ALLIANCE FOR WATER STEWARDSHIP CERTIFICATION REQUIREMENTS

ASSESSMENT OF CONFORMITY WITH THE INTERNATIONAL WATER STEWARDSHIP STANDARD (AWS STANDARD)

VERSION 4.0

30 SEPTEMBER 2024

Alliance for Water Stewardship (AWS) is registered as a Scottish Charitable Incorporated Organisation (SCO45894).
Alliance for Water Stewardship, AWS and the water droplets logo are the trademarks of Alliance for Water Stewardship
AWS, 2 Quality Street, North Berwick, Scotland, EH39 4HW | Website: a4ws.org Email: info@a4ws.org

CONTENTS

INTRODUCTION

The purpose of the *AWS Certification Requirements* is to set forth requirements for third-party conformity assessment and certification of sites against the International Water Stewardship Standard (AWS Standard). AWS reserves the right to change these requirements at any time, in accordance with the review and approval process set out by the AWS Technical Committee (TC) Terms of Reference[1].

Where events outside the control of AWS and/or CAB can be characterised as *force majeure* (for example, pandemic, war, act of terrorism, travel restrictions, international trade sanctions, etc.), AWS reserves the right to create additional policies that may affect these Certifications Requirements.

RESPONSIBILITY FOR THIS DOCUMENT

The TC is the body responsible for the AWS Certification Requirements. The TC will review the contents of this document on an ongoing basis. A record of amendments is shown below:

VERSION HISTORY

VERSION NO.	DATE OF PUBLICATION	DESCRIPTION OF AMENDMENT
V1.0	July 2015	Approved
V1.1	January 2018	Replacement of Appendix 3. AWS Objection Procedure with AWS Comments, Complaints and Appeals Procedure. Replacement of Section 7. Communication of AWS Assets with AWS Claims Policy and Procedure.
V2.0	December 2019	Updated in line with Version 2.0 of the AWS Standard and accompanying documents, and revised to reduce repetitions, language clarity and to integrate Professional Credentialing.
V3.0	20 December 2022	Updated to strengthen system integrity, improve language consistency, clarity and reduce repetition.
V3.1	25 October 2023	Alignment with ISEAL Alliance Assurance Code (see Sections 2.4, 2.6, 3.1, 3.2 and 6.2) and addition of the Assurance Derogation procedure.
V4.0	30 September 2024	Strengthened Internal Control System. Removal of Multi-site Operation. Removal of single catchment and homogeneous production requirements. Group Operation redefined. Overall review of certification process for clarity.

TRANSITION PERIOD

The changes in this document shall be effective six months after the release of this version, which is 1 April 2025.

AWS STANDARD SYSTEM

The Alliance for Water Stewardship (AWS) is a global, non-profit organisation whose mission is to ignite and nurture global and local leadership in credible water stewardship that recognises and secures the social, cultural, environmental, and economic value of freshwater. AWS developed The International Water Stewardship Standard (AWS Standard) as part of this mission. The AWS Standard was the result of an international, ISEAL Code Compliant, multi-stakeholder process that responds to the growing need for evidence of robust water risk and impact mitigation efforts. It is built around the notion of implementing water stewardship at the site level in a way that understands and engages with the broader catchment and works with other stakeholders to address shared water-related challenges and opportunities. As a

[1] Technical Committee Terms of Reference – a4ws.org/download/technical-committee-terms-of-reference-may-2024

Code Compliant ISEAL member[2], AWS is committed to an equitable, open, and transparent approach to setting and maintaining its Standard System.

The AWS Standard System means the set of standards, policies and procedures established by AWS, including the AWS Standard and associated guidance, governance bodies, training programme, conformity assessment and associated intellectual property.

The AWS Assurance System[3] has been developed to assess conformance with the AWS Standard, which is consistent with the ISEAL Credibility Principles, providing truthfulness, impartiality, transparency, reliability, and value creation. A central feature of the AWS Standard System is the role of impartial assessment by a Conformity Assessment Body (CAB). The AWS Standard System strives to leverage the competencies of ISO 17065 accredited CABs.

AWS is the owner of the AWS Standard. As such, AWS is responsible for standard-setting, training, assurance, claims, and monitoring and evaluation. These programmes are complementary and serve to reinforce one another to ensure that the AWS Standard System provides credible and robust implementation of the AWS Standard to deliver on the AWS mission.

KEY AWS STANDARD SYSTEM DOCUMENTS

The AWS Standard System is rooted in three key documents. Table 1 shows their scope and interrelationship.

TABLE 1. KEY DOCUMENTS OF THE AWS STANDARD SYSTEM

NORMATIVE DOCUMENT	PURPOSE	AWS LEAD	TARGET AUDIENCES
1. **International Water Stewardship Standard (AWS Standard)**	Defines the criteria and indicators for conformance. Supporting the AWS Standard is also the General Guidance.	System Integrity Business Unit	- **Sites** - **CABs** - **Consultants**
2. **AWS Certification Requirements**	Sets the process for certification to the AWS Standard.	System Integrity Business Unit	- **Sites** - **CABs** - **Consultants**
3. **AWS Professional Credentialing Programme Handbook**	Describes the training, competency, fee structure, claims, and recordkeeping requirements for those wishing to be AWS Professionally Credentialed.	System Integrity Business Unit	- **Professionally Credentialed individuals**

[2] The ISEAL Alliance – www.isealalliance.org/about-iseal/what-is-code-compliant

[3] An Assurance System consists of a normative standard or standards; a risk management plan; criteria for accepting assurance providers to the scheme; criteria for accepting sites to the scheme; criteria for group assessments where applicable; methodology for assessment of clients e.g. application, audit, review and decision, surveillance, sanctions, complaints and appeals; requirements for the certificate, which identifies the product, process or service to which it applies; and requirements for oversight of assurance providers.

SCOPE

The requirements presented in this document, the *AWS Certification Requirements*, apply to all Conformity Assessment Bodies (CABs) that are approved to engage in the provision of conformity assessment services in relation to the AWS Standard, as well as to the sites seeking AWS Certification.

