scheduled) audits.
- 2.4. If the certification body lacks the means, competence and capability to undertake the relevant audit and certification activities, it shall decline the application and inform the member of this as soon as possible, but no later than 15 working days from receipt of the member's application, so that the member has sufficient time to engage with a different certification body and comply with the RJC certification timelines.
- 2.5. Based on this review, the certification body shall also determine the competences it needs to include in its audit team, and for the technical review and certification decision.
- 2.6. The certification body shall be aware of both the intent and practical application of instructive documents such as regulations, standards, policies, contracts, procedures, specifications and guidelines.
- 2.7. The certification body shall identify whether the company applying for certification is a rejoining company by accessing the Auditor Portal and engaging with the RJC, as need be. RJC rejoining companies are companies that wish to rejoin the RJC within a stand-down period of two years from termination for any reason, or members who have recently rejoined the RJC after a stand-down period of two years from termination for any reason.
- 2.8. Certification bodies shall follow the following certification process and timeline on receiving a certification application from RJC rejoining companies:
 - 2.8.1. For companies that wish to rejoin the RJC within a stand-down period of two years from termination:
 - The certification body shall audit the company (while it is not yet a member) against the relevant RJC mandatory standard and shall submit the completed audit report (including statement of conformity and certification decision) to the RJC before the company reapplies for RJC membership.
 - If the certification decision is positive and certification can be granted, the RJC will accept and process the company's membership application.
 - Once RJC membership has been approved, the certification body shall issue certification with the date of the RJC membership approval.
 - 2.8.2. For companies that have recently rejoined the RJC after a stand-down period of two years from termination:
 - The certification body shall audit the company (recently approved as a member) against the relevant RJC mandatory standard within six months of the member rejoining the RJC.
 - The company, as a recently approved member, shall achieve certification within 12 months from rejoining the RJC or forfeit membership.

Step 1 – Pre-Certification Activities

3. CERTIFICATION SCOPE

The RJC certification scope refers to the extent of a member's business (process(es), service(s), or product(s)) to which the relevant RJC standard(s) apply and for which certification is granted based on conformity evaluation. Each member's certification scope will be different, depending on the standard in question as well as the type and structure of the member's business.

- 3.1. For the RJC mandatory standards, the certification body shall verify the accuracy of the certification scope by reviewing whether the RJC membership scope (as approved by the RJC) and certification scope of the RJC commercial member (as proposed by the member) match, with no exclusions allowed for the certification scope compared to the membership scope. To do so, the certification body may want to follow the guidelines below.

RJC MEMBERSHIP

The RJC membership scope for commercial members is defined on member application and RJC review and approval of application. It is available to certification bodies and their auditors via the Auditor Portal.

The RJC membership scope for commercial members includes all the following that are owned/controlled by the member and covers mining, selling, manufacturing or buying RJC-scope materials and other activities that contribute to the jewellery and watch supply chain:

- Entities (individual legal business or similar); and/or
- Facilities (site or premises that are operated by an entity, including retail stores, trading offices, manufacturing sites, etc.); and
- Business activities (including tasks, roles, functions or services, noting that business activities may or may not take place at a member's entity/facility and may be in separate locations).

Control means having the beneficial ownership of 50% or more of the issued share capital of a company or the power to direct or cause the direction of the management of the company (including by setting workplace standards and enforcing their application; see [RJC glossary](#) for more information).

The following activities are considered to actively contribute to the precious metal, diamond and coloured gemstone jewellery and watch supply chain and fall within the RJC membership scope:

- Exploration and mining.
- Laboratory-grown materials producers.
- Diamond and coloured gemstone trading, cutting and polishing.
- Precious metal refining, trading and hedging.
- Jewellery and watch manufacturing and wholesaling.
- Jewellery and watch retailing.
- Service industries, including grading, assaying, appraising, secure transport providers, sales platforms and others.

Step 1 – Pre-Certification Activities

By means of including all its entities and facilities that contribute to the jewellery and watch supply chain, each applicant company is required to (and is responsible for so doing) clearly and accurately identify, propose and document its own RJC membership scope for review and approval by the RJC.

If a mine produces several different mineral products, it must be included in the membership scope if precious metals, diamonds or coloured gemstones make up a significant³ saleable element in the mineral concentrate or process by-products. If the mine's contribution to these is minimal⁴ relative to the mine's total production, it may be appropriate to exclude it from the membership scope. Inclusion of multi-commodity sites will be considered on a case-by-case basis.

Note that the RJC shall reject attempts to register just one company out of a group as a member, and require the parent company of a group to become the RJC member and seek RJC certification in its own name. In exceptional circumstances, and at the RJC's sole discretion, on a case-by-case basis, the RJC may allow individual memberships for companies that are part of a group, for example where neither the central office/holding group nor the majority of its entities contribute to the jewellery and watch supply chain, as an exclusion from membership scope. For more details, see [RJC applications guidance](#). For any queries on the RJC membership scope, please contact the RJC at membership@responsiblejewellery.com.

- 3.2. The certification body shall verify the accuracy of the COC certification scope depending on which entities within the RJC membership scope contribute to the material they wish to declare as COC material; which materials within the COC scope the member wishes to pursue COC certification for; and whether or not the member uses outsourced contractors (see Section 9, COC Outsourced Contractors).
- 3.3. The certification body shall only certify against the COC those RJC members, or entities under the control of RJC members, that are already COP-certified or are audited in a combined COP/COC audit to achieve simultaneous certification.
- 3.4. The certification body shall consider the following when verifying a member's proposed COC certification scope:
 - a) All entities/facilities that the member (or all facilities that the entity) owns or controls and intends to use to extract, process, manufacture and/or trade COC material.
 - b) All outsourcing contractors that the member intends to use to process and/or manufacture COC material.

Note that member-owned or affiliated entities providing warehousing, logistics and transport are considered service providers and subject to risk assessment, as opposed to inclusion in the COC certification scope.
 - c) Which types of COC material (gold, silver or platinum group metals (PGMs)) the member wishes to handle as COC.
 - d) Whether the member intends to make eligible material declarations and, if so, for which type of eligible material (see the COC standard for details on eligible material types).

³ Typically, a threshold of 10% by value is applied.

⁴ Typically, a threshold of 10% by value is applied.

Step 1 – Pre-Certification Activities

- 3.5. Based on the information obtained and reviewed during the application stage and for any RJC standard, the certification body shall:
- verify the certification scope, including consistency of information between the RJC membership scope on the Auditor Portal, the member website, the (certified) organogram and any other relevant piece of information.
 - clearly and accurately define and document the certification scope.
 - confirm the full alignment of the certification scope with the RJC membership scope via the Auditor Portal; or
 - communicate any differences between the RJC membership scope and certification scope to the RJC and the member within five working days of identification.
 - revise the verified and defined certification scope if any new and relevant information is obtained at a later stage during an audit of any type, and repeat points (a) to (d), as applicable.
 - use the certification scope to confirm the audit scope and define exactly which RJC standard provisions apply and include this in the audit report (see relevant standard and corresponding guidance).
 - include the certification scope in the audit report and in the RJC certificate.

Stakeholders are encouraged to contact the RJC through the RJC Complaints Mechanism if they believe anything has been omitted from, or misrepresented in, a member's membership and certification scope.



Step 1 – Pre-Certification Activities

EXAMPLES OF CERTIFICATION (AND MEMBERSHIP) SCOPE

Every company is different and so it will have a distinct certification (and membership) scope, reflecting the diversity in size and structure among members. See below for some examples of different business structures and how they may impact this scope for the RJC mandatory standards. For more examples, see the Commercial Membership Application Guidance on the [RJC website](#).

FIGURE 3. A SIMPLE STRUCTURE TYPICAL OF SMALL AND MEDIUM-SIZED COMPANIES

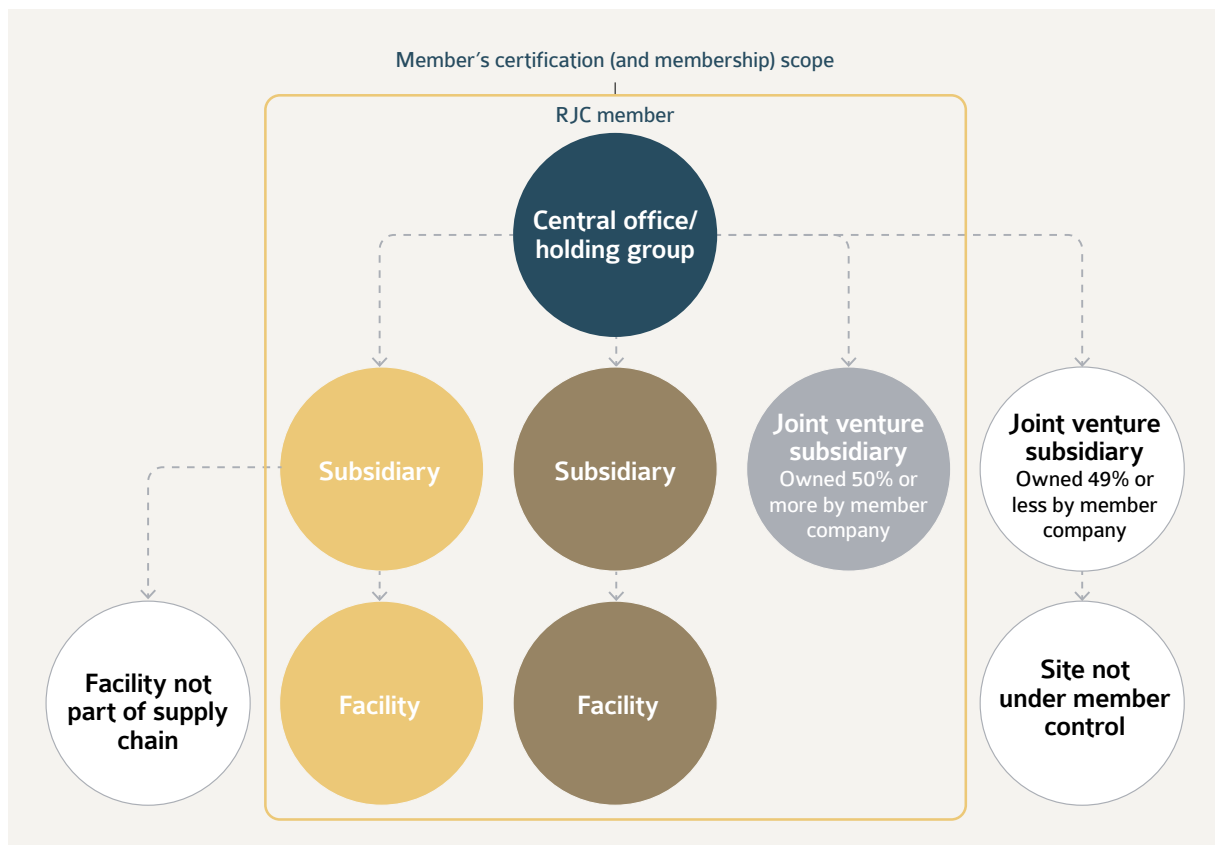


In Figure 3, the member's business has a simple structure. All the business activities are owned or controlled by the member and all contribute to the precious metal, diamond and coloured gemstone jewellery and watch supply chain. Here the entire business falls within the RJC certification (and membership) scope.



Step 1 – Pre-Certification Activities

FIGURE 4. A MULTILAYERED, COMPLEX STRUCTURE TYPICAL OF A LARGE COMPANY



In Figure 4, the member's business is more complex and includes several subsidiaries and facilities, some of which are not under the member's control and some of which do not contribute to the precious metal, diamond and coloured gemstone jewellery and watch supply chain. In this example, the certification (and membership) scope is a subset of the whole business.

MEMBERS IN THE MINING SECTOR

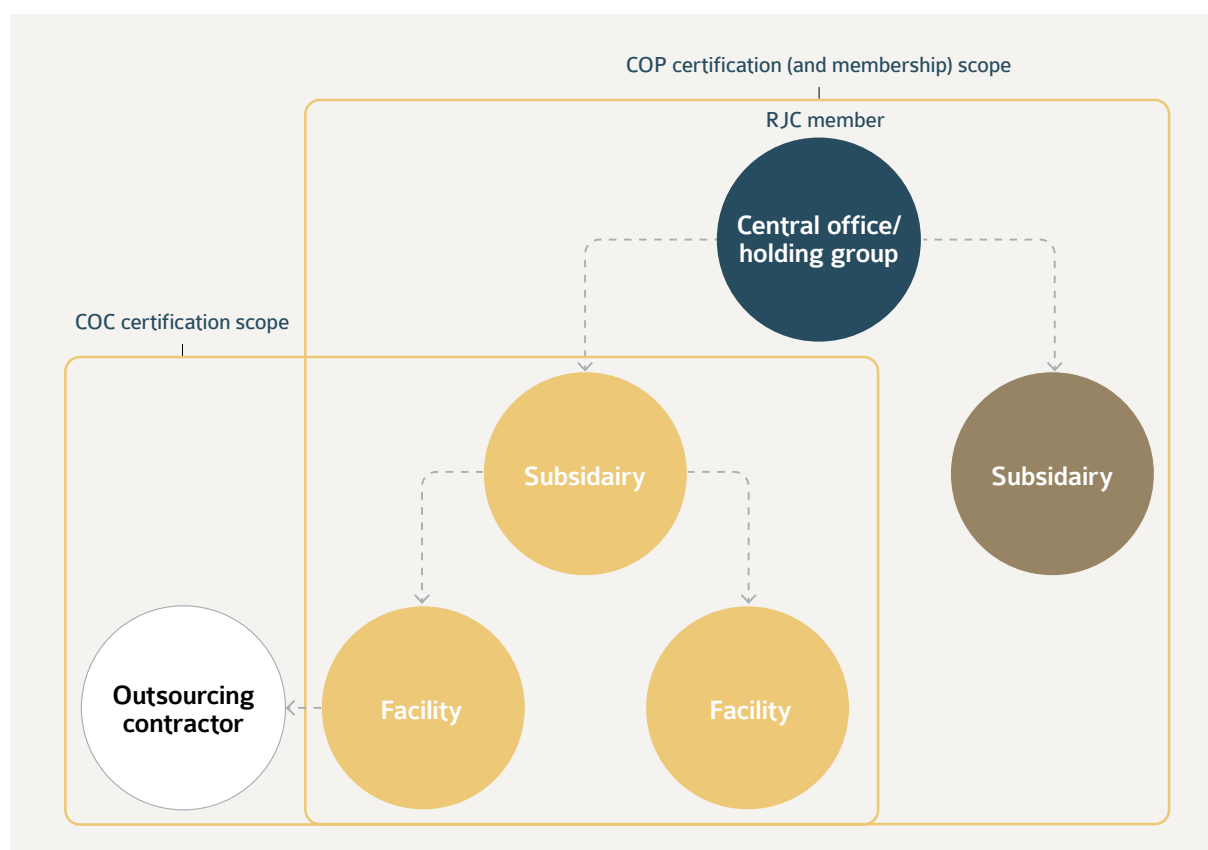
Several COP provisions apply directly to the early stages of mine development. For RJC commercial members in the mining sector, the certification scope shall include exploration activities, or any other business practices aimed at developing future mining facilities. These practices will be evaluated by an auditor through desktop reviews or site visits as appropriate (for more information, see 8.5, Incorporating early mining activities (COP only)).

Step 1 – Pre-Certification Activities

COC CERTIFICATION SCOPE

A COC certification scope does not have to cover all parts of a member's business, nor does it necessarily have to match the COP certification scope. COC certification may be granted to members as a whole or to individual entities under a member's control in the COC pipeline. It also does not need to cover all of a member's precious metals sourcing or sales but can be specifically limited to some or all of the materials in scope for the COC standard, as the member wishes. For example, a member can choose to seek COC certification for only some of the mines or factories under its control. In Figure 5, the company seeking COC certification is a subsidiary of the RJC member, so the COP and COC certification scopes are different.

FIGURE 5. COP VERSUS COC CERTIFICATION SCOPE FOR AN ENTITY AND ITS PARENT MEMBER



Step 1 – Pre-Certification Activities

4. AUDIT PROGRAMME AND AUDIT TYPES

- 4.1. Based on the above member information, and considering any changes to the certification requirements, certification body approval criteria or legal requirements, the certification body shall develop an audit programme for the full certification cycle to clearly identify the audit activity/activities required to demonstrate that the member's systems and processes fulfil the requirements for certification to the selected RJC standard(s).
- 4.2. The determination of the audit programme and any subsequent adjustments shall consider the size of the member; the scope and complexity of its activity, management system, products and processes; the demonstrated level of its management system and process effectiveness; and the results of any previous audits. The following additional items can be considered when developing or revising an audit programme or when determining the audit scope and developing the audit plan:
- a) Complaints received by the certification body or RJC about the member. RJC auditors may be asked to conduct investigations or verify required corrective actions during the audit. In such cases, the auditor is not permitted to inform the member of the investigation or of any particular focus area during the audit.
 - b) Relevant interested parties' concerns.
 - c) Combined, integrated or joint audit.
 - d) Changes to the certification requirements.
 - e) Changes to legal requirements.
 - f) Changes to certification body and auditor approval criteria.
 - g) Organisational performance data (e.g. key performance indicator data).
 - h) Any external certifications against specific standards and initiatives that are recognised by the RJC (see Section 6, Harmonise Efforts for Responsible Business Practices: Claims of Equivalency with RJC-Recognised Frameworks).
- 4.3. The audit programme for the initial certification evaluation shall include a documentary review and an audit, followed by one mandatory surveillance audit between 12 and 18 months from the certificate start date, including timely scheduling of these audits.
- 4.4. The certification body shall use the audit types and frequency in Table 1, below, to verify member conformity against the RJC standards. All audit types shall include a built-in follow-up stage to verify implementation of corrections and corrective actions for critical breaches and/or major nonconformities (if applicable), either desktop or on-site, based on the type of issue, and the need to triangulate evidence. This follow-up stage is included in the mandatory audit and different from a special follow-up audit, as defined in Table 1(f), below. The special audit types can be stand-alone or included in any of the initial certification, surveillance and recertification audits, depending on the next scheduled audit. Any audit type may assess identified risks, and the RJC management team will contact the auditor in advance to ensure the issue is included in the member's upcoming audit scope.

