ASSESSMENT MANUAL - QUICK GUIDE

RESPONSIBLE JEWELLERY COUNCIL

Introduction

This document offers an overview of the expectations and certification process that the Responsible Jewellery Council (RJC) has set out to our members and our RJC accredited auditors. Indeed, members who wish to be certified against the RJC standards - Code of Practices (CoP) and/ or Chain-of-Custody (CoC) must utilise an RJC-accredited audit firm to verify their conformance against the standards' requirements.

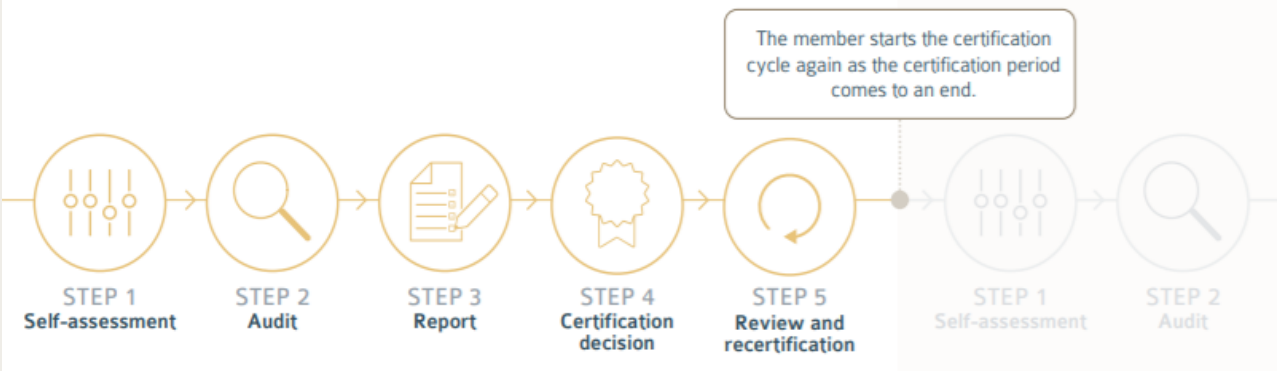
Please CLICK HERE for the full Assessment Manual (latest version), further detailing RJC guidelines for both members and RJC accredited auditors. You will find more useful links at the end of this document.

Overview

All RJC members are expected to:

- ✓ Operate their business in a way that meets the RJC standards (CoP & CoC)
- ✓ Dedicate resources to ensure ongoing conformance with the RJC standards' requirements over time.
- ✓ Communicate and train personnel about the RJC standards and how to meet their requirements in a timely manner before their first certification audit and as per required frequency thereafter.
- ✓ Contact an RJC accredited audit firm and engage them to carry out their certification audits once they have completed their self-assessment workbook. In doing so, the members must ensure that relevant certification deadlines are met: 2 years from joining the RJC for non-certified members, 12 to 24 months from the certificate issue date for mid-term reviews and surveillance audits and/or current certificate expiry date for certified members.
- ✓ During the audit, give auditors open and unhindered access to facilities, personnel and any information and records they require to assess conformance with RJC standards.
- ✓ Implement corrective actions or improvement plans, as appropriate, after the audit has ended.
- ✓ Promote responsible business practices within their supply chain, in line with the RJC standards.

The Certification Cycle in 5 Steps



Step 1: Self-assessment

The member examines their own practices and completes their self-assessment workbook, ideally 6 to 12 months before the audit. This enables the member to identify any areas of company policy or procedure requiring improvement or amendment, gather all the necessary documents to evidence compliance, and generally prepare for the audit. Members are strongly advised to complete the self-assessment workbook diligently and thoroughly.

The completed self-assessment workbook must be made available to the auditor well in advance of the audit.

Note: A member must not book an audit before they have completed their self-assessment workbook.

ASSESSMENT MANUAL - QUICK GUIDE

RESPONSIBLE JEWELLERY COUNCIL

- Other (non-RJC) standards and initiatives may be **recognised** by the RJC as equivalent to one or more CoP or CoC Standard provisions. In these cases, members and auditors can use external certifications to evidence RJC conformance without additional self-assessment or review, under certain conditions (see p. 22-25).
- The auditor will review the member's certificate scope (and document it in the audit report) and define which & how many sites will be audited (audit scope), based on the total number of sites in the certificate scope.

Step 2: Audit

The member selects an RJC accredited audit firm (list can be found **HERE**) and schedules the audit. The member provides their self-assessment workbook to the auditor. During the audit, the auditor reviews evidence to assess conformance.

- **CoP audit types** are: Initial certification (within 2 years of joining the RJC), Mid-term review (12-24 months after certification) and Recertification (at the end of the certification period). In addition, members can:
  - transition from a 1-year to a 3-years certificate, by completing a Transition audit within 6 months from initial audit.
  - add Provenance Claims to their certificate outside their normal auditing cycle by completing a Bolt-on audit.
- **CoC audit types** are: Initial certification (at the same time as, or after, a CoP audit, but not before), Surveillance (12-24 months after certification) and Recertification (at the end of the certification period).

Step 3: Report

The auditor reports findings. These can be minor or major non-conformances, critical breaches (see below) and business suggestions for improvements.