DEROGATIONS

In exceptional circumstances, AWS reserves the right to grant derogations, when requested by CABs, to the Certification Requirements (this document). CABs shall inform AWS in writing using the AWS Assurance Derogation form, submitted to email: assurance@a4ws.org. CABs are to wait for written approval before proceeding. Where a derogation is granted by AWS, it will be recorded in the AWS Derogation Log and may be made publicly available.

REFERENCES[4]

International Water Stewardship Standard (AWS Standard).

AWS Claims Policy.

ISO/IEC 17065:2012(E) Conformity assessment – Requirements for bodies certifying products, processes, and services.

ISO 19011:2018(E) Guidelines for auditing management systems.

ISO 17011:2017(E) Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies.

European Union (EU) General Data Protection Regulation (GDPR) Compliance Guidelines.

UK General Data Protection Regulation (UK GDPR).

UK Data Protection Act 2018.

EC Privacy and Electronic Communications (EC Directive) Regulation 2003.

TERMS AND DEFINITIONS

Relevant definitions are as noted in Part 3 of ISO 17011:2017 and the Glossary of Terms included in the AWS International Water Stewardship Standard.

GENERAL REQUIREMENTS

Conformity assessments with the AWS Standard shall be completed by CABs appointed by AWS and accredited for the scope of the AWS Standard under the *ISO 17065:2012(E) Conformity Assessment — Requirements for bodies certifying products, processes, and services.* The accreditation shall be obtained through an Accreditation Body that is a signatory of the International Accreditation Forum (IAF) (see https://iaf.nu/en/recognised-abs).

For the purposes of certification, AWS distinguishes two types of operation: Single Site or Group Operation.

[4] Or most recent version.

1 REGISTRATION AND CERTIFICATION AGREEMENT

1.1 CONFIRMATION OF REGISTRATION

1.1.1 Before proceeding with a Certification Agreement, the CAB shall confirm that the site has registered its site(s) with AWS and their intent to pursue certification of the proposed site(s) or group operation, and

1.1.2 The CAB shall record the AWS Site Registration Number (see Box 1) and include this identifier in all certification documents and communications relating to the site(s) (for example, audit reports, certificates, surveillance reports, and email correspondence).

BOX 1 AWS SITE REGISTRATION NUMBER

When a site is registered on the AWS website, AWS assigns it a unique AWS Site Registration Number. This number is used to track all stages of a site's status over time. AWS Site Registration Numbers have the following format: AWS-XXXXXX.

1.2 INITIAL ARRANGEMENTS AND CERTIFICATION AGREEMENTS

1.2.1 Prior to entering a Certification Agreement, the CAB shall confirm with the site(s) the scope of the proposed conformity assessment and verify that it falls within the CAB's scope of AWS accreditation (for example, for region and sector, as applicable).

1.2.2 The CAB shall enter into a Certification Agreement with the site(s) seeking certification, including the agreed-upon costs. Certification Agreements shall be made available to AWS upon request.

1.2.3 The CAB shall maintain a written estimation of the cost and the time needed to execute and complete certification activities considering, but not limited to:

- 1.2.3.1 pre-assessment, when requested by the applicant
- 1.2.3.2 preparation of the audit
- 1.2.3.3 conducting the opening and closing audit meetings
- 1.2.3.4 performing document and records review
- 1.2.3.5 conducting interviews
- 1.2.3.6 traveling to and between sites
- 1.2.3.7 collecting and verifying information
- 1.2.3.8 evaluating open non-conformities
- 1.2.3.9 analysing and compiling audit findings
- 1.2.3.10 technical reviews and certification decision

1.2.4 The CAB shall inform the site(s) about its *Comments, Complaints and Appeals Procedure* prior to entering into a Certification Agreement.

1.2.5 Throughout the provision of AWS assurance services, the CAB shall comply with all the requirements of the European Union (EU) General Data Protection Regulation (GDPR) Compliance Guidelines; UK General Data Protection Regulation (UK GDPR); UK Data Protection Act 2018; and EC Privacy and Electronic Communications (EC Directive) Regulation 2003.

2 CONFORMITY ASSESSMENT

2.1 PRE-ASSESSMENT

2.1.1 Pre-assessment[5] can be useful to facilitate the implementation process leading to successful certification against the AWS Standard. In the event a CAB is requested to conduct a pre-assessment, the CAB must ensure the required impartiality and avoidance of conflict of interest if they wish to also provide conformity assessment services to the same site(s).

2.1.2 In cases where a CAB is retained to do a pre-assessment at a site where they will also be providing conformity assessment services, the pre-assessment is not considered consulting unless the report provides recommendations.

2.2 AUDIT TEAM

2.2.1 The CAB shall assign at least one Lead Auditor for each assessment that fulfils AWS requirements found in Annex 1A.

2.2.2 A Support Auditor (see Annex 1B) may be appointed at the discretion of the CAB when there is a need for capacity (Group Operations) or a deeper understanding of local context (e.g., applicable legislation). Where expertise on production processes is needed, a Technical Expert may be appointed by the CAB to support the audit team (see requirements in Annex 2).

2.2.3 Which part of the audit team must be onsite at any given time of the audit is based on the specifics of availability of documents and site personnel. At a minimum, audit team personnel need to be onsite if necessary to fulfil the requirements of the audit team qualifications and the audit plan.

2.3 AUDIT PREPARATION

2.3.1 The site(s) shall collaborate on the audit preparation to optimize the time and resources of the CAB. For this, the site shall:

2.3.1.1 Confirm with the CAB the exact audit dates not less than eight (8) weeks before the beginning of the audit, as well as the availability of the relevant personnel who should take part in the audit. This helps the Audit Team to provide an accurate Audit Plan.

2.3.1.2 Submit relevant information on the management system for water stewardship to the CAB, at a minimum:

- A list of identified relevant internal and external stakeholders for the site(s), including their contact data. This is used by the audit team to better estimate the time to allocate to indicators related to stakeholder engagement;
- The site's Water Stewardship Plan. This is used by the audit team to better calculate the level of effort to address actions the site has initiated; and
- In the case of Group Operations, provide an internal audit report per site, with genuine and reproducible comments, conducted within six (6) months prior to the initial/recertification audit. This will allow the Lead Auditor to assess the complexity of the system in place and confirm that the Standard has been effectively implemented before calculating the sample of sites to visit during the audit (see Section 5.3.2).