Step 1 – Pre-Certification Activities

TABLE 1. RJC AUDIT TYPES

MANDATORY AUDIT TYPE	RJC STANDARD	WHEN IT HAPPENS	WHY IT'S NEEDED	SCOPE
a) Initial certification audit	COP/ LGMS	Within 18 months of becoming a member, unless the member is a rejoiner (see 2.8).	To achieve certification within two years of joining the RJC and maintain RJC membership (mandatory for all commercial members).	Sections 6–9
	COC, if applicable	At the same time as, or after, a COP audit, but not before. Certification cycle and/or expiry date shall be aligned with COP.	To add value to businesses and brands (voluntary for RJC members).	
b) Surveillance audit	COP/ LGMS	12–18 months after the certificate start date.	To ensure ongoing conformity with key provisions and validity of the demonstration of fulfilment of process requirements. To review progress against a corrective action plan, as applicable. Surveillance audit may be conducted remotely (see Section 22, Surveillance Audit Format and Scope). To consider: <ul style="list-style-type: none"> • Those entities/facilities and provisions that were not visited or were given less attention in the last audit. • The nature of any nonconformities found in the last audit. • Any corrective action plans, past or present. • Any changes in certification scope since the last audit. • Any business changes since the last audit, including organisational structure and resources. • Any complaints about the member received by the certification body or the RJC. 	Section 22 Surveillance Audit Format and Scope
	COC			
c) Recertification audit	COP/ LGMS	Within six months before certification expiry date.	To renew certification. Please note that ongoing recertification against the COP/LGMS is mandatory for all commercial members to maintain RJC membership.	Section 23 Recertification
	COC, if applicable			

Step 1 – Pre-Certification Activities

SPECIAL AUDIT TYPE	RJC STANDARD	WHEN IT HAPPENS	WHY IT'S NEEDED	SCOPE
d) Scope change	COP/ LGMS COC	As required.	To enable a change to the certification scope, such as the addition or removal ⁵ of an (additional) entity/facility, or to add materials in scope outside a scheduled audit such as surveillance or recertification.	Verification of the new/changed scope against the applicable provisions.
e) Provenance claim bolt-on	COP/ LGMS	As required.	To enable verification and certification of a new or changing provenance claim.	Verification of a new or changing provenance claim.
f) Follow-up (short notice)	COP/ LGMS COC	As required.	To conduct additional verification outside a scheduled audit such as surveillance or recertification. This audit type may be triggered as an input to, or as an outcome of, the RJC Complaints Mechanism or disciplinary proceedings.	Verification of the focus area against the applicable provisions.



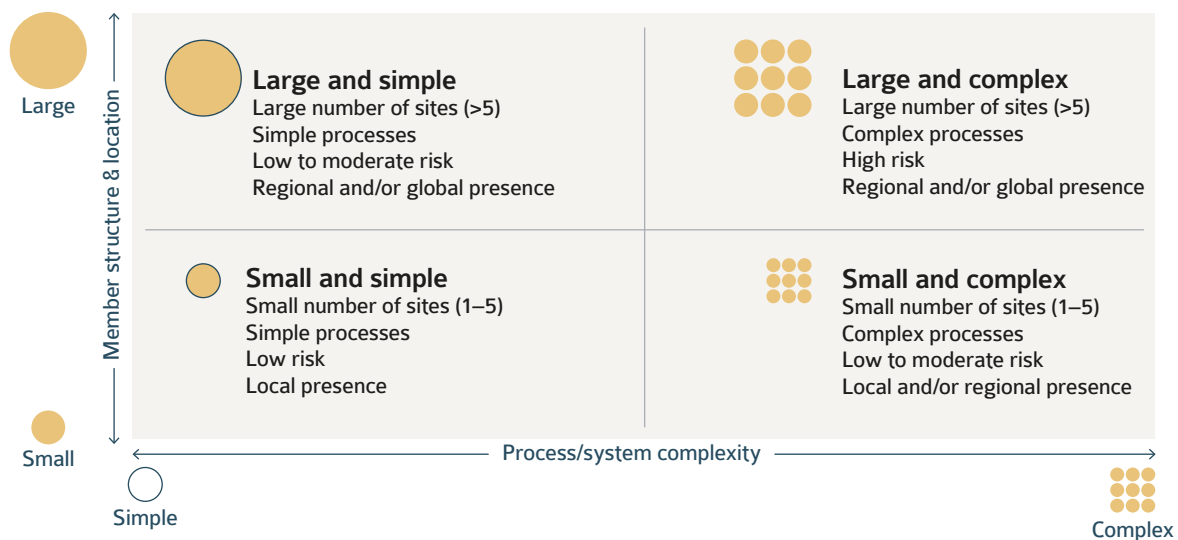
⁵ When the removal of an entity/facility may impact the overall processes, system and activities of a certified member. This is especially relevant to COC certifications.

Step 1 – Pre-Certification Activities

5. DETERMINING AUDIT TIME

This section focuses on how much time is generally required to plan and undertake a complete and effective RJC audit. The audit time (measured in in-person days of eight hours each) depends on factors such as the size, complexity of processes to be certified and the supply chain, and location of the member being audited (see Figure 6). These factors should be seen as part of a continuous spectrum rather than as stepped change between members.

FIGURE 6. MEMBER TYPES AND COMPLEXITY FACTORS THAT AFFECT AUDITING TIMES⁶



5.1. The certification body shall determine the time needed by considering, among other things, the following aspects:

- a) The requirements of the relevant RJC standard(s).
- b) The complexity of the member and its systems, processes, activities.

Organisational structure, location and complexity (the axes in Figure 6) comprise a continuum of business types rather than discrete categories. So, for example, the complexity continuum moves from businesses with limited product lines or simple processes (e.g. retailers) to those with multiple products and varied operations (e.g. diamond traders or jewellery manufacturers) to those with complex, unique or significant operations (e.g. miners). In general, the larger and more complex a company is, the more time the auditor will need to effectively audit it.

- c) Technological and regulatory context.
- d) Any outsourcing of any activities included in the certification scope.
- e) The results of any prior audits.

⁶ Based on the International Accreditation Forum (IAF), Determination of Audit Time of Quality, Environmental and Occupational Health & Safety Management Systems (IAF MD 5:2023) https://iaf.nu/iaf_system/uploads/documents/IAF_MD5_Issue_4_Version_3_14062023.pdf

Step 1 – Pre-Certification Activities

- f) Size and number of entities/facilities, their geographical locations and multi-site considerations.

The location continuum moves from companies with a local presence (usually within a city or locality) to those with a regional presence (typically within a country or several countries) to those with a global presence (typically multinational companies).

- g) The risks associated with the member's processes or activities.

- h) Whether audits are combined, joint or integrated.

- i) Factors that can increase the amount of audit time:

- i. Multiple entities/facilities in scope with varying activities and conditions or specific geographic or activity risks.
- ii. Presence of on-site contractors engaged in high-risk activities not under the direct control of the member.
- iii. Any changes to scope, as applicable.
- iv. The use of complicated provenance claims.
- v. The complexity of the member's supply chain, taking into account the number of different materials, the geographic spread of suppliers and associated risks.
- vi. The presence of any pending complaint investigations.
- vii. The level of preparation the member has done.
- viii. A higher number of people to be interviewed: interview time will vary based on total number of employees, the risks, nature and scale of activities (see Appendix 7, Sampling Techniques), and the use of any translators and interpreters.

- j) Factors that can decrease the amount of audit time:

- ix. Members who are well prepared.
- x. RJC recognition of the member's existing certifications and/or initiatives.
- xi. Commonality of activities across entities/facilities that could allow a multi-site sampling approach.

5.2. The certification body shall allocate sufficient time to each entity/facility to be audited depending on the nature of the operations and the geographic or activity risks. For example, more time would be required at a factory with workers paid on an hourly or performance basis, and/or with potentially more serious health and safety risks, or for on-site contractors engaged in mining activities, than at a sales office or retail store. Equally, verifying conformity of a sourcing office that is responsible for conducting due diligence on the supply chain would require more time than verifying conformity of a subsidiary receiving office that is responsible for quality control.

5.3. The certification body shall consider Tables 2 and 3, below, which offer a general guide to how much audit time (on-site/remote) the auditor will likely need to audit each of the four broad types of business for initial certification against the RJC standards. Where the total allocated time for the audit of the entire member's scope exceeds or falls below these ranges due to the factors above, this shall be fully explained by the lead auditor in the completed audit report. However, the duration of the audit shall not normally be less than 80% of the general guide duration, subject to verified RJC-recognised certifications.

Step 1 – Pre-Certification Activities

TABLE 2. GUIDELINES FOR AUDIT TIME REQUIREMENTS FOR A STAND-ALONE COP/LGMS CERTIFICATION AUDIT, ACCORDING TO COMPANY SIZE AND COMPLEXITY

NUMBER OF PERSONNEL WORKING IN FACILITIES INCLUDED IN THE CERTIFICATION SCOPE*	BASE TIME (AUDIT DAYS)	ADDITIVE FACTORS (BUSINESS COMPLEXITY AND LOCATION) AUDIT DAYS			
		SMALL AND SIMPLE	SMALL AND COMPLEX	LARGE AND SIMPLE	LARGE AND COMPLEX
1–25	2	-1	0	+1	+2
26–100	3	-1	0	+1	+2
101–500	4	-1	0	+2	+5
501–1,000	6	-2	+1	+2	+6
1,001–5,000	7	-2	+1	+4	+6
5,001–10,000	10	-3	+2	+4	+8
10,001–20,000	12	-4	+3	+6	+10
>20,000	>12	-<4	+>3	+>6	+>10

* The number of part-time employees should be treated as full-time equivalents based on the number of hours worked as compared with full-time employees.

TABLE 3. GUIDELINES FOR AUDIT TIME REQUIREMENTS FOR A STAND-ALONE RJC COC CERTIFICATION AUDIT, ACCORDING TO COMPANY SIZE AND COMPLEXITY

NUMBER OF ENTITIES/FACILITIES IN COC SUPPLY CHAIN (including high- and medium-risk outsourced contractors)	BASE TIME (AUDIT DAYS)	ADDITIVE FACTORS (MATERIALS AND TRANSACTION VOLUMES) AUDIT DAYS			
		SIMPLE LOW-RISK*	SIMPLE MEDIUM-RISK**	COMPLEX MEDIUM-RISK***	COMPLEX HIGH-RISK****
1	2	-1	0	n/a	+1
2–5	4	n/a	-1	0	+3
5–10	8	n/a	0	+2	+5
>10	13	n/a	0	+2	+6

* Single location processing materials on consignment, e.g. outsourced contractor wishing to hold own certification.

** Small number of entities/facilities in single country/region, manufacturing operations sourcing materials from low-risk sources including materials on consignment or refineries, no high-risk outsourced contractors.

*** Entities/facilities spread across regions/globally, outsourced operations that include high-risk activities, sourcing materials from low-risk sources including materials on consignment or refineries.

**** High-risk operations with critical control points for contamination, e.g. refineries; members sourcing from primary producers or including collection centres for recycled materials.

Step 1 – Pre-Certification Activities

5.4. The certification body shall consider:

- a) up to half the time spent on the initial certification audit for a surveillance audit where the certification scope has not changed (see Tables 4 and 5).
- b) between two thirds of and the same time as an initial certification audit, for recertification audits, particularly in (but not limited to) instances where the certification body has changed (see Tables 2, 3, 4 and 5). To determine the recertification audit time (starting at two thirds of the time for the initial certification audit), the certification body shall first determine what the required audit time would be for an initial certification audit of the member if such an initial audit were to be carried out at the time of recertification, and then calculate two thirds of this time, as opposed to calculating two thirds of the original time actually spent on the initial certification audit.

TABLE 4. GUIDELINES FOR AUDIT TIME REQUIREMENTS FOR SUBSEQUENT COP/LGMS RJC AUDITS⁷

NUMBER OF PERSONNEL WORKING IN FACILITIES INCLUDED IN THE CERTIFICATION SCOPE*	INITIAL CERTIFICATION AUDIT DAYS	SURVEILLANCE AUDIT DAYS**	RECERTIFICATION AUDIT DAYS**
1–25	1–4	0.5–2	1–3
26–100	2–5	1–3	2–4
101–500	3–9	2–5	2–6
501–1,000	4–12	2–6	3–8
1,001–5,000	5–13	3–7	4–9
5,001–10,000	7–18	4–9	5–12
10,001–20,000	8–22	4–11	6–15
>20,000	>(8–22)	>(4–11)	>(6–15)

* The number of part-time employees should be treated as full-time equivalents based on the number of hours worked as compared with full-time employees.

** In most cases, the number of days was rounded up.

TABLE 5. GUIDELINES FOR AUDIT TIME REQUIREMENTS FOR SUBSEQUENT COC AUDITS

NUMBER OF ENTITIES/FACILITIES IN COC SUPPLY CHAIN	INITIAL CERTIFICATION AUDIT DAYS	SURVEILLANCE AUDIT DAYS*	RECERTIFICATION AUDIT DAYS*
1	1–3	0.5–2	1–2
2–5	3–7	2–4	2–5
5–10	8–13	4–7	6–9
>10	12–18	6–9	8–12

* In most cases, the number of days was rounded up.

⁷ Based on estimates for management system certification schemes as published by the International Accreditation Forum (IAF). See IAF, Determination of Audit Time of Quality, Environmental and Occupational Health & Safety Management Systems (IAF MD 5:2023) https://iaf.nu/iaf_system/uploads/documents/IAF_MD5_Issue_4_Version_3_14062023.pdf

Step 1 – Pre-Certification Activities

5.5. Off-site time requirements:

- a) In general, the time spent doing an audit is distributed as follows, although the percentage of off-site time may decrease as the on-site/remote portion of the audit extends:
- 30% of time devoted to planning and preparation.
 - If documentary review is required, the allocated time shall be deducted from the planning and preparation time, as opposed to the audit time.
 - 50% of time for audit.
 - 20% of time for post-audit desktop follow-up and reporting. Any follow-up necessary to verify and triangulate evidence on-site shall be additional.

This means that the total time needed to complete the audit may be up to twice that spent auditing the member's premises (on-site or remotely). For smaller members, the percentages above may vary to ensure the certification body is able to evaluate the member's readiness for audit.

- b) Time spent travelling to and from audited locations is not included in the calculation of the duration of the audit days.
- c) The time spent by translators, interpreters, observers and auditors-in-training shall not count in the established audit durations above. Note that the use of translators and interpreters can necessitate additional time.

5.6. The certification body shall follow the requirements below, when combining RJC audits:

- a) LGMS audits shall always be combined with COP audits, provided the COP version is COP 2024 or later. An audit against COP 2019 cannot be combined with an LGMS audit.
- b) Where the LGMS is applicable to a member that is already certified to the COP 2019 version, the member must book a combined COP 2024/LGMS audit within the relevant implementation period for LGMS (see [RJC frequently asked questions \(FAQs\)](#)), even if this means an early recertification against COP. A combined COP/LGMS audit may need up to an additional 25% of audit time compared to a COP audit.
- c) If a member starts dealing in materials subject to one of the mandatory standards while already certified to the other mandatory standard (provided the COP version is COP 2024 or later), the certification body shall verify compliance with the relevant requirements of the new mandatory standard at the same time as conducting a surveillance audit for the existing certification, or shall follow 5.6a-b for recertification, or Section 26, Transfer of Certification, as applicable. The expiry date of the certificate for the newly applicable mandatory standard shall coincide with that of the existing certificate for the other mandatory standard, even if the total length of the new certificate is shorter than three years.

Step 1 – Pre-Certification Activities

- d) To help members achieve time and cost efficiencies in auditing, certification audits for the COP and COC standards should be combined. If a COC audit is being conducted alongside the COP audit, the associated time could be reduced by up to 25% for the COC audit. The certification body shall check with the member whether it wants to combine them. If this is the case, a combined audit plan shall be developed and clearly document how each element applies to each standard.
 - e) If the member chooses not to combine its COP and COC audits, or if a combined audit is not possible, then the auditor shall carry out a COC certification audit only after the member has completed its COP audit, not before. Whether or not the audits are conducted as combined, the expiry date of the COC certificate shall coincide with that of the COP certificate. In the case of queries please contact assurance@responsiblejewellery.com.
- 5.7. To support the broader harmonisation of efforts for responsible business practices, the certification body should facilitate any member request to plan its RJC audit so that it coincides with other audits for external RJC-recognised frameworks or for company protocols such as the De Beers Best Practice Principles and the Signet Responsible Sourcing Protocol. In doing so, the certification body shall ensure the integrity of the RJC certification.

6. HARMONISE EFFORTS FOR RESPONSIBLE BUSINESS PRACTICES: CLAIMS OF EQUIVALENCY WITH RJC-RECOGNISED FRAMEWORKS

The RJC's standards are designed to recognise and align with other frameworks for responsible business practices wherever possible. External certifications against specific standards and initiatives are recognised by the RJC as equivalent to one or more provisions in the RJC standard(s), as per Appendix 4, RJC-Recognised Frameworks.

- 6.1. In these cases, the auditor can use the RJC-recognised external certification as baseline evidence to verify conformity without additional self-assessment or independent review, or with limited additional verification, under specific conditions. However, auditors shall still have the right to take a risk-based approach to further investigate these provisions during an audit if they deem it necessary.
- 6.2. In this regard, the auditor shall obtain the following from the member making any claims to be certified against one or more of the RJC-recognised standards or initiatives listed in Appendix 4, RJC-Recognised Frameworks, for each relevant standard:
 - a) A valid certificate.
 - b) The most recent detailed audit report for the standard or initiative, together with details of any corrective actions identified and plans for rectification.
 - c) Details of any substantial changes to the audit scope since the last external audit.

Step 1 – Pre-Certification Activities

- 6.3. Based on the above documents, the auditor shall:
- a) include details of any external certificates and their expiry dates in the audit report.
 - b) verify the last audit date relating to the relevant certificate – this shall not exceed 12 months.
 - c) verify that the external certification scope applies to the member’s RJC certification scope and the specific entity/facility being audited – make sure that any entities, individual facilities or parts of the business that are not covered by the external certificate are included in the RJC certification scope (see Section 3, Certification Scope).
 - d) review the latest external audit report and corrective action plan (where applicable) to verify the assessment and ensure:
 - i. there are no open major or critical nonconformities (or equivalent, as identified in Appendix 2, Critical Provisions) or high risks. If any such nonconformities have not been corrected, the equivalent RJC provision shall be assessed to determine conformity.
 - ii. for any minor nonconformities, a corrective action plan is in place to be implemented within the next 12 months.
 - e) document the findings in the audit report (see Section 15, Audit Report), including any minor nonconformities identified under these RJC-recognised frameworks that have corrective action plans pending implementation.
 - f) identify the equivalent provisions of the relevant RJC standard(s) that required additional verification and explain why.

News of any further initiatives or standards that the RJC officially recognises as equivalent are published on the RJC website at [RJC harmonisation](#). Questions about an initiative not listed here should be referred to assurance@responsiblejewellery.com.

7. DETERMINING AUDIT OBJECTIVES AND SCOPE

- 7.1. The certification body shall consider the following audit objectives:
- Determine the member’s compliance with the requirements of the RJC standard(s) and the member’s own defined processes and documentation.
 - Determine the ability of the member’s systems and processes to ensure the member meets applicable statutory, regulatory and contractual requirements. Please note that an RJC certification audit is not a legal compliance audit.
 - Determine the effectiveness of the member’s systems and processes to ensure the member can reasonably expect to achieve the objectives of the RJC standard(s) on an ongoing basis.
- 7.2. Based on the above steps and information, the certification body shall determine the audit scope, which shall describe the extent and boundaries of the audit such as entities/facilities, organisational units, activities and processes to be audited against applicable requirements.

Step 1 – Pre-Certification Activities

- 7.3. The audit scope shall comprise entities/facilities and business activities from within the member’s RJC certification scope. For multi-site members, the central office shall be visited before other entities/facilities in scope. Where an entity/facility cannot be included in the audit scope for geopolitical reasons, e.g. armed conflict, its exclusion from the audit scope shall be assessed and documented by the certification body and marked accordingly in the certification documentation.
- 7.4. The certification body shall ensure that the audit teams are thoroughly briefed prior to the audit; materials or processes NOT in the member’s RJC scope are not subject to an RJC audit, e.g. watch batteries.
- 7.5. In all cases, when defining the audit scope, the certification body shall make sure that it:
- takes account of risk and relevance using available information (e.g. the member’s self-assessment, public reports, legislative frameworks, previous audit scopes and results, corrective action plans and any external RJC-recognised frameworks).
 - can deliver the service within the recommended time limits, or as otherwise negotiated (see Tables 2–5).
 - will be able to get the necessary objective evidence to produce a statement of conformity and make a certification decision.
 - documents the scope in the audit plan detailing which provisions are to be assessed at which entities/facilities and which external recognised frameworks, if any, it has verified or will review further during the audit (see Appendix 4, RJC-Recognised Frameworks).
 - communicates the audit plan to the member in a timely manner.
 - records the audit date(s) via the Auditor Portal within the required timelines for RJC visibility as per 2.3, by avoiding member downtime periods.

