RESPONSIBLE JEWELLERY COUNCIL

RJC Summary of Changes

Assessment Manual v1.3, December 2020

About

This document presents the substantive changes between the Assessment Manual version 1.2 (published January 2020) and the latest version 1.3 published in December 2020. Substantive changes are defined in the RJC's Assurance System Change Protocol as those that give a new intent or are a modification of the previous intent of a clause, provision, or requirement. Minor changes are defined as those that do not change the intent of a clause, provision, or requirement and therefore have no effect on the audit process.

The substantive changes described in the table below have been made in response to stakeholder feedback during Auditor Roundtables in April and September 2020, and to align the RJC's assessment methodology with ISEAL Assurance Code of Good Practice v2.0 criteria. The table shows which clauses have been updated, why, how, and what this means for the audit process.

Effective date and implementation

The Assessment Manual version 1.3 supersedes the previous version 1.2 (published January 2020) as of 1 April 2021. From the effective date all certification and recertification audits conducted against the COP 2019 and CoC 2017 standard must use this updated assessment methodology. Mid-term reviews and surveillance audits against the COP 2019, COP 2013, CoC 2017, or CoC 2012 standard should use v1.2 as the assessment methodology, unless the Assessment Manual v1.3 was used for the previous audit.

Questions and feedback are welcome for the attention of the Assurance Manager to accreditation@responsiblejewellery.com

Clause or section	Previous wording or intent	New wording or intent	Impact	Rationale for change
5.2 Procedures	The RJC will suspend the member	The RJC will consider suspending the member	The member may not immediately be suspended	There may not always be sufficient grounds to suspend the member
Disciplinary procedures for a critical breach	None	The auditor must give notice to RJC and the member of critical breaches raised within three working days of identification	New timeline for notifying	Streamlined, consistent procedure
Disciplinary procedures for a critical breach	None	The audit must be completed in the event of finding a critical breach	Audit process lengthened	Clarification and consistency of audit process where critical breaches are found
Table 5a COP conformance ratings – minor	Minor non-conformance is triggered when a member has failed to identify a relevant legislative or regulatory requirement	Minor non-conformance is triggered when a member is not in compliance with a relevant legislative or regulatory requirement, but has made good faith efforts to comply	Revised intent	The previous wording was more akin to a major non-conformance grading
Table 5a COP conformance ratings – major	Major non-conformance is triggered when a member failed to identify a relevant legislative or regulatory requirement, or knows it has not complied with one and has not adequately tried to rectify the non-conformance	Major non-conformance is triggered when a member has knowingly ignored a relevant legislative or regulatory requirement, or has not adequately tried to rectify a non-conformance with a relevant legislative or regulatory requirement	Revised intent	The previous wording was more akin to a minor non-conformance grading
Table 5b CoC Standard conformance ratings – major	Major non-conformances occur when there is the total absence of the implementation of the provision or systemic failure or	Deleted	Reduced definition of CoC critical breach	Systemic failures and an absence of controls were previously classified as CoC major non-conformances, which is severe and hence upgraded to critical

Clause or section	Previous wording or intent	New wording or intent	Impact	Rationale for change
	total lack of required controls			
8.3 Identifying critical breaches	A CoC critical breach is any finding or observation, supported by objective evidence, of deliberate falsification of information to support a conformance rating	A CoC critical breach is a critical non-conformance raised against any of the CoC provisions, supported by objective evidence that is triggered by: • deliberate falsification of information required to support a conformance rating; or • a systemic failure of the management system to implement the CoC; or • total lack of controls needed to manage risks to the CoC.	Revised intent, broader definition of CoC critical breach	Systemic failures and an absence of controls were previously classified as CoC major non-conformances, which is severe and hence upgraded to critical
Table 6 List of critical provisions in the COP	None	Provision 7 Due diligence for responsible sourcing from conflict-affected and high-risk areas	New requirement	To strengthen implementation of this provision, which is key to improving transparency and integrity in the supply chain. Strong stakeholder feedback
8.4.2 Non-conformances at multi-sites	None	All non-conformances shall be raised against the site at which they are identified, and recorded in the audit report as such.	New requirement	Clarification and consistency for how non-conformances are raised for multi-site members
Table 7 Consequences and follow up action resulting from a non-conformance Table 8 Dealing with COP and CoC Standard	None	A corrective action plan for minor non-conformances must be submitted to the auditor within one month of the closing meeting of the audit	New requirement	Clarification and consistency with existing process for major non-conformance corrective action plans