2.3.2 In preparation for the audit, the Lead Auditor shall:

2.3.2.1 provide the site(s) with a list of information and other materials that shall be prepared by the site prior to the on-site audit;

2.3.2.2 inform the site(s) that the audit team requires free and safe access to facilities at the site(s);

2.3.2.3 arrange and agree the audit dates with the site(s);

2.3.2.4 send an Audit Plan to the site(s); and

[5] A pre-assessment is an optional preliminary review conducted by a CAB, Consultant or AWS Professionally Credentialed Individual to inform a site whether it is ready to enter full assessment.

2.3.2.5 confirm whether the audit team will need a translator (for example, to conduct internal and external stakeholder interviews).

2.3.3 Where a translator is used, the CAB shall record their name(s) and affiliation(s) in the Audit Report. Translators shall be independent of the site(s) and not be a direct employee of the site(s), site owner or subsidiaries of the audited site owner. Otherwise, the CAB shall record the justification for their use.

2.3.4 Prior to the audit, the audit team shall prepare the audit by reviewing, at least, the following:

2.3.4.1 the information submitted by the site(s) (as per 2.3.1.2); supplementary materials submitted by the site(s) at the time of or after application to the CAB for AWS Certification;

2.3.4.2 internal audit reports (for Group Operations);

2.3.4.3 information about the site(s) or request for interview submitted by stakeholders prior to the audit (to be provided by AWS);

2.3.4.4 water risk maps using tools such as: https://www.wri.org/initiatives/aqueduct, or https://riskfilter.org/water/explore/map, or https://www.globalwaterwatch.earth); and

2.3.4.5 applicable laws and regulations relevant to the site(s) (e.g., https://aqualex.fao.org[6]) and potential open water-related conflicts around the site (e.g., https://ejatlas.org).

2.4 STAKEHOLDER ANNOUNCEMENT

2.4.1 The Stakeholder Announcement shall invite stakeholders to submit oral and/or written comments and feedback or to meet with the Audit Team. A stakeholder's wish for anonymity shall be upheld. Oral and/or written submissions made in reference to the site's operation should be supported with objective evidence wherever possible.

2.4.2 At least eight (8) weeks before the start date of the initial certification audit or the re-evaluation audit, AWS will publish on its website the dates of the assessment of the site(s) with the intention to pursue AWS (Re-)Certification. Stakeholder submissions are accepted from this date and during the entire period of validity of the AWS Certificate. Submissions, comments and/or feedback received by AWS will be shared with the CAB so the audit team may use the information for their investigations during the next audit (see Section 2.3.4.3).

2.4.3 The site(s) seeking certification shall complete the Stakeholder Announcement Form found on the AWS website, and release it in at least two outlets: published in local language(s) on the site's website(s) and in a local media outlet (if applicable, economical, practical, and available) that is appropriate for the site and the related stakeholders (for example, local newspaper, radio, or websites).

2.4.4 At a minimum, the Stakeholder Announcement shall specify:

2.4.4.1 AWS Site Registration Number(s) of all sites within the scope of certification;

2.4.4.2 CAB client name, site (s) owner name(s), site name(s); site address(es); GPS coordinates of all sites within the scope of certification; type of site (single site or group operation);

2.4.4.3 full name of the CAB and CAB website;

2.4.4.4 full name of AWS and AWS website;

2.4.4.5 the reference to submit feedback (email: assurance@a4ws.org);

2.4.4.6 date(s), location(s), and type of audit (for example, initial audit, re-evaluation audit, re-certification audit); and

2.4.4.7 how the audit is to be conducted (for example, on-site or remote[7]).

[6] Aqualex provides free access to national and international legal instruments regarding water.

[7] Remote audit is defined as 'An audit of a site that is not conducted on-site. Remote audits may include off-line (e.g., document review) or real-time virtual (for example, video calls) approaches, or combinations thereof'. (Source: based on ISEAL Alliance guidance)

2.5 CONDUCTING THE AUDIT

The audit team shall gather objective evidence of the site's conformity with all the applicable criteria and indicators in the current version (at the time of the audit) of the AWS Standard for every certification and re-certification. The structure of the audit should generally follow the auditor guidance given in ISO 19011:2018 - Guidelines for auditing management systems.

2.5.1 All audits (certification, recertification, and surveillance) shall include an opening meeting, document review of the site's Water Stewardship Plan, physical observation of the site(s) included in the scope of the audit, interviews with internal and external stakeholders, and closing meeting. For initial audits only, sites have the option to complete the audit in two stages (see Section 2.6).

2.5.2 The Lead Auditor shall assess the effectiveness of the corrective actions implemented after the previous audit(s).

2.5.3 As part of the audit, the audit team shall conduct interviews with representative internal and external stakeholders and/or stakeholder groups to assess site conformity with relevant indicators of the AWS Standard. Within the three-year cycle of each certificate, interviews shall be conducted by the auditors with persons and/or groups representing at a minimum:

- 2.5.3.1 one relevant water-related government authority within the site(s) catchment area (or with responsibility for it);
- 2.5.3.2 one contracted supplier to the site(s);
- 2.5.3.3 one civil society organisation operating within the catchment; and
- 2.5.3.4 one representative of an affected community, especially from those that use the same water source and/or are affected by water discharge from the site(s).

2.5.4 The audit team shall also conduct interviews with site staff to assess conformity with relevant indicators of the AWS Standard.

2.5.5 The CAB shall visit the relevant water source locations and water-related discharge locations during the onsite audits; the Lead Auditor shall provide the rationale behind their judgment-based sampling.

2.5.6 The audit team shall record evidence for each indicator during the audit; this evidence shall be traceable, genuine, and objective. Audit checklists, prepared against the AWS Standard, shall be used by the CAB.