8. MULTI-SITE SAMPLING

- 8.1. For a COP/LGMS audit, the certification body may not visit all the entities/facilities within the member’s certification scope, and in this case shall apply a selection of the same (see 8.3, Multi-site member companies, below). For some types of member activity, it may also be possible to undertake a fully remote or partially remote audit, depending on eligibility criteria (see Section 10, Decide on On-Site or Remote Audit Methodology).
- 8.2. For a COC certification audit, the certification body shall include every entity/facility that falls within the member’s certification scope in the audit scope. For a COC surveillance audit, the certification body can apply sampling as per Table 6 for multi-site members that are eligible for sampling. Member-owned warehousing, logistics and transport are considered services and subject to risk assessment and are not part of the COC certification and audit scope. Note that a fully remote audit is not permitted for COC certification audits.

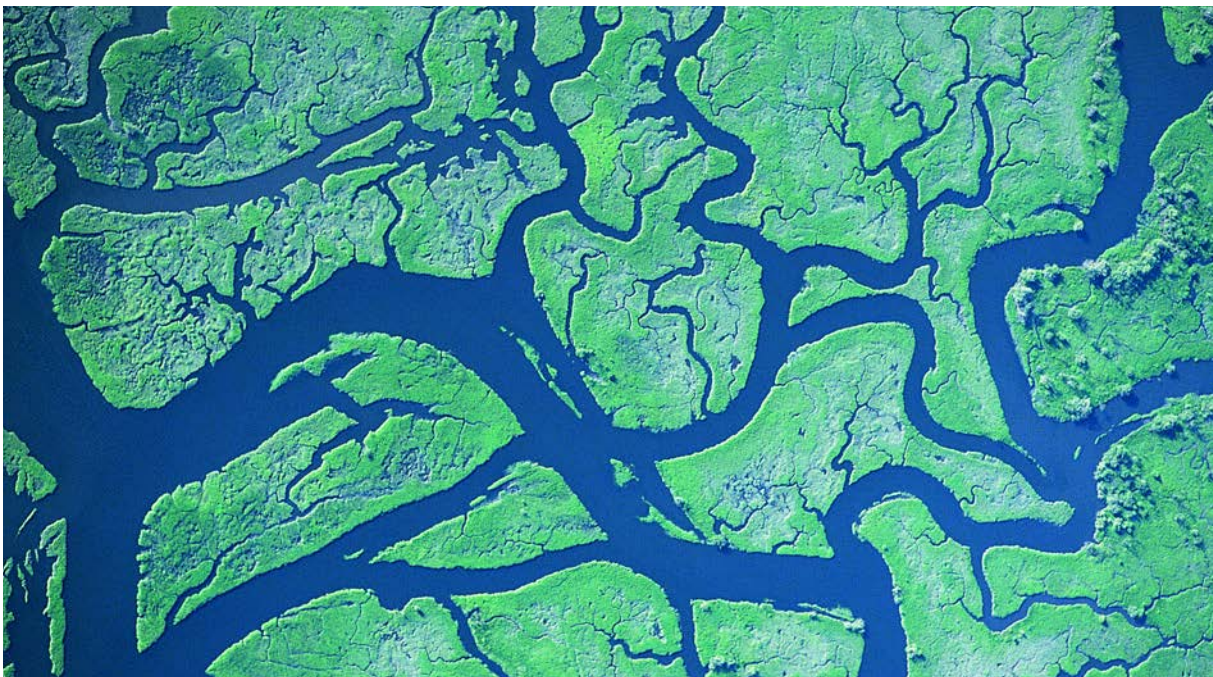
Step 1 – Pre-Certification Activities

8.3. Multi-site member companies

In many cases, the RJC member being audited will be a multi-site company. The RJC defines this type of company as any member with an identified central office (functional or central office, geographic headquarters, etc.) that controls or oversees a network of owned or joint-venture sites. A multi-site company need not be a single legal entity, but all of its entities/facilities have legal or contractual links with the central office and are subject to common management. Examples include:

- mining companies with a combination of mines and concentration/processing plants, offices and sales operations. Note that all the mines and concentration/processing plants operating as entities/facilities under a mining member should be audited across the three-year certification cycle. The certification body shall provide a written justification for any mines and concentration/processing plants under a mining member that are not audited during the three-year cycle.
- manufacturing companies with a network of factories.
- retailers with multiple outlet stores (or any other company that has multiple branches).
- companies with a mix of manufacturing sites and retail outlets.
- service companies with multiple sites (e.g. a transport provider with multiple depots).
- companies operating with franchises.

Note that sites may be permanent (e.g. mines, factories, retail branches, etc.) or temporary (e.g. construction sites, project sites, testing facilities, etc.).



Step 1 – Pre-Certification Activities

8.3.1. For multi-site member companies, the certification body may choose to limit the audit to the central office and a representative sample of entities/facilities under the member's certification scope. To this end, it shall use the criteria below to determine whether a multi-site company is eligible for sampling. Note that entities/facilities with fundamentally different activities or management systems cannot be grouped together for sampling purposes, even if they are part of the same certification scope of a multi-site member. The sampling criteria are that:

- the different entities/facilities largely comprise retail or other low-risk outlets; or
- most of the activities undertaken, equipment used and products made and sold at each entity/facility are substantially the same; and
- the risk profiles for the entities/facilities and operating conditions are similar in nature; and
- the activities, equipment and products are governed by common management systems, under the direction of the central office.

8.3.2. After establishing sampling eligibility as per the above, the certification body shall use Table 6, below, to select the minimum number of entities/facilities to audit, in addition to the central office, per each category (activity) of the eligible entities/facilities (e.g. if a member has six sales offices, then four need to be included in the audit scope at initial certification; if the same member also has eight warehouses, then four need to be included in the audit scope at initial certification, etc.).

TABLE 6. MINIMUM NUMBER* OF ENTITIES/FACILITIES TO VISIT (EXCLUDING THE CENTRAL OFFICE) FOR RJC AUDITS

NUMBER OF ELIGIBLE ENTITIES/ FACILITIES	COP/LGMS INITIAL CERTIFICATION AUDIT	COP/LGMS/COC SURVEILLANCE AUDIT	COP/LGMS RECERTIFICATION AUDIT
1	1	1	1
2	2	1	2
3	3	2	2
4–10	4	2	3
11–30	5	3	4
31–60	6	3	4
61–80	7	4	5
81–100	8	4	5
≥101	Square root, multiplied by 0.9, rounded up to the nearest whole number	Square root, multiplied by 0.5, rounded up to the nearest whole number	Square root, multiplied by 0.8, rounded up to the nearest whole number
If, and only if, square root methodology is not practical and feasible in economic and operative terms, the reduced sampling size below can be applied conditionally and only to retail outlet stores (whether owned or franchised) and where there are no significant risks based on geographic or other factors.			
≥101	10	5	8

*These minimum numbers may increase depending on the results of the certification in terms of nonconformities.

Step 1 – Pre-Certification Activities

- 8.3.3. The certification body shall choose which entities/facilities to audit before starting the audit. However, if the auditor decides they need to change the number or type of entities/facilities to audit as a result of their initial findings at the central office, the certification body shall inform the member, provide a reason justifying the change and give the member enough time to prepare for the change.
- 8.3.4. The certification body shall choose which and how many entities/facilities to audit in a way that ensures the audit can confidently verify full conformity with the RJC standard(s) while remaining practical and feasible in economic and operative terms.
- 8.3.5. The audit of any multi-site member shall be completed within six months of the opening meeting.
- 8.3.6. The certification body shall clearly justify the use of the reduced sampling size for retail outlet stores on a risk basis.
- 8.3.7. The auditor shall consider whether nonconformities identified at an individual entity/facility are likely to be identified at other entities/facilities that will therefore also require corrective action.
- 8.3.8. The certification body shall consider the following when selecting entities/facilities, including conditions for reduced retail outlet store sampling:
- Significant variations across entities/facilities in terms of size, shift patterns and work procedures.
 - Complexity of the different entities/facilities' management systems or processes (e.g. mining operations will have more complex systems).
 - Maturity of the member's management systems and processes, and own knowledge of the member. The certification body shall consider the presence of an effective internal audits process and grievance mechanism, including a process for employees to whistleblow/raise concerns.
 - Likely impact of the member's activities, equipment and products on human rights, the environment and health and safety risks.
 - Differences in geography, culture, language, regulatory requirements and risk profiles across entities/facilities. The certification body shall ensure the selection covers key regions in scope and explain the basis on which the 'key' regions were selected.
 - Records of complaints and other relevant aspects of corrective and preventive action.
- 8.3.9. When conducting a subsequent audit, the certification body shall consider the results of previous audits when selecting entities/facilities and also consider the following:
- The number and severity of any nonconformities found. If a retail outlet store had major nonconformities identified in previous certifications, then it needs to be audited again; in addition, the scope needs to be expanded to include other, similar locations where the same issue might be occurring, and others in the reduced sample size need to be visited.
 - Any site-specific changes, or changes to certification scope, that have since been made.
 - Those entities/facilities that have not already been audited (rotate and audit different entities/facilities across subsequent audits, especially with regard to retail outlet stores, unless there is a specific reason for revisiting a particular one). See also the requirements for visiting all mining sites within the three-year cycle under 8.3, Multi-site member companies and 8.5, Incorporating early mining activities (COP only).

Step 1 – Pre-Certification Activities

For more requirements on auditing multi-site companies, see the following documents:

- International Accreditation Forum (IAF), IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization (IAF MD 1:2023).
- ISO 2859-1:1999, Sampling Procedures for Inspection by Attributes, Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection (second edition amended in 2011 – third edition under development).

8.4. Virtual entities/facilities

Some RJC members may be virtual entities/facilities and therefore an on-site audit might not be possible.

- a) When remotely auditing virtual entities/facilities, understood as virtual locations where a member performs work or provides a service using an online environment allowing persons from different physical locations to execute processes⁸ the certification body shall consider:
- whether there are any processes that are executed in a physical environment (owned by the member or third parties), e.g. warehousing, physical testing in laboratories, logistics, installation or repairs to physical products, where the virtual member has ownership of the materials handled. In this case, parts of the audit may need to take place on-site unless the physical location is already RJC-certified under its own or another member's certification scope.
 - whether all employees performing work are located remotely and working in a virtual environment (e.g. the cloud).

8.5. Incorporating early mining activities (COP only):

- a) When auditing a member that carries out activities from exploration to the pre-commissioned stage of a mine's life cycle, the certification body shall use the criteria given in Table 7 below to decide which activities to include in the audit scope.

Note that these early stages of a mine's life cycle encompass a wide range of activities, and the certification body may need to use auditors' professional judgement to decide how to sample these through desktop reviews and on-site visits. For instance, mining exploration involving remote surveillance (e.g. aerial surveys) or minimal disturbance may not warrant an on-site visit, although a desktop review may still be carried out. However, if these exploration activities include pilot-scale operations or construction of mining operations, an on-site visit may be necessary.

⁸ IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization (IAF MD 1:2023) https://iaf.nu/iaf_system/uploads/documents/IAF_MD1_Issue_3_181020231.pdf.

Step 1 – Pre-Certification Activities

TABLE 7. CRITERIA FOR INCLUDING ACTIVITIES FROM MINING EXPLORATION TO PRE-COMMISSIONED STAGES IN A COP AUDIT SCOPE

ELIGIBLE FOR AUDIT SCOPE INCLUSION FOR A DESKTOP AUDIT (see b)	ELIGIBLE FOR AUDIT SCOPE INCLUSION FOR A DESKTOP AUDIT* OR ON-SITE VISIT	ELIGIBLE FOR AUDIT SCOPE INCLUSION FOR AN ON-SITE VISIT
<p>Activities leading up to the ore body delineation stage, including:</p> <ul style="list-style-type: none"> • prospecting; or • area selection; or • target identification; or • document or small-scale drilling of ore sample collection (e.g. exploration involving a single drilling rig with little or no vegetation clearance or disturbance to the local community). 	<p>Delineation or evaluation activities, taking into consideration:</p> <ul style="list-style-type: none"> • scale, expenditures (e.g. US\$100 million cut-off); or • presence of controlled social or environmental issues; or • works such as new airstrips, permanent or high-impact roads, and multi-year camps; or • bulk sampling and on-site processing facilities; or • start of feasibility studies. 	<p>Projects where:</p> <ul style="list-style-type: none"> • there are works such as new airstrips, permanent or high-impact roads, and multi-year camps; or • the mine is now under construction; or • there are significant social or environmental issues; or • a free, prior and informed consent (FPIC) process is under way (if applicable).

- b) If the member has no other active mining facilities, the certification body may need to include a representative sample of these activities in the audit scope for on-site visits.



Step 1 – Pre-Certification Activities

9. COC OUTSOURCED CONTRACTORS

9.1. When conducting COC certification audits (including surveillance and extension to scope, if applicable), the auditor shall do the following:

9.1.1. Audit all of the member's high-risk outsourced contractors (criteria dependent) to ensure that the member has conducted its risk assessments, on-site visits and any mitigation actions verifying that high-risk outsourced contractors conform to COC 2024 provision 3/COC 2017 provision 5 (Outsourcing Contractors and Service Companies).

High-risk outsourced contractors are classified as those that change the physical properties of the material or product, and the typical activities covered are listed in the COC guidance document. Outsourced contractors who do not change the physical properties of the product are not high risk.

NOTE: The physical properties of a metal are its intrinsic characteristics. At room temperature and standard atmospheric pressure, a dimensional change or a form change does not materially affect the physical properties of such material. However, the possibility that non-COC materials may be added to or mixed with segregated COC materials presents a high risk of changes to the physical properties of the material or product.

9.1.2. Audit the outsourced contractors identified as medium risk via a recognised sampling methodology and assess the member's overall due diligence programme. Audits of medium-risk outsourced contractors can be assessed remotely.

Medium-risk outsourced contractors are classified as those that add to or adapt the physical properties of the material or product, through activities such as plating, stone setting or similar.

9.1.3. Verify that the correct risk rating has been applied to low-risk outsourced contractors.

9.1.3.1. The auditor shall consider the reasons below and may decide to conduct an audit of low-risk outsourced contractors:

- a) The member has not sufficiently assessed a low-risk outsourced contractor within the past 18 months.
- b) The auditor finds a discrepancy with material received from a contractor and needs to investigate further.
- c) The auditor has any other justifiable reason to assess contractors' processes or conformity with the relevant COC provisions.

Low-risk outsourced contractors are classified as those that do not change, adapt or add to the physical properties of the material or product through activities such as polishing, engraving and hallmarking.

9.2. When an outsourced contractor provides a number of activities with a range of associated risks, the risk level assigned (see above) to that outsourced contractor shall always be highest risk. When the auditor considers that a member has mis-classified the risk level of an outsourced contractor, they shall refer to the descriptions above and to the COC guidance document section dedicated to COC 2024 provision 3.1, to clarify and revisit the member's process for classifying the risk level of outsourced contractors. This may require a deeper assessment of the member's process and the auditing of a larger sample of contractors.

Step 1 – Pre-Certification Activities

- 9.3. Member retail/distribution/logistics entities shall be treated as low-risk outsourced contractors/ service providers for the member to conduct its own risk assessment and management. The auditor shall verify that the member's processes are effective in this regard.
- 9.4. An audit of each member's outsourced contractor should take no longer than 0.5 days, unless the outsourced contractor's circumstances require more time (for example, multiple locations, large processing quantities, complex processes). When the auditor recommends a longer audit time than 0.5 days for each outsourced contractor, they should provide the rationale for this to the member. Given the limited scope of the assessment at each outsourced contractor site, consideration should be given to whether these assessments can be conducted remotely without affecting the effectiveness of the audit, in order to minimise the travelling time and costs, in line with Section 10, Decide on On-Site or Remote Audit Methodology.
- 9.5. Total time spent at outsourced contractors should not normally exceed the total time spent on the rest of the COC audit (including planning, on-site time, off-site time and reporting). This can be exceeded if the circumstances of the COC audit warrant this, such as the (high) number of outsourced contractors, activity risks present or the geographic location of the facilities.
- 9.6. For shared outsourced contractors (i.e. where the same entity/facility is used by two or more RJC members), if the member can share an audit report conducted by an RJC auditor that is less than 12 months old and demonstrates full conformity, this can be used as evidence of conformity and as a substitute for an additional on-site audit.
- 9.7. The objective of the audit is to verify the member's risk assessment and on-site assessment and whether the outsourced contractor is compliant with the relevant COC provision. However, if an auditor witnesses a critical situation (related to the critical provisions of the COP, such as child labour, human rights violations or evidence of failings in supplier due diligence), they should notify the outsourced contractor and the RJC member, if reporting the issue does not put individuals at risk, and shall notify the certification body immediately of this situation. The certification body shall inform the RJC as soon as possible.

10. DECIDE ON ON-SITE OR REMOTE AUDIT METHODOLOGY

The RJC recognises that effective remote audit practice can support a more resilient and flexible audit process through increased time efficiency, lower costs and lower carbon footprint, and facilitate access to a broader range of experts⁹ and certification continuity. It can also improve the potential reach of audits by increasing the number and type of entities/facilities that can be covered, for example by making it possible for entities/facilities where there is no local presence of auditors to be audited, or for specific topics to be evaluated across a wider sample of locations in a time- and cost-effective manner.

At the same time, the inherent nature of the remote audit requires specific conditions in order for the integrity and robustness of the audit programme to be maintained. The RJC adopts a scenario-driven approach to remote auditing, defined as a combination of prescriptive audit types and formats and member risk factors.¹⁰

9 Better Gold Initiative, Remote Audits and Assessments. Experiences from the forestry and mining sectors, p. 24, https://www.projekt-consult.de/newsletter/downloads/641266/BGI_Report_-_Remote_Assessments.pdf.

10 ISEAL Guidance – Remote Auditing Good Practices p. 5 <https://www.isealalliance.org/sites/default/files/resource/2021-03/Remote%20Auditing%20Good%20Practices%20ISEAL%20Guidance%20v0.1%20March%202021.pdf>.

Step 1 – Pre-Certification Activities

- 10.1. When considering the use of remote audit elements, either as regular assessment tools or for exceptional circumstances amounting to force majeure, the certification body shall follow the remote auditing process and protocol described in Appendix 9, Remote Audit Protocol. In particular:
- conduct an eligibility criteria analysis (by completing the applicable questionnaires) to determine whether the entity/facility is eligible and for what type and format of remote audit.
 - for combined audits, ensure all schemes covered allow for a remote audit.
 - record the remote audit in the RJC Auditor Portal, including the completed eligibility analysis questionnaire(s), at least five working days before the audit takes place.
 - for remote audit elements used due to force majeure only, request and obtain RJC approval prior to conducting the audit.