- Member has **one week** from the audit closing meeting (final meeting marking the end of the audit, where the auditor communicates findings to the member) to try and close non-conformances by submitting a corrective action plan **with evidence of implementation** to auditor, as applicable. Any non-conformances closed this way do not count.
- Should the one-week opportunity to close any non-conformances not be used, the member has **one month** to develop a corrective action plan and submit it to the auditor for review, as applicable. Once reviewed and approved, the auditor finalises the audit report and sends it to the member for approval. The non-conformances are maintained.
- The approved audit report is sent to the RJC within **two months** of the audit being completed.

Post-audit process:

- The effective implementation and closure of corrective actions will be reviewed by the auditor during the next scheduled audit (mid-term review, surveillance, transition or recertification audit).
- **Should corrective actions not be implemented before the next recertification audit, any remaining minor non-conformance will be escalated to a major non-conformance.**
- A **critical breach** is any major non-conformance identified against **CoP critical provisions** (6.1, 7.1, 16.1, 16.2, 17.1, 17.4, 18.1, 19.1, 19.2, 20.1, 22.1, 25.2, 26.2c, 28.1, 29.1, 33.1, 38.1, 38.2, 38.4, 39.2a, as per p. 34, Table 6) or **any CoC provision** where a deliberate falsification of information, systemic failure of management systems, or a total lack of controls of business risks has taken place.
- The auditor must notify both the member and the RJC within **three working days** of identifying the critical breach and provide full details. The audit must be completed upon finding a critical breach.
- The RJC may **temporarily suspend** the member from the RJC website while the critical breach is under review.
- The auditor will ask the member to submit a corrective action plan with evidence of implementation in relation to the critical breach, within a maximum of **four weeks from the day the critical breach was formally notified to the member.**
- The auditor will review the member's response within **two weeks** of receipt. At this stage, the RJC or the auditor may ask the member to provide further information.
- At the auditor's recommendation, the RJC will decide the next step (such as downgrading or closure of the critical breach, onsite verification audit, disciplinary action etc).
- If the critical breach has been either downgraded to a minor non-conformance or closed, the audit report is finalised, and the process resumes.

ASSESSMENT MANUAL - QUICK GUIDE

RESPONSIBLE JEWELLERY COUNCIL

Step 4: Certification decision

The RJC reviews the audit report and certifies the member (or not), based on the auditor's recommendation. The member promotes their RJC certification.

- Auditor decides whether a **CoP mid-term review** is needed during the certification audit, depending on several criteria (p. 62 Table 14). For example, **four or five** minor non-conformances will trigger a desktop mid-term review, whereas **six or more** minor non-conformances will trigger an onsite mid-term review.
- Depending on the results of each type of audit, a certificate is granted, extended, suspended, or denied.
- CoP and CoC certificates can have **three years**, if only minor non-conformances are identified.

Step 5: Review and recertification

The auditor carries out mid-term or other reviews as and when required, according to the member's latest audit outcome and certificate.

- The member starts the certification cycle again as the certification period comes to an end.
- Re-certification audits must be completed **before the certificate expiry date**, otherwise the member will have **a gap in certification**. Any such gap in CoP certification **invalidates the CoC certification**.
- CoP mid-term reviews and CoC surveillance audits must be completed **within 24 months** after certification.
- If any of the required audits are not completed within the above deadlines, the RJC will suspend the member's profile page until the relevant audit is at least booked and dates are communicated to the RJC.
- Members are required to maintain certification against the CoP to maintain their RJC membership.

One-year certificates (CoP only)

- If an auditor finds **any major non-conformances** during a CoP audit, the member may only be granted a CoP certificate for **one year**. If a major non-conformance is found during a mid-term review, the CoP certification period of three years will be reduced to one year.
- All members given a one-year CoP certificate are expected to use their best efforts to transition to three-year certification status as quickly as practical. Any **transition audit** taking place within **six months** of the previous one may be more like a mid-term review than a certification audit, with the auditor focusing on the open non-conformances, as opposed to revisiting areas that were previously found in compliance.
- Members may be granted up to **three consecutive CoP one-year certificates.** But if, at the **fourth attempt**, there are still any major non-conformances, the member's CoP certification and membership will be immediately withdrawn, and it will have to reapply for membership upon successful completion of an RJC CoP audit with no major non-conformances.

CoC audits

- Members with any major non-conformances cannot get certified. Similarly, outsourcing contractors with any major non-conformances cannot be included in the scope of the certification.
- If a major non-conformance is found during the surveillance audit, CoC certification will be suspended.
- Once all major non-conformances have been addressed, member can ask for another audit.

Any **critical breach** would suspend an existing CoP or CoC certificate or prevent the issue of a new one.

Useful links:

- ✓ STANDARDS, ASSESSMENT MANUAL & SELF-ASSESSMENT
  - Codes of Practices (CoP): click here | Chain of Custody (CoC): click here |Find an Auditor
- ✓ RESOURCES
  - Member training CoP 2013 vs 2019 video
  - CoP 2019 Walkthrough Page, where you will find sections dedicated to:
    - Provision 6 - Human Rights | Provision 7 - Due Diligence Guidance for Responsible Sourcing from Conflict Affected and High-Risk Areas | Provision 12 Know Your Counterparty: Money Laundering and Finance of Terrorism | Provision 14 - Provenance Claims | Provision 28 - Product Disclosure
  - Small Business Sustainability Toolkit & Retailer Sustainability Toolkit