2.6 STAGE 1 AND STAGE 2 INITIAL AUDIT

2.6.1 The site(s) may request the CAB to conduct the initial audit in two stages referred to as Stage 1 and Stage 2.

2.6.2 Stage 1 may be completed remotely and shall be followed by Stage 2 no later than three (3) months after the site receives the Stage 1 preliminary report.

2.6.3 The CAB shall send the site a preliminary report with findings immediately after the Stage 1 audit, which assesses all documents for all relevant indicators of the AWS Standard.

2.6.4 Stage 2 of the initial audit will assess onsite the implementation of the AWS Standard and result in a Findings Overview (see Section 2.9). The audit process will continue as described in the following sections of this Certification Requirements document.

2.6.5 The site(s) shall be responsible to ensure the availability of the relevant personnel and a stable internet connection that allows Stage 1 to be completed efficiently and effectively.

2.7 AUDIT RESULTS

2.7.1 The assessment of each indicator shall be graded as a conformity or non-conformity. It is not permitted to assign "not applicable (N/A)" to any indicator.

2.8 MANAGEMENT OF NON-CONFORMITIES

2.8.1 Where the audit team determines that the site does not conform with an indicator, the audit team shall raise a non-conformity.

2.8.2 For each non-conformity identified, the CAB shall require the site(s) to provide a Corrective Action Plan which includes:

2.8.2.1 an analysis of the root cause/s of the non-conformity; and

2.8.2.2 the specific corrective action(s) to address the identified root cause/s.

2.8.3 All non-conformities shall be satisfactorily addressed by Corrective Action Plans prior to certification being granted. For this, sites have ninety (90) calendar days after the audit. The day of the closing meeting is “Day zero (0)".

2.8.4 The CAB shall review the evidence submitted by the site(s) as part of the Corrective Action Plan as soon as they are received. This evidence shall be considered sufficient to state that the non-conformities are closed. The effectiveness of the corrective actions will be verified during the subsequent audit.

2.8.5 If a certificate holder does not address a non-conformity within 90 days after the audit, the CAB shall suspend the process and the certificate, when applicable (see section 4.5), for a maximum of six (6) months. After this period, without resolution of the pending non-conformity, the CAB shall cancel the process as it is not possible to take a certification decision. The site may then restart the process and complete a new full audit, to achieve certification.

2.9 REPORTING AUDIT RESULTS

2.9.1 The audit team shall prepare a Findings Overview at the end of the audit to be presented during the Closing Meeting, including at a minimum:

2.9.1.1 the information of the assessment: company general information, AWS registration number, dates of the assessment, scope of the audit and level of the assessment;

2.9.1.2 the reference of the nonconformities detected with a brief description of the deviation, sufficiently detailed for the site(s) to initiate its root cause analysis;

2.9.1.3 the indication of whether a technical review may identify additional nonconformities (or remove some of the granted ones) shall be provided to the site(s) not later than six (6) weeks after the audit;

2.9.1.4 details about the next steps in the process: period for submitting the corrective action plan for all non-conformities; and

2.9.1.5 a reference to the CAB complaints/appeal procedures.

2.9.2 For internal purposes and to support the certification decision, the CAB shall prepare an Audit Report containing, at a minimum:

2.9.2.1 the information in the Findings Overview.

2.9.2.2 names and roles of the members of the audit team (including translator(s), technical and/or local experts, including their affiliation), and site staff that participated in the audit.

2.9.2.3 audit date(s) and total audit duration (in person-day); to unify criteria, the day of the closing meeting is considered the audit date (when no reference is made to “start – finishing” dates).

2.9.2.4 scope of the audit, including all locations and facilities that were audited and an indication of whether the audit was conducted on-site or remotely.

2.9.2.5 overview of all internal and external interviews conducted during the audit, including names of the interviewees, their positions, and their organisations. If the internal or external stakeholder(s) wish to remain anonymous this shall be upheld.

2.9.2.6 name and description of the catchment(s) in which the site operates and a summary of shared water challenges.

2.9.2.7 a checklist or table of all AWS indicators assessed as conformity or non-conformity and the evidence that was considered during the audit; a section summarising site strengths and any identified opportunities for improvement.

2.9.2.8 the audit team's overall recommendation to the CAB reviewer(s) whether to issue certification and, if so, clearly identify the certification level to be awarded (AWS Core, AWS Gold, or AWS Platinum).

2.10 CERTIFICATION DECISION

2.10.1 The CAB shall inform the site(s) of its certification decision no later than thirty (30) calendar days after all non-conformities are considered by the CAB as closed (i.e., no later than four (4) months after the audit.)

2.10.2 A certificate of conformity shall only be awarded when all indicators for the corresponding certification level have been met to the satisfaction of the CAB.

2.10.3 Once the certification decision is taken, the CAB has 10 working days to share the relevant information of the process with AWS.

2.10.4 The CAB shall retain records to demonstrate that it has reviewed audit documents and has taken the certification decision in accordance with the AWS Requirements for Conformity Assessment Bodies Appointed from 1 October 2021.

2.10.5 AWS will not acknowledge a site as being certified until a Certification Report is submitted and approved by AWS for posting on the AWS website.

2.10.6 The CAB shall inform the site(s) that their AWS certificate is only valid once the Certification Report has been posted on the AWS website. The site(s) shall not communicate publicly about the certification until the Certification Report is made publicly available on the AWS website.

2.10.7 AWS certificates issued by the CAB shall indicate the following:

2.10.7.1 CAB Client name, name of site owner, full site name and address (or certificate holder where it is not the site)

2.10.7.2 name and address of the site(s) (if different from above or in case of Group Operation);

2.10.7.3 full name of CAB;

2.10.7.4 version of AWS Standard used;

2.10.7.5 date certificate issued and date of expiry;

2.10.7.6 certificate scope (single site or group operation);

2.10.7.7 certification level (Core, Gold, or Platinum) achieved; and

2.10.7.8 AWS Site Registration number(s) of all sites within the scope of certification for the certificate.

2.10.8 The CAB shall issue original official AWS Site Certificates in English. Where requested in writing by the AWS Certified Site contact, a second certificate may be issued by the CAB in the requested relevant local language.