11. AUDIT TEAM SELECTION AND ASSIGNMENT

- 11.1. The audit may be carried out by one or more individual auditors and the audit team may include topic/local experts, observers, translators and facilitators.
- 11.2. In all cases, the audit team shall include a lead auditor, who is responsible for ensuring the audit is conducted and completed efficiently and effectively, within the approved scope and plan.
- 11.3. The audit team shall include appropriate expertise based on the activities undertaken to address specific risks, e.g. for mining: health and safety, tailings, biodiversity, community relations, etc., and human rights issues that may be prevalent across the supply chain (also see 11.10-13).
- 11.4. The lead auditor shall:
- appoint the audit team and direct its activities.
 - consult with the RJC member when determining the audit scope and plan.
 - prepare the audit plan and communicate it to the RJC member and audit team.
 - get the relevant background information needed to meet the audit objectives.
 - be present at the audits of the principal entities/facilities and direct all other audits for the remaining entities/facilities, for a multi-site member.
 - coordinate the preparation of working documents.
 - resolve any problems that arise during the audit.
 - recognise when audit objectives are unattainable and report the reasons to the RJC member and the certification body.
 - represent the audit team in all discussions.
 - notify the RJC member of the audit findings.
 - approve corrective action plans for any nonconformities identified in the audit.
 - report the audit results to the RJC member and the certification body, including signing a statement of conformity.
- 11.5. The audit team members **between them** shall have the **totality of the competence** necessary in terms of knowledge, skills and risk areas regarding geographical and member activity, to meet the audit's objectives effectively and efficiently.

Step 1 – Pre-Certification Activities

- 11.6. Every auditor within the team shall:
- a) be independent and without any conflict of interest.
 - b) be RJC approved and trained either:
 - as a lead auditor with full competence for the entity/facility they are auditing if sole auditor; or
 - as part of an audit team that overall has at least one lead auditor and altogether fully covers the geographical and activity fora of the entity/facility being audited.
 - c) have knowledge of practices, processes and equipment typically used by the member being audited.
- 11.7. The certification body shall consider the factors below, which are expected to influence the precise size and composition of the audit team:
- a) Audit scope.
 - b) Composition of previous audit team:
 - The certification body shall have documented and effective processes in place to minimise the risks that may be posed by auditor familiarity, lack of impartiality or conflict of interest, and shall consider mitigation measures such as, but not limited to, auditor rotation, second auditor shadowing/review, etc.
 - Where rotation is in place, each lead auditor shall review the previous audit report to determine whether a nonconformity is reoccurring.
 - c) Availability of qualified auditors.
 - d) Geographic location of the member being audited.
 - e) Requirements for specialist knowledge including risks.
 - f) Cultural and language considerations (e.g. national or regional social familiarity, religion, gender, etc.).
- 11.8. The lead auditor, in consultation with the audit team, shall assign to each team member responsibility for auditing specific processes, functions, entities/facilities, areas or activities. Such assignments shall take into account the need for competence, and the effective and efficient use of the audit team, as well as different roles and responsibilities of auditors, auditors-in-training and topic/local experts. Changes to the work assignments may be made as the audit progresses to ensure achievement of the audit objectives. If the audit is being witnessed by the oversight body, the lead auditor shall immediately inform the assessor of any changes made to the audit plan or work assignment.
- 11.9. Auditors-in-training may participate in the audit, provided an auditor is appointed as an evaluator. The evaluator shall be competent to take over the duties of and have final responsibility for the activities and findings of the auditor-in-training.
- 11.10. The certification body may include topic/local experts or translators in the audit team to provide specific subject-matter expertise or to help translate foreign-language evidence.

Step 1 – Pre-Certification Activities

- 11.11. The certification body shall choose experts and translators in a way that does not allow them to unduly influence the audit. Note that no one involved in the RJC member's development of management systems or in its self-assessment (including personnel, external consultants or advisors) shall be part of the audit team, as this represents a conflict of interest.
- 11.12. A topic/local expert:
- may provide advice to the audit team for the preparation, planning or audit.
 - shall not be the only audit team member on-site.
 - shall be under the on-site or remote supervision of the lead auditor (or another auditor delegated), if present during the audit, and can contribute towards the audit in-person days.
- 11.13. Any topic/local experts, translators or interpreters used shall be assigned/recruited by the certification body, be independent/external of the member and the entity/facility being audited (e.g. workers cannot translate for each other) and be available to assist the audit team on-site or remotely, as applicable.
- 11.14. The certification body shall agree the presence of and justification for observers during an audit activity with the member prior to the audit being conducted.
- 11.15. The audit team shall ensure that observers do not influence or interfere in the audit process or outcome of the audit. Observers can be member's staff, consultants, RJC personnel, witnessing oversight or accreditation body personnel, regulators or other justified persons.
- 11.16. Where conducting a remote audit, the certification body may include a facilitator for those parts that are more difficult to carry out remotely, such as worker interviews on social topics or site tours. These elements shall only be conducted if there are RJC lead auditors remotely and closely guiding facilitators on the ground (for full details, see Appendix 9, Remote Audit Protocol).
- 11.17. If any topic/local experts, translators or facilitators are used to support the audit, or any auditors-in-training participate, the certification body shall identify them in the audit report and explain their role, where applicable.
- 11.18. As a group, the audit team shall:
- support, and follow the directions of, the lead auditor.
 - plan and carry out the assigned tasks objectively, effectively and efficiently.
 - collect and assess objective evidence.
 - prepare working documents under the direction of the lead auditor.
 - document audit findings.
 - help prepare audit reports.
- 11.19. How the team fulfils these expectations depends on the individual style of auditing. While this may well differ from one auditor to another, all RJC auditors shall abide by the ISO auditing guidelines (see Figure 7). The fundamental objective of using these principles is to ensure that different auditors working independently of one another will reach similar conclusions in similar circumstances.

Step 1 – Pre-Certification Activities

FIGURE 7. THE SEVEN PRINCIPLES FOR EFFECTIVE AUDITING AS IDENTIFIED BY ISO 19011¹¹

Principles for effective auditing	<p>1 INTEGRITY</p> <p>The foundation of professionalism</p>	<p>Do your work ethically, with honesty and responsibility. Only undertake activities if you are competent to do so. Work in an impartial way.</p> <p>Be sensitive to potential influences on your judgement.</p>
	<p>2 FAIR PRESENTATION</p> <p>The obligation to report truthfully and accurately</p>	<p>Ensure your reports and conclusions truthfully and accurately reflect the company's practices.</p> <p>Report significant obstacles and differences of opinion.</p> <p>Ensure all communications are truthful, accurate, objective, timely, clear and complete.</p>
	<p>3 DUE PROFESSIONAL CARE</p> <p>The application of diligence and judgement in assessments</p>	<p>Exercise competence and care commensurate with the importance of the task you perform and the confidence placed in you.</p>
	<p>4 CONFIDENTIALITY</p> <p>Security of information</p>	<p>Be discreet when using data acquired during audits.</p> <p>Protect sensitive or confidential information.</p> <p>Never use audit information for personal gain.</p>
	<p>5 INDEPENDENCE</p> <p>The basis for impartiality and objectivity of conclusions</p>	<p>Be independent of the company and activity under audit.</p> <p>Remain free from bias and avoid any situation that could undermine your capacity for impartiality (i.e. conflicts of interest – for example, a personal, professional or financial relationship with the company you are auditing).</p>
	<p>6 EVIDENCE-BASED APPROACH</p> <p>The rational method for reaching reliable and reproducible conclusions in a systemic assessment process</p>	<p>Make sure your findings and conclusions are based purely on objective evidence (evidence that is verifiable).</p> <p>Use appropriate sampling techniques to ensure you gather enough objective evidence to secure confidence in your results and conclusions.</p>
	<p>7 RISK-BASED APPROACH</p> <p>An audit approach that considers risks and opportunities</p>	<p>Consider risks and opportunities when planning, conducting and reporting your audit.</p> <p>Focus on matters that are significant for the company being audited, and for achieving the audit objectives.</p>

11 ISO 19011:2018 Guidelines for Auditing Management Systems, <https://www.iso.org/standard/70017.html>.

Step 1 – Pre-Certification Activities

12. DOCUMENT AND COMMUNICATE THE AUDIT PLAN

- 12.1. The certification body shall obtain the member's completed or updated self-assessment workbook, or equivalent, as long as all RJC standard(s) provisions are included (if the member used other tools), including any provenance claim(s) the member is making or intends to make, during application stage or up to one month before the evaluation activities, but no later, and shall review the same. The self-assessment workbook shall not be older than six months.
- 12.2. Once the certification body has defined the audit scope and methodology (on-site or remote), calculated the audit time and appointed the audit team, all audit activities shall be carefully documented in an audit plan. The plan shall be communicated to and agreed with the RJC member at least 10 working days before the evaluation starts. This process will give the member time to prepare and, if necessary, suggest changes to minimise disruption to its business. Note that while RJC members can ask to change the time or date of specific activities, they cannot request a change to the audit scope and objectives that the certification body has set.
- 12.3. The certification body shall use the audit plan to outline what activities the audit team will review, when, in which organisational areas and involving which personnel, allowing sufficient flexibility to accommodate changes in emphasis based on information gathered during the audit.
- 12.4. The audit activities should be planned logically in a way that causes minimum disruption to normal business processes while still building the sequence of objective evidence needed to verify conformity. The audit plan should make the best use of available resources (both those of the auditor(s) and those of the RJC member).
- 12.5. Audit plans are typically set out as a timetable. In all cases, they shall include the following information:
 - a) Audit objectives, criteria and scope.
 - b) Dates, places and times of audit, including remote auditing activities, where appropriate.
 - c) Names and roles of auditors (which activities they will be assessing) and accompanying persons, such as topic/local experts, observers or translators.
 - d) The primary language of the audit.
 - e) Business practices and the entities/facilities to be assessed.
 - f) Documentation likely to be reviewed.
 - g) Expected time and duration of each major audit activity.
 - h) Personnel (or functional roles) to be interviewed.
 - i) Outline schedule of meetings to be held (with managers, other employees, contractors and the member's designated RJC coordinator).
 - j) Schedule for revisiting and reviewing information.
 - k) Time allocated for miscellaneous activities such as inductions and breaks.

Step 1 – Pre-Certification Activities

- 12.6. The tasks given to the audit team shall be defined in the audit plan, and require the audit team to:
- a) examine and verify the structure, policies, processes, procedures, records and related documents of the member relevant to the RJC standard(s).
 - b) determine whether these meet all the requirements relevant to the intended scope of certification.
 - c) determine whether the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the member's systems and processes.
 - d) communicate to the member, for it to action, any inconsistencies between the member's policy, objectives and targets.
- 12.7. On sending the audit plan to the member, the certification body shall also send its anti-corruption and conflict-of-interest policies and shall ask the member to:
- a) confirm availability of interviewees and their understanding that all employee interviews will be driven by the auditor with no involvement/interference by the member, and confirm access to documents.
 - b) invite senior management to attend opening and closing meetings.
 - c) arrange for guides to be available during on-site visits.
 - d) confirm any health and safety requirements for visitors.
 - e) make office facilities (including space and meeting rooms) available to conduct interviews and review information.
 - f) arrange appropriate technology facilities for any remote activities.
 - g) arrange for any personal protective equipment the auditors may need when visiting facilities.
 - h) allocate time for inductions and introductions.
 - i) advise all staff of the audit arrangements.

Step 2 – Evaluation



13. INITIAL CERTIFICATION EVALUATION ACTIVITIES

DOCUMENTARY REVIEW

- 13.1. A documentary review shall take place either remotely or on-site, prior to the initial certification audit. Both the documentary review and the audit shall take place within a maximum of six months before the deadline.
- 13.2. The objectives of documentary review are to:
- review the member's supporting documentation, including any external RJC-recognised certifications (see Section 6, Harmonise Efforts for Responsible Business Practices: Claims of Equivalency with RJC-Recognised Frameworks) and any provenance claim(s) the member is making or intends to make.
 - confirm that there are no new elements that may impact the already verified and defined certification scope.
 - undertake discussions with the member to determine the preparedness for audit, including evaluating the level of documentary implementation of the RJC standard(s), and discuss any site-specific conditions.
 - review the member's status and understanding regarding requirements of the RJC standard(s), in particular with respect to significant aspects, processes, objectives and operations, as well as critical provisions, as applicable.
 - review the allocation of resources for audit and agree the details of the audit with the member, as applicable.
 - provide a focus for planning the audit by gaining a sufficient understanding of the member's system, processes and operations in the context of the RJC standard(s).

Step 2 – Evaluation

- 13.3. During this stage, adjustments can be made to the certification scope, audit scope and audit plan to accommodate any new pieces of information resulting from the submitted documentation.
- 13.4. If the certification scope needs to be revised following new information obtained during this review, the certification body shall follow the requirements in 3.5.
- 13.5. The certification body shall communicate to the member documented conclusions with regard to the fulfilment of the documentary review objectives and the readiness for audit, including identification of any areas of concern that could be graded as nonconformities during audit.
- 13.6. The documentary review output does not need to meet the full requirements of a report. The documentary review does not require a formal audit plan.
- 13.7. When determining the interval between documentary review and audit, the certification body shall ensure that the same is appropriate and allows the member to resolve areas of concern identified during the documentary review, while not exceeding the six-month timeline for completion.
- 13.8. The certification body may also need to revise its arrangements for audit. If any significant changes that would impact the member's system and processes occur, the certification body shall consider the need to repeat all or part of the documentary review stage. The certification body shall inform the member that the results of the documentary review may lead to postponement or cancellation of the audit, where applicable.
- 13.9. Documentary review may also be used as part of surveillance and recertification audits or special audits in situations where there have been significant changes to the member's business, system, processes or activities or the context in which the member operates, e.g. changes to legislation. The certification body shall assess and decide on the need for documentary review on a case-by-case basis, for such audits.

INITIAL CERTIFICATION AUDIT

- 13.10. The purpose of the audit is to evaluate whether the business, systems and processes of an RJC member (or an entity under its control) conform to RJC requirements as set out in the RJC standards, based on evaluation activities such as documentation review, interviews, observation, sampling and audits. To this end, the certification body shall ensure all necessary information and/or documentation is obtained for performing the evaluation tasks.
- 13.11. The audit shall take place either on-site or remotely, as applicable (see Section 10, Decide on On-Site or Remote Audit Methodology), and it shall include the auditing of at least the following:
- a) Information and evidence of conformity with all requirements of the RJC standard(s).
 - b) Implementation of the member's processes, policies and procedures, including operational control and management responsibility for the policies.
 - c) Performance monitoring, measuring, reporting and reviewing against all applicable RJC standard(s) provisions.
- 13.12. The audit team shall analyse all information and evidence gathered during documentary review and audit, to review the audit findings and agree on the audit conclusions.

Step 2 – Evaluation

14. CONDUCTING AUDITS

- 14.1. The certification body shall have a process for conducting audits. This process shall include an opening meeting at the start of the audit and a closing meeting at the conclusion of the audit. Where any part of the audit is conducted by electronic means (either remotely and/or for virtual businesses), the certification body shall ensure that such activities are conducted by personnel with appropriate competence and following the remote auditing protocol (see Section 10, Decide on On-site or Remote Audit Methodology). The evidence obtained during such an audit shall be sufficient to enable the auditor to take an informed decision on conformity with the requirement in question.

MEET TO OPEN THE AUDIT

- 14.2. A formal opening meeting shall be held with the member's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting, usually conducted by the lead auditor, is to provide a short explanation of the audit objectives and how the audit activities will be undertaken. The degree of detail shall be consistent with the familiarity of the member with the audit process, and the following actions shall be completed:
- a) Introduce the audit team to the RJC member's representatives.
 - b) Confirm briefly the purpose and scope of the certification and the audit.
 - c) Review audit plan (timetable of activities).
 - d) Provide a short summary of the methods and procedures used to conduct the audit.
 - e) Explain the confidential nature of the audit process and confirm report distribution.
 - f) Explain the grading of minor and major nonconformities and critical breaches and how findings shall be reported.
 - g) Explain timelines and consequences of potential findings.
 - h) Arrange for guides to accompany the audit team, as required.
 - i) Check if there are any on-site rules the audit team should follow.
 - j) Answer any questions that the meeting participants may have.
- 14.3. The auditor or audit team shall record the job titles and names of all meeting participants, obtain signatures to confirm their attendance and include the agenda and brief notes of the discussion.

COMMUNICATE DURING THE AUDIT

- 14.4. During the audit, the audit team shall periodically assess audit progress and exchange information. The lead auditor shall reassign work as needed between the audit team members (and inform the oversight assessor if the audit is being witnessed) and periodically communicate the progress of the audit and any concerns to the member.

Step 2 – Evaluation

- 14.5. Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g. safety, restricted access to the member's information and/or employees), the lead auditor shall report this to the member (unless the reported issues might put individuals at risk, including the auditor; see 14.27(e) on reporting sensitive issues), and to the certification body to determine appropriate action. The certification body may inform the RJC. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The lead auditor shall report the outcome of the action taken to the certification body.
- 14.6. The lead auditor shall review with the member any need for changes to the certification scope and/or audit scope that become apparent as auditing activities progress and report this to the certification body, which shall follow the process described in 3.5, where applicable.

COLLECT, SAMPLE AND RECORD OBJECTIVE EVIDENCE

- 14.7. Objective evidence shall be any verifiable information, record, observation or statement of fact gathered during an audit.
- 14.8. Objective evidence shall involve assessing, verifying and reviewing business practices and activities; it shall be qualitative or quantitative and shall comprise:
- a) documentation (hard or soft copy): this includes written policies and procedures for implementing the RJC standard(s), forms and records generated from implementing practices and processes or verified statements.
 - 1) For an initial certification audit, the auditor shall review records and other documents for the previous 12 months.
 - 2) For a surveillance audit, the auditor shall review records and other documents for at least the period since the previous (re)certification audit.
 - 3) For a recertification audit, the auditor shall review records and other documents for at least the previous 36 months for those records not reviewed at the surveillance audit, or for the time period since the surveillance audit for those records that were reviewed at surveillance.
 - 4) In some cases, this may not be sufficient to provide accurate and useful evidence, and the auditor will need to see older documents (see Appendix 6, Examples of Records and Documentary Evidence).
 - 5) In some cases, it may not be possible to find documentary evidence to support a finding, especially in relation to human rights issues. In such cases, where there is sufficient corroboration, a finding may be raised in the absence of documentary evidence.
 - b) observations: information gathered by observing activities and practices can be used as objective evidence, but it is important to verify an understanding of what has been observed.
 - c) testimonials: these comprise information gathered from employee interviews, which can be verified by reviewing records, observing activities or interviewing others.
- 14.9. For any materials, components or products purchased and handled by the member up to 36 months prior to the initial COC certification audit and which the member wishes to include in the audit scope, the auditor shall verify whether the member can demonstrate that these have been handled and processed in accordance with the requirements of the COC standard. They can then be sold as COC materials once certification is achieved.

Step 2 – Evaluation

- 14.10. Because objective evidence serves as the basis on which the auditor determines conformity with the RJC standards, it shall be clearly and unambiguously recorded, relevant to the period or scope of the assessment, and relevant to what is being assessed or verified and is also traceable.