Clause or section	Previous wording or intent	New wording or intent	Impact	Rationale for change
corrective action plans				
Table 7 Consequences and follow up action resulting from a non-conformance	The effective implementation and closure of corrective actions will be reviewed by the auditor during subsequent audits	The effective implementation and closure of corrective actions will be reviewed by the auditor during the next scheduled audit	Auditors must check corrective action implementation for all minor non-conformances at the next scheduled audit	Streamlined and consistent process for verifying the closure of minor non-conformances
Table 10 Minimum number of sites to visit	Retail sites excluded from sample plan	Retail sites included in the sample plan, revised methodology using square root for members with more than 100 sites	New and revised requirements	To capture retail site sampling within this table creates consistency in retailer site sampling approaches across all CABs
12.3.5.a Suggestions for improvement	None	Suggestions for improvement can only be offered for operations or processes that are unrelated to areas where non-conformance has been identified	New requirement	Clarification and differentiation
Table 14 Criteria for determining mid-term reviews	Mid-term review not required when no non-conformances are raised (i.e. full conformity)	Mid-term review not required when up to three minor non-conformances are raised	Revised intent	Strong stakeholder feedback regarding triggers for mid-term reviews
Table 14 Criteria for determining mid-term reviews	Desktop mid-term review triggered with up to two minor non-conformances for critical provisions, or up to four minor non-conformances in total raised	Desktop mid-term review triggered with four or five non-conformances raised	Revised intent	Strong stakeholder feedback regarding triggers for mid-term reviews
Table 14 Criteria for determining mid-term reviews	Onsite mid-term review triggered with three or more minor non-conformances for critical provisions, or five or non-conformances in total raised	Onsite mid-term review triggered with six or more minor non-conformances raised	Revised intent	Strong stakeholder feedback regarding triggers for mid-term reviews
Table 14 Criteria for determining	Desktop mid-term review triggered when there is no risk of	Deleted requirement	Fewer triggers for desktop mid-term	Difficult for the auditor to predict whether there is a risk of non-

Clause or section	Previous wording or intent	New wording or intent	Impact	Rationale for change
mid-term reviews	non-conformance with critical provisions		review	conformance with critical provisions. If there is a non-conformance this should be raised as such and therefore will count in the number of non-conformances that trigger the mid-term review
Table 14 Criteria for determining mid-term reviews	Onsite mid-term review triggered when there are facilities that risk non-conformance with critical provisions	Deleted requirement	Fewer triggers for onsite mid-term review	Difficult for the auditor to predict whether there is a risk of critical breach. If there is an actual non-conformance this should be raised as such and therefore will count in the number of non-conformances that trigger the mid-term review
12.4.3 Submit monitoring and evaluation data	Section that requires auditors to submit information for the purposes of RJC M&E	Deleted section	Reduced reporting requirements	This information is already collected as part of the audit report template – duplicative and redundant to request it separately
12.4.4 Submit an audit report	None	Introduced process and timelines for reviewing and finalising audit report by CAB	New requirements	Streamlined and timely process for audit report review, closure and submission to RJC
12.4.4 Submit an audit report	Instructions regarding the audit report formatting	Deleted instructions	Fewer instructions	Duplicative and redundant because RJC only accepts the audit report if using the RJC template – which by default captures these instructions