2.10.9 Certificates shall be valid for a period of three (3) years. For example, a certificate issued on 15 March 2025 will expire on 14 March 2028. An extension may be granted for a period of six (6) months (see Section 4.4 Re-Certification audit).

2.10.10 Where there is a certificate scope change, from a single site to group operation, a re-certification audit is required.

2.10.11 Upon awarding a certificate, the CAB shall inform the site(s) of its eligibility and the procedures for using specific AWS Assets as determined by the AWS Claims Policy. Note that no AWS Assets (for example, logos or claims) may be used by any site(s) with an expired, suspended, or withdrawn certificate.

2.11 PUBLIC REPORTING

2.11.1 The CAB shall prepare a summarised version of the audit report, called a Public Certification Report. This report is posted on the AWS website and is intended to provide transparency on the performance of a certified site. It shall include, at a minimum:

2.11.1.1 all elements in the Findings Overview (see Section 2.9.1), as well as details on how corrective actions have been closed.

2.11.1.2 site contact details (position and a valid email address suffices) to help stakeholders contact the certified site for inquiries.

2.11.1.3 When requested by AWS, all registered and certified sites, CABs, and/or Certification Partners are to provide additional information to support AWS Monitoring and Evaluation (M&E) efforts, demonstrating progress towards the Standard's outcomes, and in accordance with the ISEAL Code of Good Practice for Sustainability Systems, other guidance and/or other requirements.

3 CERTIFICATE MAINTENANCE

3.1 SURVEILLANCE AUDIT FREQUENCY

3.1.1 The maintenance of a valid certificate is done through completing annual Surveillance Audits during the period of validity (i.e., two surveillance audits within three years). The reference date for the surveillance audit is the date of the certification audit. For example:

- If a site's initial/recertification audit takes place on 10 February 2025 (calculated from the last day of audit); and
- If the certification decision is taken on 10 June 2025, and a certificate is issued valid until 9 June 2028, then the Year 1 Surveillance Audit is to take place by 10 February 2026, and the Year 2 Surveillance Audit is to take place by 10 February 2027.

3.1.2 There is flexibility in planning the surveillance audits, allowing sites to have them up three months before and/or three months after the due dates. Following the previous example, the first surveillance audit could take place between 10 November 2025 and 10 May 2026. This flexibility does not exempt sites from meeting the main requirement of completing two surveillance audits during the period of validity of their certificates.

3.1.3 The surveillance audits are normally conducted onsite. The CAB may consider remote surveillance audits where the following occur:

3.1.3.1 The previous audit (certification, surveillance, or recertification) resulted in ten (10) or less non-conformities, and;

3.1.3.2 The CAB considers the effectiveness of corrective actions can be assessed remotely.

3.2 SCOPE OF SURVEILLANCE AUDITS

3.2.1 The surveillance audits shall focus on assessing the activities sites have undertaken following the initial/certification audit during the validity period of the certificate. Two annual surveillance audits are required to be completed (see Section 3.1.1) that cover the following:

3.2.1.1 confirmation of the physical scope of the site(s);

3.2.1.2 review of the effectiveness of corrective actions implemented for non-conformities raised at the previous audit;

3.2.1.3 interviews with internal and external stakeholders (see Section 2.5.3);

3.2.1.4 visit relevant water source locations and water-related discharge locations (see Section 2.5.5);

3.2.1.5 assess changes, updates, and improvements in relation to:

3.2.1.5.1 stakeholder engagement and participation in catchment governance;

3.2.1.5.2 Water Stewardship Plan, including quantified progress against targets;

3.2.1.5.3 shared water challenges, with attention to site or catchment risk;
3.2.1.5.4 water balance and water quality
3.2.1.5.5 communications and disclosure activities; and
3.2.1.5.6 legal and regulatory compliance.
3.2.1.6 progress on areas for improvement (best practices, opportunities).

3.2.2 For sites with Gold or Platinum certificates, 50% of the advanced indicators will be assessed for each surveillance audit.

3.3 SURVEILLANCE AUDIT REPORT

3.3.1 The audit team shall prepare a Findings Overview at the end of the surveillance audit, addressing the requirements described in Section 2.9.1.

3.3.2 The period for CAB revision (six (6) weeks) and for submitting an effective correction plan are the same (three (3) months after the audit) as in initial/certification audits. Likewise, the CAB must take the decision of maintaining or not the certificate within four (4) months after each surveillance audit. This decision shall be based on a certification report that accumulates the initial audit info plus the surveillance audits conclusions, as well as the recommendation of the Lead Auditor for maintaining the certification.

3.3.3 The CAB shall send the revised Public Certification Report to AWS. AWS may make this report public. The content may include updates on the site's efforts during the whole period of validity of the certificate.

4 CERTIFICATE CHANGES

4.1 RE-EVALUATION OF CERTIFICATION LEVEL

4.1.1 A CAB shall consider requests from sites to re-evaluate the certification level (AWS Core, AWS Gold, or AWS Platinum), which is stated on the site's certificate.

4.1.2 An 'upgrade' of certification level (for example, from Core to Gold; from Gold to Platinum; or from Core to Platinum) is contingent on successful completion of an audit covering all core indicators, and the corresponding advanced-level indicators implemented by the site(s).

4.1.3 If requested by the site(s), the CAB may incorporate a re-evaluation (of the level) as part of the site's re-certification audit (that is, in accordance with the requirements in Section 4.4) provided that the timing of the re-certification audit would fit within the certificate cycle.

4.1.4 A recommendation for a 'downgrade' in certification level (for example, from Gold to Core; from Platinum to Gold; or from Platinum to Core) shall be accompanied by a written justification from the CAB including a summary of observations on those advanced-level indicators, which had been met by the site(s) at the previous audit; and any non-conformities that were raised (if applicable).