Examples of objective evidence include, but are not limited to:

- organisational charts outlining structure, responsibilities and authorities.
 - written materials describing company policies, processes and products.
 - verified statements of fact.
 - legal permits, licences or other authorisations and related documents and correspondence.
 - reviews of previous assessments.
 - audit reports and certifications from external RJC-recognised frameworks.
 - communications with interested parties, including neighbours and other stakeholders, particularly for, but not limited to, mines or processing plants as entities/facilities under a mining member's scope.
 - risk assessment registers.
 - photographic evidence.
 - oral reports of grievances from stakeholders, particularly for, but not limited to, mines or processing plants as entities/facilities under a mining member's scope.
 - other objective means of documentation.
- 14.11. The auditor shall use the audit plan and Appendix 8, Guidelines for Auditors: Conducting Effective Audits to guide the process of collecting, sampling and recording objective evidence. Experienced auditors may not necessarily need to follow a stepwise approach to the collection of objective evidence and may be able to do all three tasks at the same time.
- 14.12. The process of collecting objective evidence requires some level of sampling – for example, reviewing a representative sample of documents and records, interviewing a representative sample of personnel or observing a representative sample of key functions.
- 14.12.1. The methods used to define the samples shall ensure that they are representative and free from bias. Ultimately, the sample shall be adequate to objectively support the conformity grading.
- 14.12.2. In part, ensuring a robust sample is about ensuring an appropriately sized sample in relation to the total population. This can serve to strengthen or undermine trust in the audit findings. The auditor shall ensure the sample size allows others to be reasonably confident that the larger group has been represented.
- 14.12.3. In addition, ensuring a robust sample is about using the right sampling technique. The auditor can choose samples based on their professional and informed judgement (e.g. to support suspicion of a problem) or through probabilistic sampling approaches (e.g. random sampling). Either way, the auditor shall make sure they collect enough samples to ensure they have the necessary evidence to verify whether systems and processes are in place and whether they are effective (for more guidance, see Appendix 7, Sampling Techniques).
- 14.13. The auditor shall record details of all objective evidence collected, including where it came from. Where data are obtained as a result of worker interviews, the auditor shall record the information but disguise any information that could identify the individual.

Step 2 – Evaluation

- 14.14. Based on the collected objective evidence for everything within the audit scope, the auditor shall:
- verify the certification scope, including whether it covers all parts of the business that actively contribute to the precious metal, diamond and coloured gemstone jewellery and watch supply chain.
 - verify the reasons given for any 'not applicable' conformity gradings present in the member's self-assessment.
 - verify the validity and relevance of any certifications against RJC-recognised frameworks.
 - determine the level of conformity with each certification requirement evaluated.
 - grade each of the applicable certification requirements.

EVALUATE FINDINGS

The purpose of this step is to integrate the individual findings and observations across the audit team and grade the RJC member's conformity with each provision in the audit scope (as per 14.20, Table 8), based on objective evidence and in a clear, unambiguous manner.

- 14.15. Auditors shall also check the guidance associated with the relevant RJC standard(s), as it provides specific instructions on conformity grading for some provisions (for example COP provision 16.2, on overtime and tolerance levels for assessing conformity with COP requirements on working hours).
- This is typically done through a series of audit team meetings held periodically throughout the audit, followed by a final auditors' conference once all interviews and inspections have finished.
- 14.16. The lead auditor shall ensure that opportunities are created to identify commonalities across the team's findings that may impact the RJC member's conformity grading. This is particularly important in relation to multi-site audits where different auditors have led the assessment.
- For example, a group of related, repetitive or persistent minor nonconformities may indicate a company-wide systemic failure or total lack of required controls that justifies a rating of major nonconformity.
- 14.17. The audit team, under the direction of its lead auditor, shall reach a consensus in grading conformity with the applicable RJC standard(s).

GRADE CONFORMITY

Grading conformity is a central part of the RJC certification process. Conformity is graded based on the extent to which the processes and underpinning management systems of a member (or entity under its control) meet each provision and prevent risk to employees, the community or the environment.

- 14.18. All conformity grading shall be clear, unambiguous and supported by objective evidence.
- 14.19. All nonconformities shall be raised against each entity/facility at which they are identified and recorded in the audit report as such. It is important to assess whether a nonconformity is limited to the entity/facility at which it was found or is indicative of a systemic issue (see 14.22 on related, repeated or persistent nonconformities).
- 14.20. Auditors shall use the definitions set out below to grade conformity with the RJC standards:

Step 2 – Evaluation

TABLE 8. CONFORMITY GRADING

CONFORMITY GRADING	RJC STANDARDS
a) Conformity	The member's business practices (including its policies, systems, procedures and processes) perform in a way that conforms to the relevant standard provision.
b) Minor nonconformity	<p>The member's business practices (including its policies, systems, procedures and processes) perform in a way that does not wholly conform to the relevant standard provision, due to an isolated lapse in performance, discipline or control, which does not lead to a major nonconformity, unless, when lapses are taken together, they indicate inadequate implementation as defined under major nonconformity, below.</p> <p>In addition, for COP/LGMS, minor nonconformities do not indicate a breakdown of the systems that underpin conformity, nor result in an imminent significant risk to employees, the community or the environment (see details below). They can occur when the member:</p> <ul style="list-style-type: none"> • is not in compliance with a relevant legislative or regulatory requirement, but has adequately tried to rectify it (if in the know) or made good faith efforts to comply; or • is found to have a business practice that does not breach the standard now but could potentially cause a major nonconformity in the future.
c) Major nonconformity	<p>The member's business practices (including its policies, systems, procedures and processes) perform in a way that does not conform to the relevant standard provision.</p> <p>Major nonconformities occur when there is:</p> <ul style="list-style-type: none"> • a total absence of implementation of the provision. • a group of related, repeated or persistent minor nonconformities, indicating inadequate implementation (see 14.22). • an escalated minor nonconformity, understood as either: <ul style="list-style-type: none"> – a minor nonconformity previously corrected and consecutively identified as reoccurring, where there is evidence that the underlying root cause has not been addressed; and/or – a minor nonconformity with previously approved corrective actions that have not been implemented by the next scheduled mandatory audit (surveillance or certification). <p>This escalation shall not apply if implementation sits outside member control or requires a longer timeline (e.g. waiting for local authorities' response to a request they have submitted and followed up in a timely manner before their audit or similar or to avoid unintended adverse consequences).</p> <p>In addition, for COP/LGMS, major nonconformities indicate an imminent significant risk to employees, the community or the environment (such as risks to life, limb or function); livelihood (wages); access to education; biodiversity; and reputation (of the member or the RJC), as well as risk of environmental damage and risk of RJC logo misuse or miscommunication about certified member status. They can occur when the member:</p> <ul style="list-style-type: none"> • has a persistent (or isolated high-impact) lapse in the performance, discipline or control of its business practices. • has a systemic failure or total lack of the controls needed to manage business risks related to the COP/LGMS. • has knowingly ignored a relevant legislative or regulatory requirement or has not adequately tried to rectify a nonconformity relating to a relevant legislative or regulatory requirement. <p>For COC, any situation that impacts the integrity of the COC or could allow non-eligible material to enter the COC supply chain is a major nonconformity.</p>

Step 2 – Evaluation

CONFORMITY GRADING	RJC STANDARDS
<p>d) Critical breach</p>	<p>For COP/LGMS, a finding is rated as a major nonconformity against any critical provision as per Appendix 2, Critical Provisions, including where serious doubts are raised as to whether the member has the business practices necessary to avoid a critical breach (except major nonconformities that fall within the scope of Table 16.2/23 Tolerance Levels for Assessing Conformance with COP Requirements on Working Hours in the COP 2019/2024 guidance). Note that if the auditor observes practices or conditions that could pose an immediate threat to the health and safety of the workforce or visitors to the site, this can be fully documented and raised as a critical breach that requires immediate rectification.</p> <p>For COC, a critical nonconformity, supported by objective evidence, is raised against any of the COC provisions, in the case of:</p> <ul style="list-style-type: none"> • deliberate falsification of information required to support a conformity grading; or • a systemic failure of the management system to implement the COC; or • a total lack of controls needed to manage risks to the chain of custody.
<p>e) Not applicable</p>	<p>The relevant standard provision genuinely does not apply to the member because of the nature of its business covered by the relevant certification scope – in other words, when it would be illogical or impossible to apply the provision. For example, COP 2024 provisions 32–45 (Responsible Mining and Mineral Processing)/COP 2019 provisions 31–42 (Responsible Mining) are not applicable to members with no mining or exploration activities.</p> <p>The applicability of each provision in the RJC standard(s) is clearly defined in the corresponding guidance documents. Credible and verifiable reasons shall be given for all provisions rated as not applicable. Reasons given by members shall be validated by the independent auditors.</p> <p>Note that a provision with a low risk of a nonconformity does not mean the provision is not applicable.</p>



Step 2 – Evaluation

14.21. The auditor shall review all findings before finalising nonconformity gradings to spot groups of related, repeated or persistent nonconformities, as per 14.22 below.

14.22. A group of minor nonconformities may be elevated to a major nonconformity rating if there is evidence that the minor nonconformities are:

- a) related in terms of the provision, activity being controlled or, even, the nature of the nonconformity across multiple departments, function, entities/facilities; or
- b) repeated, bringing up the same issue throughout the company (which is often symptomatic of a systemic failure or absence of controls); or
- c) persistent, occurring again and again because of ineffective corrective action.

For example, a single instance of a missing material safety data sheet, employee time sheet or incoming invoice verification is considered a genuine single oversight or mistake. But several instances across the company, or over time, indicate a deeper problem with the member's business practices that prevents it from conforming to the RJC standard's record-keeping requirements.

The key to deciding when to elevate a minor nonconformity to a major one is whether it is related to any other minor nonconformities in a way that indicates common root causes through weaknesses in management systems and processes.

14.23. If one or more critical breaches are identified during an audit, the audit shall continue and shall not be stopped due to finding the critical breach, except where there is a need to safeguard at-risk individuals.

14.24. The auditor should consider that the level of records/data can depend on the size/maturity of the member. For example, a small member may have more informal systems, compared to a large member.

If, for example, the auditor knows that objective evidence about a business procedure exists, but it cannot be found because of poor record-keeping practices, then the lack of objective evidence shall result in a nonconformity.

Equally, if there is sufficient consensus through oral testimony from worker interviews about poor practices, but there is no documented evidence to support this, this is considered a nonconformity.

But if, for example, the RJC member has developed a procedure but has not yet had to use it, then there can be no records of it. Therefore, a lack of objective evidence does not demonstrate poor performance and does not automatically constitute a nonconformity.

In this case, the auditor shall simply note the procedure in the audit report and flag it for future review. Of course, even though the auditor cannot say whether the procedure in this case is effectively implemented, they can still determine whether the procedure as written meets the requirements of the relevant provision.

Step 2 – Evaluation

DOCUMENT NONCONFORMITIES

- 14.25. All nonconformities shall include clear and concise details about the nonconforming practice and shall be documented in the audit findings section in the audit report. Regardless of how thoroughly and efficiently the audit was conducted, certification shall not be issued where there is ambiguous, untidy or poorly worded nonconformity information in audit reports.
- 14.26. When documenting a nonconformity, the auditor shall:
- a) state the nature of the nonconformity clearly and exactly and ensure that the extent of the problem is fully communicated to the member.
 - b) clearly reference the standard provision against which the nonconformity has been identified.
 - c) use familiar terminology.
 - d) not draw unsubstantiated conclusions.
 - e) not focus on individuals or their mistakes.
 - f) not criticise.
 - g) cross-reference the requirement of the provision being audited.
 - h) give regulatory or external references where relevant.
 - i) support the finding with relevant and verified objective evidence.
 - j) avoid contradictory messages.
 - k) review the nonconformity with the RJC member to ensure the facts are correct and fair.
 - l) explain the required timelines for corrective action plans and any consequences of the nonconformity grading or if the required timelines are not met.

PREPARE AUDIT CONCLUSIONS

- 14.27. As applicable, under the responsibility of the lead auditor and prior to the closing meeting, the audit team shall:
- a) review the audit findings, and any other appropriate information obtained during the audit, against the audit objectives and audit criteria, and grade the nonconformities.
 - b) agree on the audit conclusions, taking into account the uncertainty inherent in the audit process.
 - c) agree any necessary follow-up actions.
 - d) confirm the appropriateness of the audit programme or identify any modification required for future audits (e.g. scope of certification, audit time or dates, audit team competence).
 - e) document any sensitive issues (which are different from evidence-based critical breaches, as per 14.20, Table 8(d)), such as, but not limited to, a member's lack of transparency, attempts to bribe or to control worker sampling and interview, auditor intimidation/harassment, any issues that if reported might put individuals at risk, whistleblowing, criminal activity, etc., and share them as soon as possible with the certification body only. The certification body shall communicate them to the RJC, where legally allowed, via the Auditor Portal, within a maximum of five working days from identification.
 - f) for COP/LGMS, determine the surveillance format, as per Section 22, Surveillance Audit Format and Scope.

Step 2 – Evaluation

MEET TO CLOSE THE AUDIT

- 14.28. Just as the audit opened with a meeting, so too shall it close with one, whether it be the final closing meeting per a multi-site company or the closing meeting per each entity/facility in audit scope. The purpose of the closing meeting, usually conducted by the lead auditor, is the oral presentation of the audit conclusions and post-audit process.
- 14.29. The auditor shall:
- a) hold the meeting with the member's management and, where appropriate, those responsible for the functions or processes audited.
 - b) record attendance and job titles of all meeting participants, as well as the agenda of the meeting and brief notes of the discussion.
 - c) communicate to the member the need to revise the certification scope following new information obtained during the audit, as applicable. In this case, the auditor shall inform the certification body, which shall follow the requirements in 3.5.
 - d) orally present the findings, including any nonconformities, their grading and the consequences in such a manner that they are understood. Note that 'understood' does not necessarily mean that the nonconformities have been accepted by the member.
 - e) if one or more critical breaches have been identified, communicate to the member that within a maximum of five working days the member's existing certificate, if applicable, shall be suspended and the RJC notified as per 16.3, subject to 14.29(h)). Communicate that this situation shall trigger membership suspension by the RJC, with a risk of further disciplinary actions by the RJC, should the critical breach(es) not be addressed within the allocated timeframe as per 16.7.
 - f) if one or more major nonconformities have been identified, communicate to the member that within a maximum of five working days the member's existing certificate, if applicable, shall be suspended as per 28.1, Table 10(b), subject to 14.29(h).
 - g) communicate the requirement for the member to undergo a surveillance audit between 12 and 18 months from the certificate start date, and confirm the surveillance format (COP/ LGMS only), subject to 14.29(h).
 - h) communicate that the findings, their grading and the surveillance format are preliminary, and details and/or grading may change subject to full evaluation during audit report writing and technical review.
 - i) document the findings, including any nonconformities and their grading, in the audit findings section in the audit report and obtain the member's signed acknowledgement of being informed of and understanding the same. A copy of this signed section shall remain with the member.
 - j) communicate the expected timeframes for receiving a corrective action plan and evidence of implementation from the member; additional evaluation tasks needed to verify that nonconformities have been corrected; and the consequences of failing to meet the timeframes, as applicable.
 - k) communicate the certification body's post-audit activities – i.e. corrective action plan and evidence review, as applicable, technical review, certification decision and certificate issue.
 - l) state that a more detailed report shall be provided (after receipt of the member's corrective action plan and evidence of implementation, as applicable), documenting the overall findings.

Step 2 – Evaluation

- m) confirm the recipients of the completed audit report and communicate about the process to obtain the member's acknowledgement and acceptance of the same, including the fact that the member will not be able to challenge any audit findings at that stage, but only any incorrect factual information.
 - n) clear up any misunderstandings and explain the certification body's process for reporting disputes and handling complaints and appeals.
 - o) discuss and provisionally book a date for the audits below, avoiding member downtime periods:
 - i. An on-site follow-up audit if it is already apparent that it shall be needed to verify the implementation and effectiveness of corrective actions; and/or
 - ii. The next mandatory audit to ensure the member does not miss its next audit deadline. This provisional date shall be confirmed in good time with the member closer to the next audit deadline.
- 14.30. The auditor shall give the member the opportunity to ask questions or to highlight any incorrect factual information.
- 14.31. Any divergences in opinion regarding the audit findings or conclusions between the audit team and the member shall be discussed and resolved where possible.
- 14.32. Any divergences in opinion that are not resolved shall be documented in the grievance section of the audit report and referred to the certification body for resolution as per internal procedures. The certification body may choose to share them with the RJC.
- Any divergences in opinion that are not resolved after referral to the certification body, as per its procedure, shall be escalated to the RJC, based on the RJC Complaints Mechanism (see Governance and Support, Section B, The RJC Complaints Mechanism).
- 14.33. In the case of members with multiple entities/facilities, the auditor shall present their conclusion at the end of the audit for each individual entity/facility, with the caveat that at the overall closing meeting, or during the drafting and technical review of the report, the nonconformities grading might change, depending on whether multiple occurrences of the same finding have been observed across multiple entities/facilities (see 14.22, regarding groups of related, repeated or persistent minor nonconformities).
- 14.34. Should there be any changes or new information provided after the closing meeting regarding the audit conclusions, including nonconformities grading, an updated list of audit findings shall immediately be shared with the member and a signed acknowledgement of its receipt shall be obtained from the member's management representative.
- 14.35. While the auditor may signpost the likely root causes when identifying a nonconformity, it is important that the member conducts a root cause analysis and defines a corrective action plan that will meet its business objectives and ensure conformity with the RJC standard(s).

Step 2 – Evaluation

15. AUDIT REPORT

- 15.1. The certification body shall provide a written report for each audit to the member and the RJC (one report per member, even if the member is a multi-site company).
- 15.2. The certification body shall meet the RJC reporting requirements even if the member wants the auditor to sign a confidentiality agreement to stop them disclosing to third parties confidential or commercially sensitive information that the auditor may have access to during the audits. Confidentiality agreements are common practice for third-party verification and auditing.
- 15.3. The lead auditor shall follow any reporting structure mandated by the RJC for specific provisions to ensure clarity on the processes assessed. The audit report shall include comparison with previous audit assessment and identify performance improvements.
- 15.4. The lead auditor shall use and complete every section of the relevant RJC audit report template to provide a detailed account of the audit, listing the areas that were found to be in conformity, not applicable and in nonconformity with provisions of the relevant RJC standard(s), as the case may be.
- 15.5. The lead auditor shall ensure that the audit report is prepared and shall be responsible for its content. The audit report shall provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made and shall include or refer to the following:
 - a) Identification of the certification body.
 - b) The name and address of the member and the member's representative.
 - c) The type of audit (e.g. initial, surveillance or recertification audit or special audit).
 - d) The audit criteria.
 - e) The audit objectives.
 - f) The audit scope, particularly the identification of the entities/facilities in the member's certification and audit scope and the time of the audit.
 - g) Any deviation from the audit plan and their reasons.
 - h) Any significant issues impacting on the audit programme.
 - i) Identification of the lead auditor, audit team members and any accompanying persons.
 - j) The dates and places where the audit activities (on-site or remote) were conducted.
 - k) Audit findings, provision assessment and reference to evidence and conclusions, consistent with the requirements of the type of audit.
 - l) Significant changes, if any, that have affected the member's system and processes since the last audit took place.
 - m) For COP/LGMS, the surveillance format according to Section 22, Surveillance Audit Format and Scope.

Step 2 – Evaluation

- n) Any unresolved issues, if identified.
 - o) Where applicable, whether the audit is combined, joint or integrated.
 - p) A disclaimer statement indicating that auditing is based on a sampling process of the available information.
 - q) A certification recommendation from the audit team.
 - r) Whether the audited member is effectively controlling the use of the certification documents, certification claims and the RJC logo as per the requirements of the RJC standard(s) and RJC policies.
 - s) Documented corrections and verification of the effectiveness of the same, and documented root cause and corrective actions (and verification of the effectiveness of the same, where applicable) regarding identified nonconformities.
 - t) A statement of conformity.
 - u) A conclusion on the appropriateness of the certification scope.
 - v) Confirmation that the audit objectives have been fulfilled.
- 15.6. When making a statement of conformity, the lead auditor shall consider:
- a) the effectiveness of the member's business practices and controls in meeting the provisions of the RJC standard at hand.
 - b) the severity of the individual nonconformities found during the audit and the effectiveness of the corrective action plan.
 - c) any positive improvements since the last audit (where applicable) in performance, and major achievements and milestones that relate to the RJC standard.
 - d) the member's demonstrable commitment to continual improvement.

16. CORRECTIVE ACTION PLANS AND EVIDENCE – SUBMISSION AND VERIFICATION

- 16.1. In the case of any nonconformity (minor, major or critical), the certification body shall require the member to submit a documented corrective action plan to include all of the below:
- a) Corrections (immediate action) eliminating the identified nonconformity, including supporting evidence.
 - b) A root cause analysis for the identified nonconformities (an understanding of the underlying cause of the actual or anticipated nonconformity so that the proposed corrective action would be deemed effective in addressing the issue).
 - c) Corrective actions intended to remove the root cause and prevent future recurrence.
 - d) The means, resources and timeframe set for implementing each corrective action in the plan.
 - e) Corrective action implementation, where applicable (see 16.7-8).
- 16.2. In addition, corrective action plans should also include preventive actions intended and/or implemented to eliminate the causes of potential nonconformities and avoid unintended consequences.

Step 2 – Evaluation

- 16.3. In the case of critical breach(es), within a maximum of five working days from critical breach identification, the certification body shall:
- formally notify the RJC of the same.

The RJC shall temporarily suspend the member by removing its profile page on the RJC website while the critical breach is under review. The RJC shall inform the member of suspension and available resources that may be useful for the member in addressing the critical breach.
 - where a critical breach is identified during the audit of a certified member, ensure that the auditor's conclusions are technically reviewed and confirmed, and suspend the existing certificate.
 - formally notify the member in writing with details of the certificate suspension, if applicable (also see Section 28, Reduction, Suspension, Withdrawal or Termination of Certification).
- 16.4. Members may use either the RJC corrective action plan template (see Appendix 5, Corrective Action Plan Template, available in multiple languages), or their own equivalent, ensuring that all required information and documentation are included in the corrective action plan as per 16.1.
- 16.5. The identification date of a nonconformity is in most cases the closing meeting (or the overall final closing meeting for multi-site member companies), or, if identification of findings or (change of) grading occurs later during report writing or technical review, the date when the certification body communicated the same to the member.
- 16.6. The certification body shall apply the timeframes at 16.7-8 for corrective action plans and evidence submission, as applicable. During these timeframes, the certification body shall regularly communicate with the member to check on progress and remind it of the consequences of failure to comply with them.
- 16.7. The certification body shall require:
- for all nonconformities** – a corrective action plan, including sufficient correction and evidence of the same, root cause analysis, and proposed corrective actions including timeframes for implementation of corrective actions, to be submitted by the member within **a maximum of one month** from identification date. Note that members will be expected to implement corrective actions as soon as possible if they do not already fall under 16.7(b). Where critical breaches and/or major nonconformities have also been identified, alongside minor nonconformities, and unless the nonconformities relate to serious harmful situations that need to cease immediately, such as child labour, forced labour or similar ongoing harmful conditions, supporting evidence of implementation of corrections may be submitted within three months, together with supporting evidence of corrective action implementation as per 16.7(b).
 - for critical breach/major nonconformity** – sufficient supporting evidence of corrective action implementation to at least achieve regrading as a minor nonconformity with correction in place, as applicable, to be submitted by the member within **a maximum of three months** from identification date, via one or more rounds of evidence submission.

Step 2 – Evaluation

- 16.8. If the member chooses to also submit evidence of corrective action implementation for minor nonconformities after the audit, the certification body shall accept it:
- within a maximum of one month** from identification, together with the corrective action plan, where the audit outcome contains only minor nonconformities; or
 - within a maximum of three months** from identification, where the audit outcome also contains critical breaches and/or major nonconformities, alongside evidence for the latter.
- 16.9. The certification body shall communicate to multi-site members the option to start working on their corrective action plan as soon as the audit findings become available at the individual closing meeting of each audited entity/facility, and not wait for the overall closing meeting, unless entities/facilities under a multi-site member need to address a systemic failure and align with each other.
- 16.10. For initial and recertification audits, any delays in submission of corrective action plans and evidence (where applicable) by the member may delay the certification decision and consequently may lead to a gap in member certification and lack of continuity. For additional consequences of members failing to submit a complete corrective action plan on time, see 21.8, Table 10 (b)) Extension (to scope), reduction, suspension, withdrawal or termination of certification and Section 17, Audit Invalidation.
- 16.11. Within **a maximum of 15 working days** from receipt of the member's corrective action plan and round of evidence, where applicable, the lead auditor shall:
- verify the corrections and supporting evidence to determine whether these are acceptable and effective (including for regraded minor non-conformities from critical breaches or major nonconformities).
 - review the root causes and proposed corrective actions to determine whether these are acceptable and do not introduce any new actual or potential risks, or create unintended consequences.
 - verify the effectiveness of any implemented corrective actions, based on a review of documented information/evidence provided by the member, to ensure that they:
 - were sufficient to close any critical breach or major nonconformity or regrade it as a minor nonconformity.
 - addressed the root cause of a nonconformity (so preventing it from happening again).
 - record the evidence obtained to support the correction of nonconformities.
 - inform the member of the result of the review and verification, including of the necessity of an on-site follow-up audit to fully verify the effectiveness of any implemented corrective actions, where applicable. The date of the follow-up audit shall be confirmed to the member, if already provisionally booked as per 14.29(o)(i), or scheduled as soon as possible, subject to auditor availability and member downtime periods.

Step 2 – Evaluation

- 16.12. If a critical breach has been either regraded as a minor nonconformity or closed within the above timeframes as per 16.7, the certification body shall inform the RJC as soon as possible and provide a brief assessment narrative for reference, clearly documenting the correction and corrective action evidence and any outstanding actions. Based on this information, the RJC shall reinstate the member on the RJC website and inform the member of the same, subject to 28.2.
- 16.13. If a critical breach has not been either regraded as a minor nonconformity or closed within the above timeframes as per 16.7, the certification body shall inform the RJC of the same, as soon as possible. In this case, the RJC shall take further disciplinary actions against the member.
- 16.14. The auditor shall verify the implementation of the approved corrective actions for minor nonconformities at the next scheduled mandatory audit (surveillance or certification).
- 16.15. If the approved corrective actions are not implemented by the next scheduled mandatory audit (surveillance or certification), the certification body shall follow 14.20, Table 8(c), and may escalate any minor nonconformity to a major nonconformity. In this case, the certification body shall require full closure, without the option of regrading as a minor nonconformity again.
- 16.16. When reviewing a corrective action plan, the auditor shall consider whether the enclosed actions are specific, measurable, achievable, realistic and timely (SMART), as per below, and the effectiveness of the corrective actions:
- a) **Specific.** Is the corrective action clear and unambiguous? Does it address the underlying cause of the nonconformity?
 - b) **Measurable.** Can the action's implementation be monitored and measured?
 - c) **Achievable.** Does the action have clearly assigned responsibilities and resources?
 - d) **Realistic.** Is the action realistic and fit for purpose, given the nature of the nonconformity? Has the means and capacity (personnel, infrastructure, funding, etc.) to implement the corrective action been assigned?
 - e) **Timely.** Is the timeframe for completing the action in line with 16.7? Actions involving capital works or approvals may require more time. In these cases, members should set progress milestones within the certification period and establish interim short-term corrective measures to mitigate the effects of the nonconformity.

17. AUDIT INVALIDATION

- 17.1. If an effective and auditor-approved corrective action plan including sufficient evidence of implementation, where applicable, is not in place within **a maximum of six months** from identification of nonconformities, the certification body **shall invalidate the audit** and inform the member of the same, except when an on-site follow-up audit is needed and scheduled but it cannot be completed within the six months due to lack of auditor availability.
- 17.2. If the invalidated audit is a mandatory one, the member shall book and undergo a full certification audit within the next six months to maintain RJC membership (including after an invalidated surveillance as per 23.7).

Step 3 – Report review and certification decision



18. TECHNICAL REVIEW

- 18.1. The certification body shall have a process to conduct an effective technical review of the clarity and completeness of the audit report, statement of conformity and other related information within the audit process, prior to making a certification decision, including determining that:
- a) the information provided by the audit team is sufficient with respect to the certification requirements and certification scope and that the audit team had the appropriate competence for the audit. The technical reviewer shall document any additional information or clarification sought from the audit team or other sources at this stage.
 - b) the narrative concerning provisions audited and reasons why any provisions are not applicable is in line with the RJC requirements in this document.
 - c) for any critical breaches and major nonconformities, it has reviewed, accepted and verified the corrections and corrective action implementation.
 - d) for any minor nonconformities, it has verified corrections and reviewed and accepted the member's corrective action plan (and verified any evidence the member may have submitted within the allocated timeframe, if applicable).
- 18.2. The technical review shall be carried out by the certification body's appointed technical reviewer(s) for RJC audits, who shall not have been involved in the evaluation process.
- 18.3. The recommendation for a certification decision based on the technical review shall be documented, unless the technical review and the certification decision are completed concurrently by the same person.

Step 3 – Report review and certification decision

- 18.4. If one or more critical breaches are identified at technical review, the certification body shall follow provisions 16.3 and 16.7 and in addition:
- a) formally notify the member of the identified critical breach and the process and deadline for addressing it, including that this situation shall trigger membership suspension by the RJC, with a risk of further RJC disciplinary actions, should the critical breach(es) not be addressed as per 16.7.
 - b) ask the member for a written acknowledgement of this notification.
 - c) ask the member for a corrective action plan and evidence of addressing the critical breach.

19. CERTIFICATION DECISION

- 19.1. The certification body shall be responsible for, and shall retain authority for, its decisions relating to certification.
- 19.2. The initial three-year certification cycle begins with the certification decision. Subsequent cycles begin with the recertification decision, or certificate start date, whichever comes later (see 21.4).
- 19.3. The certification body shall assign at least one person to make the certification decision based on all the information related to the evaluation, its technical review and any other relevant information.
- 19.4. The technical review and the certification decision can be completed concurrently by the same person(s).
- 19.5. The certification body shall ensure that the person(s) making the certification decision are different from those who carried out the evaluation activities and that they have appropriate competence. The person(s) making the certification decision may be the same as the person(s) conducting the technical review.
- 19.6. The person(s) assigned by the certification body to make a certification decision shall be employed by or shall be under contract with either the certification body or an entity under the organisational control of the certification body. A certification body's organisational control shall be one of the following:
- a) Whole or majority ownership of another entity by the certification body.
 - b) Majority participation by the certification body on the board of directors of another entity.
 - c) A documented authority by the certification body over another entity in a network of legal entities (in which the certification body resides), linked by ownership or board of director control.
- 19.7. The persons employed by, or under contract with, entities under organisational control shall fulfil the same requirements of this document as persons employed by, or under contract with, the certification body.
- 19.8. The certification body shall record each certification decision including any additional information.
- 19.9. The certification body shall grant certification when all the following conditions are met:
- a) Any critical breaches or major nonconformities have been fully closed or regraded as a minor nonconformity within the allocated timelines.

Step 3 – Report review and certification decision

- b) Any critical breaches identified against the same critical sub-provision a second time onwards have been fully closed, unless there has been a significant change in the member's business, e.g. mergers/acquisitions.
- c) Any major nonconformities originating from escalated minor nonconformities have been fully closed.
- d) Any minor nonconformities have a verified correction and an auditor-approved corrective action plan in place.
- e) The member is an RJC member in good standing with regard to its general membership commitments (e.g. RJC membership fee payment is up to date, member is not subject to ongoing RJC disciplinary proceedings, etc.).
- f) Members operating in countries where compulsory schooling ends earlier than 15 years of age have no workers below the minimum working age of 15 years (see COP 2024 provision 19.1(b) (Child Labour)).
- g) The member has met contractual obligations with its certification body.

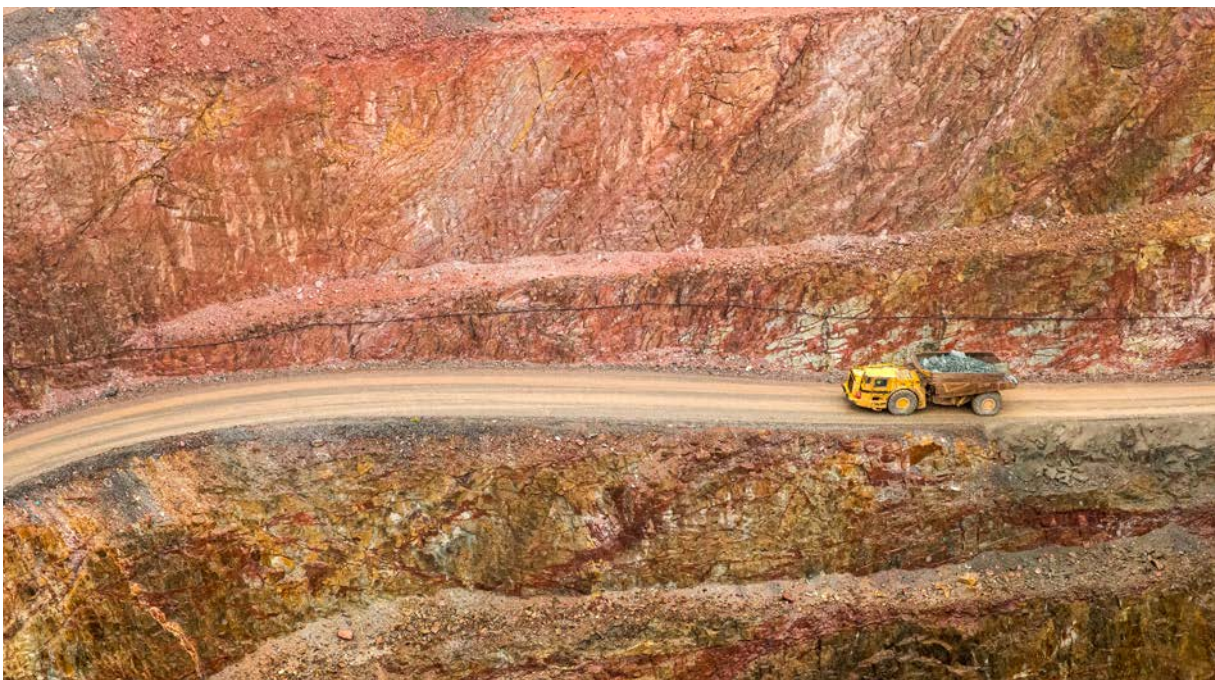
20. COMMUNICATION OF AUDIT REPORT AND CERTIFICATION DECISION

20.1. Once the certification decision has been made, the certification body shall:

- a) send the completed audit report and certification decision to the member for acknowledgement.
- b) ensure all required data have been uploaded to the RJC Auditor Portal, including the audit report, and auditor-approved corrective action plan, as applicable.
- c) require that the member complete and sign an acceptance declaration of the audit report as an accurate reflection of the RJC audit within five working days of receipt of the audit report. At this point, the member cannot challenge any audit findings – only any incorrect factual information in the audit report. Certification cannot proceed without a signed member declaration in this regard.
- d) specify to the member the timeframe and conditions for issuing the certificate, where applicable.
- e) reiterate the provisional date booked for and the type and format of the next mandatory audit, including whether it will be semi-announced.
- f) if certification is not granted or an existing certification is suspended, notify the member of the decision and identify the reasons, together with the process to appeal this decision, in line with the certification body's own procedures.
- g) if certification is not granted or an existing certification is suspended, record the same in the RJC Auditor Portal and identify the reasons.

Step 3 – Report review and certification decision

- 20.2. The certification body shall have a system to monitor certification and surveillance deadlines for members that it has certified before.
- 20.3. On receipt of the completed and signed member declaration, the certification body shall:
- upload the signed member declaration and share the completed audit report with the RJC via the Auditor Portal.
 - issue the certificate to the member within 10 working days after the member has provided the signed declaration, subject to the member being an RJC member in good standing with regard to its general membership commitments (e.g. RJC membership fee payment is up to date, the member is not subject to ongoing RJC disciplinary proceedings, etc.), the member meeting contractual obligations with its certification body, and force majeure. If the RJC member is not in good standing, the certification body shall not issue the certificate until the RJC has confirmed that the membership issue has been settled.
- 20.4. The certification body shall follow the timeframe below for sharing the audit report with the RJC:
- maximum **two months** from identification date if there are only minor nonconformities; or
 - maximum **four months** from identification date, with a tolerance of 10 working days, if there are critical breaches and/or major nonconformities.
- 20.5. The above timeframe may be extended if the auditor needs to verify the effectiveness of the corrective actions via an on-site follow-up audit, depending on auditor availability.



Step 4 – Certification



21. CERTIFICATION DOCUMENTATION

- 21.1. If certification can be granted to the member, the certification body shall provide the member with a certificate along with any associated documentation and clear information concerning any requirements for maintaining certification, including the recommended surveillance. The required deadline for surveillance and recertification shall be recorded in the certification body's systems to allow timely follow-up.
- 21.2. The member's certificate shall contain at a minimum:
- a) the name and address of the certification body.
 - b) the date certification is granted or renewed (start date).
 - c) the certification period and expiry date.
 - d) the three-month grace period.
 - e) the legal name and address (by city and country) of the member, including of all entities/facilities within the certification scope.
 - f) the scope of certification (processes for which certification is granted).
 - g) the applicable RJC standard version the certification is based on.
 - h) the RJC logo.

Step 4 – Certification

- i) the unique certification number for the member as a whole (for COP/LGMS) or for an individual entity (for COC), automatically generated by the Auditor Portal.

The COP, LGMS and COC certifications are completed against different standards, and so are given different certification numbers. A record of all the certification numbers for each member is also available on the [RJC website](#).

- j) the signature or other defined authorisation (name and title) of the person(s) of the certification body assigned and recorded as having such responsibility.

- 21.3. The member's certificate may contain any other information as required by the RJC, subject to periodic review, and depending on the relevant RJC standard, such as the membership, forum, audit date and type, materials in scope, eligible material declarations being issued, any claims, auditor's statement of conformity, etc. Note that any claim(s) shall be verified during the audit for conformity with the relevant COP provision but including it in the certificate is subject to the relevant RJC requirement at the time and at the member's discretion.
- 21.4. The start date of the new certificate shall be the date of the certification decision or the day following the current certificate expiry date, whichever comes later, noting that the start date of the new certificate cannot precede the certification decision date (be that granting, expanding or reducing the scope of certification, or renewing certification).
- 21.5. When a recertification audit is successfully completed prior to the expiry date of the existing certificate (with a tolerance of a maximum of 10 working days over the deadline), the expiry date of the new certificate shall be based on the expiry date of the existing certificate.
- 21.6. Whether or not the audits are conducted as combined, a COC certificate shall be dated so that the expiry date coincides with that of the COP certificate, even if the total length of the COC certificate is shorter than three years.
- 21.7. The COP and LGMS certificates' start and expiry dates shall always align, based on a combined audit, or point 5.6(c) shall be followed where the member started dealing in materials subject to one mandatory standard while already certified to the other mandatory standard.
- 21.8. All certificates shall have a grace period of three months that can be activated after expiry date, provided conditions are met (see Section 25, Certification Grace Period).
- 21.9. All the above information shall be recorded in the Auditor Portal and available to the RJC.
- 21.10. Based on the Auditor Portal, the RJC shall publish the member's certificate on the RJC website, on the member's profile page.
- Certified members are automatically provided with the RJC certificate and RJC logo via the Member Portal, which they can use in their communications and marketing materials, according to the relevant RJC rules.
- 21.11. In the event that the RJC identifies a certificate that has been incorrectly issued by the certification body, the RJC shall query the incorrect elements with the certification body (directly or via the oversight provider) and request appropriate corrective action, which may include an amendment or even suspension or withdrawal of the certificate. The certification body shall communicate the same to the member.