4.1.5 The CAB may schedule the re-evaluation to coincide with a surveillance audit:
4.1.5.1 Surveillance audit scope shall be expanded to reflect the new audit objective(s), which shall include an assessment of all core indicators and the corresponding advanced indicators for the certification level being sought.
4.1.5.2 A Stakeholder Announcement must be published in line with the requirements in Section 2.5 prior to a re-evaluation audit.
4.1.5.3 If a site's certification level changes because of a re-evaluation audit (that has coincided with a surveillance audit) the site's valid certificate can be amended to reflect the new level. However, the original expiry date of the certificate remains unchanged.

4.1.6 A CAB shall not upgrade a site's certification level based exclusively on results from a surveillance audit. That is, a re-evaluation is required for certificate upgrades.

4.1.7 The CAB may downgrade a site's certification level based on results from a surveillance audit if there is objective evidence supporting such a determination.

4.2 CHANGES TO SCOPE OF CERTIFICATION FOR GROUP OPERATIONS

4.2.1 A Group Operation with a valid certificate may include new sites in its scope following these steps:

4.2.1.1 the candidate site(s) implements the AWS Standard;

4.2.1.2 the candidate site(s) signs a Group Member Agreement with the managing legal entity;

4.2.1.3 the Group Operation Management Team confirms conformance with the AWS standard through a successful internal audit for the new site(s);

4.2.1.4 once confirmed conformance with the Standard (all non-conformities, if any, are resolved), the Group Operation Management Team requests in writing the inclusion of the new site(s) to the CAB;

4.2.1.5 the CAB confirms the inclusion of new site(s) in the scope of certification for the next assessment and will audit all new sites in addition to the required sampling methodology indicated in section 5.3.2.2; and

4.2.1.6 where the new site(s) is in conformance with the AWS Standard, the Group Operation certificate is updated by the CAB, but the period of validity remains unaltered.

4.2.2 A Group Operation Management Team with a valid certificate may remove a site or sites from its scope of certification. The Group Operation Management Team shall document the reason for removal e.g., voluntary withdrawal, poor internal audit results (see Section 5.2.6.6) and follow these steps:

4.2.2.1 The Group Operation Management Team informs the site in writing of the intent to remove it from the Group Operation; and the site is given the option to appeal;

4.2.2.2 Once the removal decision is confirmed, the Group Operation Management Team informs the CAB in writing of the change in scope of certification.

4.2.2.3 The CAB documents the changes, amends the certificate and shares with Group Operation Management Team and AWS.

4.2.2.4 The removed site(s) shall immediately cease use of all AWS claims, certificates, logos and other assets.

4.3 CERTIFICATE TRANSFER

4.3.1 The CAB shall have procedures to handle certificate transfers to and/or from another CAB if more than one CAB exists. The procedure shall include:

4.3.1.1 the outbound transfer of a client to a different CAB; and

4.3.1.2 the inbound transfer of a client from a different CAB.

4.3.2 Note: AWS considers transfer of site ownership (e.g., due to mergers or acquisitions) of a certificate to be a contractual matter between CAB and site(s) that should be handled in accordance with the Certification Agreement.

4.3.3 Should a site opt to change to a different CAB at any point after certification (that is, the transfer of certificate during the period of surveillance) the site shall:

4.3.3.1 notify AWS in writing of the details of the certificate transfer, including the reason for the transfer;

4.3.3.2 provide the current CAB with a notice of AWS certificate transfer, identifying the new CAB; and

4.3.3.3 provide the new CAB with a copy of their last audit report and surveillance report.

4.3.4 Prior to accepting a client transfer, the new CAB shall review all available information regarding all previous AWS-related audits.

4.3.5 Where the new CAB has doubts or concerns about the status of non-conformities that were raised in audits by the previous CAB, or any other material aspect of previous audits, the site shall authorize the previous CAB to share additional audit history information with the new CAB to ensure that all outstanding non-conformities are resolved.

4.4 RE-CERTIFICATION

4.4.1 The CAB shall conduct a re-certification audit of the site before the certificate can be re-issued or the period of validity extended. A re-certification audit is a 'full' conformity assessment.

4.4.2 The process for Re-Certification shall follow all steps as described in Section 2 except for Sections 2.1 and 2.6 that are not repeated.

4.4.3 If the re-certification process is expected to be delayed beyond the expiry date of the site's certificate, the CAB shall request in writing approval from AWS to extend the certificate, a minimum of four (4) weeks in advance of the certificate expiry date. A valid justification for the need for extension will be required (e.g., force majeure, organisational issues, travel restrictions, l pandemic, war, acts of terrorism). An extension may be granted for a maximum of six (6) months.

4.4.4 AWS will remove the site's certificate from the AWS website if the certificate has expired and no request for extension has been submitted.

4.5 SUSPENSION

4.5.1 Should a certified site fail to resolve non-conformities within the required timeframe, the CAB shall:

- 4.5.1.1 issue a warning letter for suspension;
- 4.5.1.2 suspend the certificate and notify the site that during this period, no claims or AWS Assets e.g., logos may be used by the site.
- 4.5.1.3 inform AWS within two (2) working days so that AWS may publish a notice of suspension on the AWS website; and
- 4.5.1.4 prepare a suspension report and submit it to AWS within five (5) working days.
  - 4.5.1.4.1 The suspension report shall give a rationale for suspension and provide a description of all unresolved non-conformities.
  - 4.5.1.4.2 AWS may publish the suspension report on the AWS website.

4.5.2 Suspended sites shall be given six (6) months to address the cause(s) for suspension.

4.5.3 The CAB shall not reinstate a suspended certificate until the site has successfully undergone another certification audit.

4.5.4 AWS reserves the right to request from the CAB the suspension or withdrawal of the certificate of any site that violates the spirit and intent of the AWS Standard or that goes directly against AWS's organisational mission.

4.5.5 The certificate holder shall assume responsibility for all sites named on the certificate whose actions may discredit AWS, including the actions of a site that may be added to the certificate through change of ownership, merger, or acquisition.

4.5.6 Where the site fails to notify the CAB (or the CAB fails to notify AWS) in writing that it no longer intends to continue with certification, the certificate will be marked as 'Expired' on the date that the next surveillance or re-certification audit is due.