Step 5 – Surveillance



22. SURVEILLANCE AUDIT FORMAT AND SCOPE

- 22.1. Based on a system to monitor certification and surveillance deadlines for members that it has certified before, the certification body shall contact the member in good time to confirm the provisional audit dates already booked at the previous audit closing meeting.
- 22.2. The certification body shall ensure that any surveillance audits are conducted in a timely manner, with due consideration to member downtime periods.
- 22.3. The certification body shall require and obtain either a confirmation that there have been no changes since the last audit or an updated member self-assessment workbook capturing any changes since the last audit.
- 22.4. Surveillance audits may need to have a separate documentary review stage in situations where there have been significant changes to the member's processes and underpinning management system, or the context in which the member is operating (e.g. changes to legislation), as per 13.9.
- 22.5. The certification body shall plan and conduct the surveillance audit as per provisions 5–22, except requirements at 13.10-11 and 21.
- 22.6. The certification body shall consider the most effective way to undertake the surveillance, proportionate to the member's size and complexity. For example, a COP/LGMS surveillance audit can be combined with a COC surveillance audit.

Step 5 – Surveillance

- 22.7. A surveillance audit shall take place to provide assurance that the RJC member continues to conform to the relevant RJC standard throughout the certification period and:
- between 12 and 18 months from the certificate start date; and
 - regardless of whether there are any minor nonconformities with corrective actions to implement, noting that critical breaches and major nonconformities are subject to effective corrective actions before certification is granted.
 - for COP/LGMS, either fully remote or partially remote (where the member meets the relevant conditions and following the remote auditing protocol in Section 10, Decide on On-Site or Remote Audit Methodology) or on-site, depending on the criteria below:

TABLE 9. COP/LGMS SURVEILLANCE FORMAT

1. FULLY REMOTE SURVEILLANCE CAN BE RECOMMENDED IF ALL OF THE BELOW APPLY	2. PARTIALLY REMOTE/ON-SITE SURVEILLANCE IS REQUIRED IF ANY OF THE BELOW APPLY
<ul style="list-style-type: none"> • If there are any minor nonconformities resulting from the certification audit with corrective actions to implement, these can be verified through documentary objective evidence, and there is no need for: <ul style="list-style-type: none"> – employee interviews; or – on-site document sampling (i.e. wage or working-hour records); or – in-person reviews of health and safety or building changes; or – in-person reviews of confidential documents. • Any anticipated changes to the certification scope will not affect current conformity gradings. • For each 'RJC-recognised' provision during the certification period, there is: <ul style="list-style-type: none"> – a valid external RJC-recognised certification (see Appendix 4, RJC-Recognised Frameworks); and – strong internal controls that include a review of management systems and corrective actions for nonconformities. 	<ul style="list-style-type: none"> • All or some of the corrective actions for any minor nonconformities resulting from the certification audit need the audit activities below in order to be verified: <ul style="list-style-type: none"> – employee interviews; or – on-site document sampling (i.e. wage or working-hour records); or – in-person reviews of health and safety or building changes; or – in-person reviews of confidential documents. • The previous mandatory audit was fully remote (see Appendix 9, Remote Audit Protocol). • Known and anticipated changes to certification scope will arise before recertification. • An external RJC-recognised certification programme (see Appendix 4, RJC-Recognised Frameworks) will stop being supported before recertification. • The lead auditor presents a compelling reason for requesting an on-site surveillance audit.

Step 5 – Surveillance

- 22.8. The certification body shall consider the following, when setting the surveillance audit scope:
- Those entities/facilities and provisions that were not visited or were given less attention in the last audit, other than as permitted under Section 8, Multi-site Sampling.
 - The activities of the entities/facilities to be audited (as opposed to the declared member forum), when determining the COP/LGMS provisions in scope for the surveillance audit, as per Appendix 3, Criteria for Determining Provisions to be Assessed during COP/LGMS Surveillance Audits.
 - The nature of any nonconformities identified in the last audit.
 - Any corrective action plans, past or present.
 - Any changes in certification scope since the last audit.
 - Any business changes since the last audit, including organisational structure and resources.
 - Any complaints about the member submitted to the certification body or the RJC.
- 22.9. A surveillance audit shall be used to complete all of the following, as applicable:
- Assess and report on progress in implementing and/or maintaining corrective actions from the (re)certification audit, including verification of evidence for the implementation of any pending corrective actions for minor nonconformities, and nonconformities previously identified and closed to ensure they have not reoccurred, as applicable.
 - Verify and report on the current status of provisions that were classed as not applicable in the certification audit.
 - Verify the continuing validity of the certification for provisions covered by external RJC-recognised frameworks by reviewing, as a minimum, the latest full report.
 - Assess known and anticipated changes to the member's certification scope, or to any of its recognised external certifications, that may arise before recertification.
 - Assess the member's use of RJC certification claims and the RJC logo.
 - Include any relevant complaints that the member has received since the previous audit and/or that the certification body or the RJC has received about the member and that require review.
 - Review any changes in the member's procedures and processes since the last audit using a Simple Sampling Plan.
 - For COC, review eligible material declarations and subsequent transfer documents and control mechanisms for the same.
 - For COP/LGMS, assess entities/facilities that were not assessed in the certification audit or that have risks of nonconformities against critical provisions.
 - For COP/LGMS, assess continuing conformity against critical provisions or where there are known risks to conformity due to the entities'/facilities' activities or geographic presence, as per Appendix 3, Criteria for Determining Provisions to be Assessed during COP/LGMS Surveillance Audits, regardless of whether there are, and in addition to, any implemented corrective actions to assess, and depending on the activities related to the relevant entities/facilities (and not to the declared member forum).
- 22.10. If a complaint submitted to the RJC has been flagged for follow-up during a subsequent review, the RJC management team will contact the certification body in a timely manner to ensure the issue is included in the audit scope, based on visibility of booked audits recorded by the certification body in the Auditor Portal.

During the certification cycle



23. RECERTIFICATION

- 23.1. Based on the full certification cycle, the certification body shall consider the following, when setting the recertification audit scope:
- Those entities/facilities and provisions that were not visited or were given less attention in the last audit.
 - The nature of any nonconformities identified in the last audit.
 - Any corrective action plans, past or present.
 - Any changes in certification scope since the last audit.
 - Any business changes since the last audit, including to organisational structure and resources.
 - Any complaints about the member received by the certification body or the RJC.
- 23.2. If a complaint submitted to the RJC has been flagged for follow-up during a subsequent review, the RJC management team will contact the certification body in a timely manner to ensure the issue is included in the audit scope, based on visibility of booked audits recorded by the certification body in the Auditor Portal.
- 23.3. The certification body shall conduct a recertification audit to confirm the continued conformity with the requirements of the relevant RJC standard(s) and effectiveness of the member's processes and underpinning management system, and their continued relevance and applicability for the scope of certification.

During the certification cycle

- 23.4. The certification body shall plan and conduct the audit as per provisions 1–21.
- 23.5. Recertification audits may need to have a separate documentary review stage in situations where there have been significant changes to the member's processes and underpinning management system, or the context in which the member is operating (e.g. changes to legislation), as per 13.9.
- 23.6. The certification body shall conduct the audit a maximum of six months before the expiry date of the current certificate, with a tolerance of a maximum of 10 working days over the deadline and due consideration to member downtime periods, to enable timely renewal and certification continuity (see Section 25, Certification Grace Period).
- 23.7. In the case of an invalidated surveillance audit, the certification body shall complete a recertification audit within the next six months after invalidation, namely within 2.5 years from certificate start date, shortening the certification duration (see Section 17, Audit Invalidation).
- 23.8. The certification body shall make decisions on renewing certification based on the results of the recertification audit, as well as any complaints received regarding the member.

24. SEMI-ANNOUNCED AUDIT FORMAT

- 24.1. A **semi-announced audit** format should be recommended for any mandatory or special audits (except initial certification), if any of the following apply:
 - a) For COP/LGMS, major nonconformities or critical breaches were raised against the COP/LGMS provision 6 Human Rights and the provisions in the section titled Labour rights and working conditions (even if they were corrected before certificate issue) and there is a concern that the working conditions observed at the site may not be truly representative if the member is given notice of the audit.
 - b) The nature of the previous audit finding(s) would require further investigation for the full extent of the issue to be evaluated or for the effectiveness of the implementation of the corrective actions to be evaluated.
 - c) There is evidence of falsification or withholding of data by the member.
 - d) There is worker testimony indicating potential critical breaches that require further investigation in order for conformity to be verified.
 - e) There is any other compelling reason the lead auditor can present for needing to conduct an audit with less notice.
- 24.2. When conducting a semi-announced audit, the certification body shall follow the process below:
 - a) Semi-announced audits are conducted on-site (remote audits are not permitted in this case).
 - b) Semi-announced audits shall be conducted within an audit 'window' of one month, during which the auditor shall arrive unannounced on-site.
 - c) The certification body shall inform the member that the next mandatory audit will be semi-announced at the time that certification is issued, or certification continuity confirmed, as applicable, with a brief explanation for the reasons and an indication of which entities/facilities are to be audited in this way.

During the certification cycle

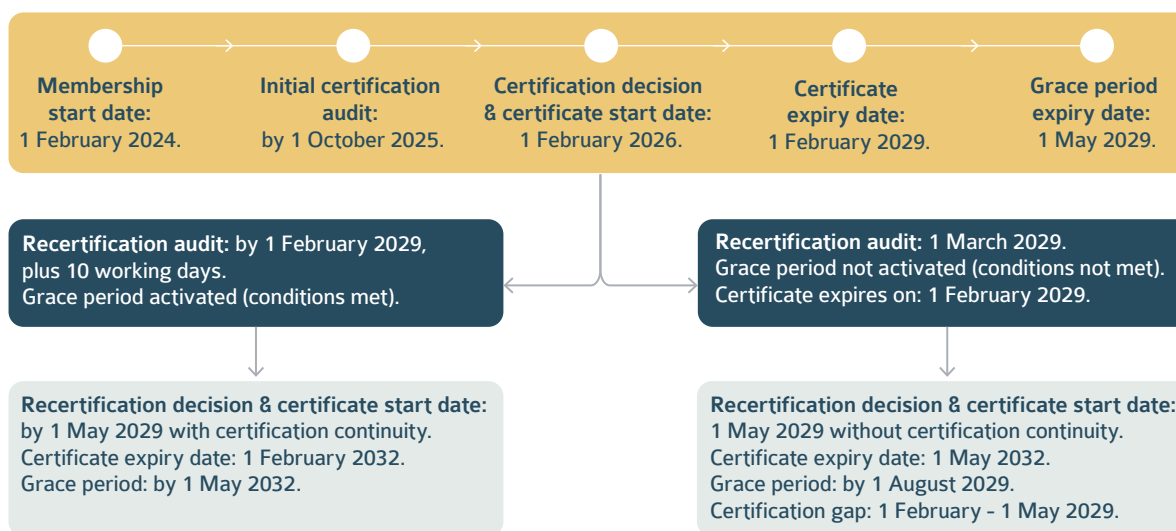
- d) The certification body shall provide notice to the member, one month before the start of the audit window.
- e) The certification body shall obtain member acknowledgement of this audit window and confirmation that the entity/facility has been advised of the audit and requested to accommodate it.
- f) On notification, the member may nominate up to three days during the audit window that would not be convenient for the audit. Sufficient time should be allowed before the start of the audit window to complete any security requirements to ensure that the auditor can gain access when required.

25. CERTIFICATION GRACE PERIOD

- 25.1. The three-month grace period after certificate expiry date may be automatically activated if:
 - a) the recertification audit takes place before the certificate expiry date, plus a tolerance of a maximum of 10 working days over this deadline; or
 - b) the member started engagement to book the audit at least six months prior to the certificate expiry date, but no certification body was able to accommodate an audit within the timeframe due to lack of auditor availability; or
 - c) the member is scheduled to undergo a combined audit that involves a non-RJC standard, during the grace period of three months; or
 - d) the auditor could not conduct a timely scheduled audit due to illness or force majeure.
- 25.2. The purpose of the grace period is to accommodate the post-audit actions without impacting the member's certification continuity, should a decision to recertify be made.
- 25.3. If the recertification audit does not take place as per 25.1(a), the member shall not benefit from the grace period and shall lose certification continuity and have a gap in certification, with the next certification cycle based on when the recertification decision is finally made.
- 25.4. Equally, if corrective actions for any critical breach and/or major nonconformity are not implemented and verified prior to the expiry of the certificate's grace period (provided the recertification audit was completed within the timeframe), then the member shall lose certification continuity and have a gap in certification, with the next certification cycle based on when the recertification decision is finally made.
- 25.5. The certification body shall not grant extensions to certification.

During the certification cycle

FIGURE 8. CERTIFICATE AND GRACE PERIOD EXAMPLE



26. TRANSFER OF CERTIFICATION

- 26.1. The certification body should contract a full three-year certification cycle with the member, including surveillance audit, at certification stage, unless an alternative shorter contract period is requested by the member.
- 26.2. If the member wishes to change certification body at any point during the three-year certification cycle, the incoming certification body shall:
- verify that there is no disagreement over certification audit findings or surveillance format between the member and the outgoing certification body.
 - verify the reasons, e.g. plausible commercial reasons or auditor scope.
 - ensure that risks posed by auditor familiarity or a lack of impartiality are managed as per documented internal procedure.
 - notify the RJC of the intention and reasons to take over a member's existing certification during the three-year cycle. The RJC may confirm the same with the outgoing certification body.
 - satisfactorily respond to any related RJC queries.
 - obtain the previous audit report, any corrective action plans and verification of implementation of the same, as applicable.
 - conduct a full recertification audit at the same time, unless the audit required is a surveillance audit and the outgoing certification body can no longer cover the member's activity for a – for example, it no longer has appropriate personnel.
 - record the transfer reason in the audit report.
 - issue a new certificate to the member, following a certification decision in this regard.

During the certification cycle

- 26.3. If applicable, the outgoing certification body shall notify the member that it can no longer conduct its surveillance audit as soon as this becomes apparent.
- 26.4. The outgoing certification body shall withdraw the existing certificate, following the above transfer of certification.

27. CHANGES AFFECTING CERTIFICATION

- 27.1. Changes affecting RJC certification (and membership) shall be accepted when:
- the RJC introduces new or revised scheme requirements that affect the existing members; or
 - changes occur within the member's business (hereinafter referred to as changes initiated by the member), such as:
 - an organisational restructure, including change to the member's legal name.
 - divestments, acquisitions or changes to the equity share.
 - new or altered activities, products and processes, including provenance claims.
 - new locations or different distribution of entities/facilities; or
 - there are changes in the statutory environment, regulations or other stakeholder expectations and commitments (external influences); or
 - new information related to the fulfilment of certification requirements is obtained by the auditor after certification has been established, including member loss of external RJC-recognised certification based on harmonisation with other schemes.
- 27.2. The certification body shall verify whether any changes have occurred since the last audit, including changes initiated by the member or the member's loss of external RJC-recognised certification, by requiring and obtaining an updated member self-assessment workbook ahead of any mandatory audit, as well as consulting the RJC Auditor Portal for the latest membership scope and the member's website.
- 27.3. If a COC-certified member or entity wishes to add new facilities, outsourcing contractors or types of materials to its certification scope – or if it decides it now wants to issue eligible material declarations – the certification body shall conduct a new certification audit for those elements.
- 27.4. If these changes are addressed through a surveillance audit, the dates of the original certification period shall continue to apply.
- 27.5. A member's seeking of COC certification for a separate entity under its control (depending on the structure of its business), for which a separate certification period and documentation would apply, is not considered a change affecting certification.
- 27.6. The certification body shall ensure any RJC-introduced changes are communicated to all its certified members.
- 27.7. The certification body shall verify the implementation of the RJC changes by its certified members and take any actions according to RJC transition requirements.

During the certification cycle

- 27.8. The certification body shall consider other changes affecting certification as per 27.1(b)–(d) and shall decide on the appropriate action(s):
- Assess the impact of the change(s) on the member’s certification status at the subsequent audit, whatever type it may be (including by adding the equivalent RJC standard(s) provisions in the audit scope if previously harmonised).
 - Determine whether the subsequent mandatory audit needs to be brought forward or a special audit needs to take place (see 4.4, Table 1, RJC audit types) and whether it needs to include a separate documentary stage as per 13.9.
 - Conduct additional technical review of the audit report.
 - Review the certification decision.
 - Issue a revised certificate to extend or reduce the scope of certification.
 - Issue certification documentation of revised surveillance activities.
- 27.9. The certification body shall document the rationale for excluding any of the above actions (e.g. when a certification requirement that is not a process requirement changes, and no evaluation – documentary review, interview, sampling, audit, technical review or certification decision activities – is necessary).

28. REDUCTION, SUSPENSION, WITHDRAWAL OR TERMINATION OF CERTIFICATION

- 28.1. The certification body may reduce, suspend, withdraw or terminate a member’s existing valid certificate for reasons including but not limited to those listed below, and shall take the associated actions.

TABLE 10. EXTENSION (TO SCOPE), REDUCTION, SUSPENSION, WITHDRAWAL OR TERMINATION OF CERTIFICATION

ACTION (WHAT)	REASONS (WHEN)	DETAILS (HOW)
a) Extension/reduction of certificate scope or reduction of certificate duration	<ul style="list-style-type: none"> There is a new entity/facility owned/controlled by the member, and which actively contributes to the precious metal, diamond and coloured gemstone (in RJC scope) jewellery and watch supply chain. An entity/facility no longer meets the criteria to be included in the certified member’s RJC certification (and membership) scope. An early recertification audit was completed (with more than six months before the recertification deadline), either by the member’s choice or following an invalidated surveillance audit, shortening the certification duration. 	<ul style="list-style-type: none"> The certification body may conduct a special audit (extension/reduction to scope), if applicable, or shall conduct a recertification audit, according to the relevant requirements in this document. The certification body shall issue an updated/new certificate (and the RJC shall update the RJC website accordingly), in order to ensure that the extended/reduced scope of certification is clearly communicated to the member (as per 21.10) and clearly specified in certification and public information.

During the certification cycle

ACTION (WHAT)	REASONS (WHEN)	DETAILS (HOW)
<p>b) Suspension of certificate (certification is temporarily invalid)</p>	<ul style="list-style-type: none"> The certified member has not met contractual obligations with its certification body. The certified member does not undergo a surveillance audit within six months of the surveillance deadline, or the surveillance audit is invalidated (see Section 17, Audit Invalidation). The certified member has voluntarily requested a suspension. Following a surveillance audit or any type of special audit, for a certified member, when: <ul style="list-style-type: none"> a critical breach is identified; or a major nonconformity is identified, including misuse of the RJC logo and/or certificate; or a complete corrective action plan has not been received within three months of identification of findings; or workers below the minimum working age of 15 years are identified at members operating in countries where compulsory schooling ends earlier than 15 years of age (see COP 2024 provision 19.1(b) (Child Labour)). The RJC suspends membership for any reason, including commencing of disciplinary proceedings against a certified member and non-payment of fees (the RJC shall notify the certification body and the member accordingly). 	<p>The certification body shall assign one or more persons who are competent (in their knowledge and understanding of all aspects of the handling of suspended certifications) to formulate and communicate the following to the member:</p> <ul style="list-style-type: none"> Notification of and reason for suspension of certification. Where critical breaches and major nonconformities are identified during the audit of a certified member, the auditor's conclusions shall be technically reviewed and confirmed before the certificate is suspended, Certificate shall be suspended within five working days from identification. Actions needed to end suspension and restore certification in accordance with this document and any other relevant RJC procedures. The interdiction regarding use of the RJC logo, during suspension. Any other actions required by the RJC. <p>The certification body shall:</p> <ul style="list-style-type: none"> suspend the certification, including the COC certification if the COP certification has been suspended; and update the Auditor Portal, which will automatically update the Member Portal and remove the suspended certificate and associated RJC logo and notify the RJC to remove the suspended certificate from its website, to ensure that there is no indication that the member continues to be certified.
<p>c) Reinstatement of certificate</p>	<ul style="list-style-type: none"> The member has completed all the necessary actions to resolve the issue that has resulted in the suspension of the certificate as per 28.1(b). The certification body has verified the member's actions, according to this document. 	<p>The certification body shall:</p> <ul style="list-style-type: none"> restore the suspended certification, including the COC certification that was suspended strictly as a result of the COP certification being suspended; and notify the member and the RJC to reinstate the certificate on its website and update the Auditor Portal, which will automatically update the Member Portal and reinstate the certificate and associated RJC logo, to ensure that all appropriate indications exist that the member continues to be certified.

During the certification cycle

ACTION (WHAT)	REASONS (WHEN)	DETAILS (HOW)
d) Withdrawal of certificate	<ul style="list-style-type: none"> If member certification is transferred to another certification body during the certification cycle. If the member fails to resolve the issues that have resulted in the certification suspension in the timeframes defined in this document. 	<ul style="list-style-type: none"> Both the new and the current certification bodies shall follow the process under Section 26, Transfer of Certification. <p>The certification body shall:</p> <ul style="list-style-type: none"> notify the member of the expiry of the deadline allocated to resolve the issues that have resulted in the certification suspension and of the resulting certification withdrawal. notify the RJC to remove the withdrawn certificate from its website (if not previously suspended) and update the Auditor Portal, which will automatically update the Member Portal and remove the withdrawn certificate and associated RJC logo, if not previously suspended.
e) Termination of certificate	<ul style="list-style-type: none"> The member cancels its membership of the RJC, or its membership is terminated by the RJC for any reason. 	<p>The certification body shall:</p> <ul style="list-style-type: none"> notify the member accordingly, including the requirement to discontinue any use of the RJC logo and certificate going forward. notify the RJC to remove the terminated certificate from its website and update the Auditor Portal, which will automatically update the Member Portal and remove the terminated certificate and associated RJC logo, to ensure that there is no indication that the member continues to be certified.

28.2. Any reduction, suspension or withdrawal of certification or lack of a valid audit shall also impact the RJC membership.

See the [RJC Member Certification Handbook](#), 5.3, Reduction, Suspension, Withdrawal or termination of Certificate and Impact on RJC Membership and 5.4, Disciplinary Proceedings for information on the actions taken by the RJC together with the actions taken by the certification body as per 28.1, Table 10 above, or separately, as applicable.

29. RECORDS

- 29.1. The certification body shall retain records to demonstrate that all certification requirements in this document have been effectively fulfilled.
- 29.2. The certification body shall keep records confidential and shall use the RJC Auditor Portal (user-protected access) as a means to transmit them to the RJC.
- 29.3. Records shall be retained at least for the current and the previous two certification cycles.

During the certification cycle

30. COMPLAINTS AND APPEALS

- 30.1. The certification body shall have a documented and publicly available process to receive, evaluate and make decisions on complaints and appeals. For complaints, this process shall be subject to requirements for confidentiality, as it relates to the complainant and to the subject of the complaint.
- 30.2. The complaints/appeals-handling process shall include at least the following elements and methods:
- a) An outline of the process for receiving, validating and investigating the complaint or appeal, and for deciding what actions need to be taken in response to it.
 - b) Tracking and recording complaints or appeals, including actions undertaken in response to them.
 - c) Ensuring that any appropriate corrections and corrective actions are taken.
 - d) Informing the complainant/appellant about the outcome, unless the complaint was made anonymously.
- 30.3. The certification body shall:
- a) be responsible for all decisions at all levels of the appeals/complaints-handling process.
 - b) on receipt of a complaint or appeal, confirm whether the complaint or appeal relates to certification activities for which it is responsible and, if so, address it.
 - c) acknowledge receipt of a formal complaint or appeal.
 - d) inform the RJC of the complaint.
 - e) inform the certified member against whom the complaint was submitted, at an appropriate time, except in cases where it may not be safe for the complainant (e.g. whistleblowing).
 - f) ensure that the decision resolving the complaint or appeal shall be made by, or reviewed and approved by, person(s) not involved in the certification activities related to the complaint or appeal.
 - g) not use personnel (including those acting in a managerial capacity, who have provided consultancy for a member or who have been employed by a member) to review or approve the resolution of a complaint or appeal for that member within two years following the end of the consultancy or employment, to ensure that there is no conflict of interest.
 - h) ensure that the complaints process is undertaken by personnel trained in its use.
 - i) ensure that submission, investigation and decisions for complaints and appeals shall not result in any discriminatory actions against the complainant/appellant.
 - j) inform the complainant/appellant that any outcome/decision does not substitute the person's right to raise complaints or appeals through any other legal channels.
 - k) be responsible for gathering and verifying all necessary information (as far as possible) to progress the complaint or appeal to a decision.
 - l) take any subsequent action needed to resolve the complaint or appeal.
 - m) provide the complainant or appellant with updates, whenever possible, and a formal notice of the outcome at the end of the complaint or appeal, unless the complaint was made anonymously.
 - n) refer any complaint/appeal that could not be resolved through the certification body's process to the RJC as an escalation point.

During the certification cycle

TABLE 11. USEFUL TIMEFRAMES

TIMEFRAME	ACTIONS
at least 1 month	<ul style="list-style-type: none"> before the audit, the member shall submit its completed/updated self-assessment workbook to the certification body (12.1).
at least 10 working days	<ul style="list-style-type: none"> before the audit, the certification body shall communicate and agree on the audit plan with the RJC member (12.2).
at least 5 working days	<ul style="list-style-type: none"> before the audit, the certification body shall record the remote audit in the RJC Auditor Portal, including the completed eligibility analysis questionnaire(s) (10.1(c)).
5 working days	<ul style="list-style-type: none"> for the certification body to: <ul style="list-style-type: none"> respond to a member once contact is initiated (1.1) communicate any identified differences between the RJC membership scope and certification scope to the RJC and the member (3.5(d)). notify the RJC regarding a critical breach or major nonconformity and suspend an existing certificate (16.3(a)–(c) and 28.1, Table 10(b)). communicate any sensitive issues identified during an audit to the RJC, where legally allowed, via the Auditor Portal (14.27(e)). respond to any RJC queries on audit report quality (see Governance and Support, Section A, RJC Ongoing Quality Checks). for the member to: <ul style="list-style-type: none"> sign the acceptance declaration on receipt of its audit report (20.1(c)). respond to the certification body to confirm the provisional audit date(s) already booked at the previous audit closing meeting (see RJC Member Certification Handbook, 4.5).
10 working days	<ul style="list-style-type: none"> for the certification body to issue the certificate on receipt of the signed member declaration and subject to conditions (20.3(b)). of tolerance: <ul style="list-style-type: none"> for the certification body to share the audit report with the RJC if critical breaches and/or major nonconformities have been identified, beyond deadline (20.4(b)). for audit deadline (21.5, 23.6, 25.1).
15 working days	<ul style="list-style-type: none"> for the certification body to: <ul style="list-style-type: none"> decline a member's application for certification and inform the member of the same, from receipt of the application, if applicable (2.4). verify a member's corrective action plan and round of evidence (where applicable) and inform the member of the result, from receipt of the same (16.11).
1 month	<ul style="list-style-type: none"> for the member to submit a corrective action plan to the auditor, including evidence of correction(s) (16.7, 16.8). for a semi-announced audit window (24.2(b)). before the audit, the certification body shall notify the member of the impending semi-announced audit (24.2(e)).

During the certification cycle

TIMEFRAME	ACTIONS
2 to 4 months	<ul style="list-style-type: none"> for the post-audit process (20.4).
3 months	<ul style="list-style-type: none"> for the member to submit evidence of corrective action implementation for critical breaches and major nonconformities. (16.7, 16.8). for the certificate grace period (21.8). for the member to submit a complete corrective action plan following a surveillance or any type of special audit (28.1, Table 10 (b)).
6 months	<ul style="list-style-type: none"> of validity of a completed/updated self-assessment workbook (1.3(p), 12.1). to complete an audit, from start to finish (8.5, 13.1, 23.6). for an effective and auditor-approved corrective action plan to be in place before audit invalidation (17). to obtain an overdue initial certificate or to undergo any overdue surveillance and recertification audits before suspension of membership (17.2, 23.7, 28.1, Table 10 (b)). for a rejoiner member to undergo audit, after the two-year stand-down period (2.8.2).
up to 12 months	<ul style="list-style-type: none"> after a corresponding audit, external RJC-recognised certificates may be accepted (6.3) for a rejoiner member to achieve certification after the two-year stand-down period (2.8.2). after an RJC audit demonstrating full conformity of shared outsourced contractors, for the associated report to be used as evidence of conformity and as a substitute for an additional on-site audit (9.6). of records to be reviewed during the initial certification audit (14.8(a)(1)).
12–18 months	<ul style="list-style-type: none"> for surveillance audits to take place (4.3, 22.7).
18 months	<ul style="list-style-type: none"> for the initial certification audit to take place (4.4, Table 1(a)).
2 years	<ul style="list-style-type: none"> for the member to achieve initial certification (4.4, Table 1(a)). as a stand-down period for rejoining companies (2.7, 2.8.1, 2.8.2). during which the certification body shall not use personnel to review or approve the resolution of a complaint or appeal for a member for which they have provided consultancy or from which they have taken employment (30.3(g)).
2.5 years	<ul style="list-style-type: none"> from certificate start date for a recertification audit to be completed, in the case of an invalidated surveillance audit (23.7).
up to 3 years	<ul style="list-style-type: none"> for the duration of an RJC certification cycle. of records to be reviewed at a recertification audit, if not reviewed at the surveillance audit (14.8(a)(3)). of records for any materials, components or products purchased and handled during this time, to be reviewed during the initial COC certification audit, if the member wishes to include them in the audit scope (14.9).

Governance and support



Learn how the RJC governs and supports implementation of the RJC standards and the certification process.

A. RJC ONGOING QUALITY CHECKS

The RJC uses multiple approaches to ensure the quality and integrity of the RJC certification process, as part of continuous performance monitoring, such as:

- providing standard processes and terminology for members and auditors to use.
- requiring all members and auditors to identify any potential conflicts of interest.
- publishing practical guidance on implementing RJC standards and certification.
- offering training and advice for members and auditors.
- conducting additional quality reviews on members' audit reports, on a sampling basis, at any given time, to ensure that audits have been conducted and certificates issued in line with the requirements of this document. As part of this process, the RJC may raise queries with the certification body. The certification body shall respond to any queries raised by the RJC within five working days or advise the RJC of any external circumstances outside its control preventing it from responding within this timeframe. A new timeframe shall be agreed between the RJC and the certification body in this case.
- shadowing member RJC audits.

Governance and support

- conducting regular calibration exercises and undertaking independent peer reviews.
- reviewing the outputs of the certification bodies' ongoing oversight.
- reviewing of certification bodies' general performance indicators, e.g. timeliness of auditing, report and issue of certificates, responsiveness to RJC queries, conformity with the RJC licencing contract, implementation of any corrective action plans requested and the outcome of any complaints from the RJC, members or other third parties, etc.

Depending on the findings of these ongoing quality checks, including actions or omissions that may affect the integrity of the RJC standards, the RJC may:

- ask auditors to undertake refresher training; or
- raise any concerns with and request an investigation from the oversight body; or
- submit a complaint to the certification body; or
- implement other controls to maintain the credibility of the RJC system; or
- remove a certification body or an auditor from the list of RJC approved certification bodies and auditors.

To support both members and certification bodies, the RJC may send all members automated advance reminders of deadlines for their certification, surveillance and recertification audits.

B. THE RJC COMPLAINTS MECHANISM

The RJC aims to ensure the fair, timely and objective resolution of complaints relating to potential nonconformity with the RJC standards or RJC policies and procedures, including, where such complaints could not be resolved at certification-body level and were escalated to the RJC, the certification and assurance system.

By taking part in RJC activities, all RJC members and RJC certification bodies and auditors agree to submit to the RJC Complaints Mechanism wherever complaints arise, and to be bound by the decisions of the RJC. This does not replace or limit access to judicial remedies.

The RJC Complaints Mechanism defines how we will respond to such complaints and is available in full at [RJC complaints](#).

The RJC also requires the RJC certification bodies to have their own complaints mechanisms and dispute resolution procedures, in line with the requirements in this document and other relevant RJC documentation.

Governance and support

C. DISCIPLINARY PROCEEDINGS

Disciplinary proceedings are a collection of administrative processes used to consider whether, and what type of, disciplinary action should be taken against:

- RJC members for known misconduct or breaches in rules, regulations, policies or standards (see the RJC's Articles of Association, 3.13, available at [RJC governance](#), and the Member Certification Handbook, 5.4 Disciplinary Proceedings, for full procedural details); and/or
- RJC certification bodies and individual auditors for failure to comply with the RJC approval criteria for the RJC scheme, including the RJC licencing contract, as applicable. (see RJC Approval Criteria for Certification Bodies and Auditors).

Disciplinary action refers to the action that is taken during or following disciplinary proceedings. Examples of disciplinary actions include written warnings, suspension or expulsion from the RJC, with removal from the RJC website, as applicable.

In some cases, the outcome of disciplinary proceedings may be a rejection of the audit report and a request for the member's entities/facilities to be re-audited at the certification body's cost.

Disciplinary proceedings may be triggered by complaints; incidents; known misconduct or breaches of rules, regulations, policies or standards; judgements of a court of law, or any other legal or administrative regulatory body; any other evidence of members and certification bodies bringing the RJC into serious disrepute; or other indicators of poor performance or failure to comply with RJC requirements.

D. DATA CONFIDENTIALITY AND LEGAL ADVICE

The RJC is committed to protecting the confidentiality of our members' commercially sensitive information (see [RJC policies](#) and [Privacy Notice](#)).

To that end, the RJC management team:

- only accesses a member's information to process a membership application or as part of the RJC recognition programme of other certifications; reviews an audit report to ensure that audits have been conducted and certificates issued in line with the requirements of this document; carries out an investigation as required under the RJC Complaints Mechanism; or assesses the effectiveness and impact of our work within the jewellery and watch supply chain; and
- keeps commercially sensitive information secure and strictly confidential, never sharing it with any third party (except for the information that is published on the RJC website, or if otherwise agreed with the individual members under the RJC recognition programme).

Note that members that are COC-certified can choose not to withhold the identity of outsourcing contractors audited as part of their certification scope from the information published on the RJC website.

Certification bodies are required to have equivalent policies and procedures as part of their management systems, and these are audited as part of the oversight process.

Governance and support

Other than as required by legislation or accreditation requirements, the RJC keeps the details of complaints (and all proceedings of the RJC Complaints Mechanism) and disciplinary proceedings, including critical breaches, confidential. We reserve the right to publicly report anonymously and in aggregate on the complaints received, disciplinary proceedings initiated and how they were resolved, and any identified critical breaches.

We base all our decisions on objective evidence. In some cases, we may seek independent legal advice or involve independent auditors to help in our investigation and decision-making.

E. TRAINING AND KNOWLEDGE EXCHANGE

The RJC provides a range of online information resources and training to all its members and auditors. This includes guidelines, toolkits, templates, best practice case studies, auditor calibration exercises, FAQs and webinars (see [RJC website](#)).

We also organise regular information sessions/webinars and workshops. And, working in partnership with others, we create opportunities for knowledge exchange through, for example, workshops, seminars, briefings, inter-member support and more.

For specific queries on standards implementation, please contact training@responsiblejewellery.com.



References

- Better Gold Initiative, Remote Audits and Assessments. Experiences from the forestry and mining sectors, p. 24, https://www.projekt-consult.de/newsletter/downloads/641266/BGI_Report_-_Remote_Assessments.pdf.
- International Accreditation Forum (IAF), IAF Determination of Audit Time of Quality, Environmental and Occupational Health & Safety Management Systems (IAF MD 5:2023), https://iaf.nu/iaf_system/uploads/documents/IAF_MD5_Issue_4_Version_3_14062023.pdf.
- International Accreditation Forum (IAF), IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization (IAF MD 1:2023), https://iaf.nu/iaf_system/uploads/documents/IAF_MD1_Issue_3_181020231.pdf.
- International Organization for Standardization (ISO), ISO 2859-1:1999, Sampling Procedures for Inspection by Attributes, Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection, <https://www.iso.org/standard/1141.html>.
- International Organization for Standardization (ISO), ISO/IEC 17000:2020 Conformity Assessment – Vocabulary and General Principles, <https://www.iso.org/standard/73029.html>.
- International Organization for Standardization (ISO), ISO/IEC 17021-1:2015 Conformity Assessment – Requirements for Bodies Providing Audit and Certification of Management Systems – Part 1: Requirements, <http://www.iso.org/standard/61651.html>.
- International Organization for Standardization (ISO), ISO/IEC 17065:2012 Conformity Assessment – Requirements for Bodies Certifying Products, Processes and Services, <https://www.iso.org/standard/46568.html>.
- International Organization for Standardization (ISO), ISO 19011:2018 Guidelines for Auditing Management Systems, <https://www.iso.org/standard/70017.html>.
- ISEAL Alliance, ISEAL Code of Good Practice for Sustainability Systems, <https://www.isealalliance.org/defining-credible-practice/iseal-code-good-practice>.
- ISEAL Alliance, ISEAL Guidance – Remote Auditing Good Practices, p. 5, <https://www.isealalliance.org/sites/default/files/resource/2021-03/Remote%20Auditing%20Good%20Practices%20ISEAL%20Guidance%20v0.1%20March%202021.pdf>.



RESPONSIBLE
JEWELLERY
COUNCIL

**THE COUNCIL FOR RESPONSIBLE JEWELLERY
PRACTICES LTD.**

Office 3, 3rd Floor Hind House
2-3 Hind Court
London
EC4A 3DL

The Responsible Jewellery Council is the trading name of the Council for Responsible Jewellery Practices Ltd.

Registered in England and Wales with company number 05449042.

Version 1.0 February 2025
Please see the RJC website to ensure this is the latest version.