4.6 TERMINATION

4.6.1 If the site has not resolved the cause of a suspension within six (6) months, the CAB shall:

- 4.6.1.1 terminate the certificate;
- 4.6.1.2 notify the site that they are ineligible to apply for AWS Certification for a period of no less than 12 months;
- 4.6.1.3 inform AWS in writing of the termination within five (5) working days so that AWS may publish a notice of termination on the AWS website; and
- 4.6.1.4 prepare a termination report and submit it to AWS within five (5) working days:

4.6.1.4.1 The termination report shall give a rationale for the termination; and
4.6.1.4.2 AWS may publish the termination report on the AWS website.

5 GROUP OPERATION

5.1 STRUCTURE

5.1.1 A Group Operation is considered when two or more sites apply together to obtain AWS Certification. The AWS Standard is implemented at each site, but the outcome of the certification process is a certificate for all sites covered in the scope of the assessment.

5.1.2 The group shall operate an Internal Control System (ICS). This structure serves as a tool to organise several sites around a common framework for the implementation of the AWS Standard and the AWS Certification Requirements in Section 5.2.

5.1.3 The ICS can be hosted by the parent company of a group of sites that seek certification as a group operation, or by one of the sites within that group (if decisions on assessment of conformity for all sites are taken independently). It is also possible for an independent entity, outside the Group Operation, to manage the ICS. In all cases, a Certification Agreement shall be signed between the Group and the CAB before initiating the certification process, and the entity hosting the ICS shall prove its legal capacity to enter into contractual agreements.

5.1.4 The group shall nominate a Group Operation Representative and inform AWS in writing. This Representative assumes overall responsibility for the group's implementation of and conformity with the AWS Standard, AWS Certification Requirements, and serves as the primary formal contact for communications with AWS and with the CAB.

5.1.5 The Group Operation Representative shall be responsible to:

5.1.5.1 establish a common management framework that explicitly adopts the objective of responsible water stewardship according to the AWS Standard;

5.1.5.2 ensure that the group structure and the Internal Control System (ICS) are in conformance with requirements of the AWS Standard and AWS requirements for group operations (see Section 5.2);

5.1.5.3 ensure that all members within the Group Operation are in conformity with the AWS Standard;

5.1.5.4 ensure that records for all Group Member sites are maintained up to date and all Group Member records are kept for a minimum of five (5) years;

5.1.5.5 prepare and approve documents, processes and procedures to be used by all sites within the scope;

5.1.5.6 carry out internal audits at all sites within the scope;

5.1.5.7 demonstrate to the CAB that the Internal Control System defined for the group will allow them to verify effectively that the group sites are in conformance with the AWS Standard; and

5.1.5.8 follow up on non-conformities raised during annual internal and external audits.

5.2 REQUIREMENTS FOR CERTIFICATION

5.2.1 The Group Operation is a legal entity that has the capacity to enter into a contractual agreement with the CAB for the purposes of certification against the AWS Standard.

5.2.2 There is a "Group Operation Management Team" nominated with the sufficient technical capacity to run an ICS within the Group Operation. The personnel involved shall fulfil, at least, the following roles:

5.2.2.1 ICS Manager: Oversight of the whole group structure and is the main person responsible for all certification-related topics and is the primary contact for AWS and the CAB);

5.2.2.2 ICS Decision Body: Person or group of persons with the authority to decide on the inclusion of new sites into the Group Operation, and on the sanctioning and/or withdrawal of existing certified sites; and

5.2.2.3 ICS Internal Auditor(s): person(s) nominated to conduct the internal audits of the Group Operation's sites against the AWS Standard. An internal auditor cannot be part of the ICS Decision body and shall comply with the competency requirements for Internal Auditors (see Annex 3).

5.2.3 Unless there is an existing legal agreement between the group sites and the entity hosting the ICS, a Group Membership Agreement shall be signed between the legal entity of the group operation and the sites that are part of the certification scope, containing at least the following:

5.2.3.1 a commitment by the Group Members to fulfil the requirements of the AWS Standard and the applicable AWS Certification Requirements;

5.2.3.2 a commitment by the Group Member to provide the group management with required information to meet the needs of the ICS in a timely manner;

5.2.3.3 acceptance by the Group Member of internal and external audits;

5.2.3.4 an obligation for the Group Member to report non-conformities; and

5.2.3.5 the rights of the Group Operation Management Team to terminate the membership of any member if continued participation by that member threatens the credibility and /or conformance against the AWS Standard of the group operation.

5.2.4 There is a system in place to keep the sites included in the certification scope aware of their obligations towards the AWS Standard (e.g., AWS Claims Policy, AWS Guidance, AWS Training).

5.2.5 The Group Operation Management Team completes a self-assessment before every (re)certification audit, where indicators are implemented centrally but executed locally at site level. The CAB will use the information supplied by the Group Operation Management Team to assess the effective implementation of the indicators at site level.

5.2.6 The ICS Internal Auditor(s) shall complete an internal audit for each of the sites that are part of the scope of the Group Operation seeking to obtain/maintain the certification, as well as for new sites joining the group proposed to the CAB. Internal audits shall be:

5.2.6.1 conducted within the six (6) months prior to the initial/certification audit (or the introduction of new sites into an existing group operation); this is a complete internal audit, assessing all indicators;

5.2.6.2 during the certificate's period of validity, internal audits shall be completed annually on each site with ensuring attention on the indicators that have been identified earlier as risky for each site during the first internal audit;

5.2.6.3 conducted independently (Internal Auditor does not work at the audited site);

5.2.6.4 documented with explanatory comments, and using the AWS Checklist, the Internal Auditor provides clear information of how the site conforms with all applicable indicators;

5.2.6.5 dated and signed by the Internal Auditor; when non-conformities are found, the Internal Auditor keeps record of the corrective actions implemented by the site and the date of resolution (which must be prior the external audit); and

5.2.6.6 lead to a decision taken by the ICS Decision Body stating that the site conforms with AWS Standard or not; in this case, it can be decided to sanction the site by excluding it from the scope of certification.

5.2.7 The "Group Operation Management Team" shall have a system to handle complaints and appeals that include independent investigations on the issues and a timely response with the decision taken. This system is to be used when:

5.2.7.1 the Group Operation receives a complaint from an external party, including the identified stakeholders, related to their water stewardship plan; or

5.2.7.2 a site disagrees with either the result of the internal audit or the decision taken by the ICS Decision Body.

5.2.8 The "Group Operation Management Team" maintains an updated list of all group members that includes at least the following information for each member:

5.2.8.1 site name and AWS registration number;

5.2.8.2 address of the site;

5.2.8.3 final product(s) or service(s), and processes undertaken at the sites;

5.2.8.4 annual volume of water use, withdrawals and discharge, per site;

5.2.8.5 group membership status (including any non-conformities and Corrective Action Plans);

5.2.8.6 date(s) of most recent internal audit;

5.2.8.7 date(s) of joining/leaving the Group Operation; and

5.2.8.8 any other group-specific information as required.

5.3 CONFORMITY ASSESSMENT

5.3.1 The CAB shall ensure that the Group is informed about the AWS Standard and AWS Certification Requirements for group operations before entering into a certification agreement.

5.3.2 Where certification of a group operation is sought, the CAB shall:

5.3.2.1 perform an audit of the Group Operation, wherever the ICS is managed, against the AWS group certification requirements outlined in Section 5.2, and the AWS Standard; and

5.3.2.2 assess the group operation's ICS to ensure conformity with the AWS Standard at site's level; for this, a representative sample of the sites that are part of the scope is audited on site every year. The sample is equal to the square root of the numbers of sites within the group, rounded up.

5.3.3 Where new members have joined the group since the previous audit, the CAB shall stratify them separately from the original pool of members at the next audit (that is, there will be two sampling strata: old members and new members) and the requirements for determining sample size shall be applied separately to each stratum (square root, rounded up).

5.3.4 The audit team shall review the ICS documentation to ensure internal audits have been carried out effectively, records are complete and non-conformities are resolved. This is to check the quality and effectiveness of the internal audits.

5.3.5 The CAB shall reserve the right to modify the initially planned sample (change of chosen sites, increase of the sample) at its discretion when findings at the central level indicate a potential issue on the implementation of the AWS Standard at the site level.

5.4 NONCONFORMITIES IN GROUP OPERATIONS

5.4.1 When a non-conformity for one indicator is identified in several sites, this may signify a systemic problem with the group's ICS. AWS sets a threshold of 25 per cent (%) for the observed non-conformity rate of sites within a group operation, rounded to the nearest whole number. If the thresholds are exceeded (that is, the number of non-conforming individual members is equal to, or greater than, this number), the CAB shall request a corrective action that is implemented in all sites, and demand proofs of implementation for the whole group (see Table 2).

TABLE 2. EXAMPLES: THRESHOLD FOR NON-CONFORMITIES IN GROUP OPERATIONS

EXAMPLE 1 GROUP OPERATION OF 35 SITES
A group with 35 sites receives an audit, with six (6) sites sampled; and two (2) sites have non-conformity with the same indicator. The non-conformity rate is 33% of sites, above the threshold of 25%. **Conclusion**: There is a systemic problem with the group's ICS; corrective action requested for all sites.
EXAMPLE 2 GROUP OPERATION OF 24 SITES
A group with 24 sites receives an audit, with 5 sites sampled; and 1 site have non-conformity with the same indicator. The Nonconformity rate is 20% of sites, below the threshold of 25%. **Conclusion**: No systematic problem with the group's ICS, corrective action requested only for the site with the NC (the Group may decide to implement actions at a wider level)

5.4.2 There is no distinction when managing non-conformities between group operations and single sites (see Section 2.8).

5.5 GROUP OPERATIONS AUDIT REPORT

5.5.1 The reporting requirements for single sites (see Sections 2.9 and 2.11) shall apply to audits of group operations.

5.5.2 In addition to single site reporting requirements, group operations audit reports shall contain the following information:

5.5.2.1 name and contact details of the Group ICS Manager;

5.5.2.2 a description of the group structure and relationships;

5.5.2.3 a register of all sites in the group suitable to be used as a schedule to the certificate with name and complete address and contact details for each site; and

5.5.2.4 the sites audited by the CAB.

ANNEX 1A - LEAD AUDITOR REQUIREMENTS

LEAD AUDITOR REQUIREMENTS			
Subject Area	A. Degree, Training or Certification	B. Previous Experience	Requirement
Education	Degree in a relevant discipline (e.g., hydrology, environmental engineering, agriculture, Water, Sanitation and Hygiene (WASH), forestry, water-related relevant social and economic issues)	Five (5) or more years of experience in the environmental sector	A or B
AWS Standard	AWS Standard System Training to Specialist level or equivalent and member of the AWS Professional Credentialing Programme	-	A
Auditing, General	ISO Lead Auditor training course	Three (3) or more years of experience (combined) serving as a Lead Auditor for: - environmental and social standards (for example, RSPO, FSC); or - ISO 14001; and/or - an equivalent standard	A or B
Auditing, AWS-Specific	AWS Standard System Training to Specialist level or equivalent, AWS Lead Auditor Training and member of the AWS PC Programme	Team member in at least two (2) AWS conformity audits and/or surveillance audits within the last five (5) years	A and B

ANNEX 1B – SUPPORT AUDITOR REQUIREMENTS

SUPPORT AUDITOR REQUIREMENTS			
Subject Area	A. Degree, Training or Certification	B. Previous Experience	Requirement
Language, culture, and local water knowledge applicable to the catchment	Fluency in the local language and knowledge of the local context	Good knowledge of the region[8] (for example, through past work experience, education) and the local environmental legislation and regulatory landscape	A or B
AWS Standard	Support Auditors to complete and pass AWS Standard System Training to Specialist level	-	A

[8] Region is understood to be based on criteria that includes culture, governance, geography, and customs.

ANNEX 2 - REQUIREMENTS FOR TECHNICAL EXPERTS FOR THE AUDIT TEAM

When a technical expert joins an audit team, he/she must be able to demonstrate competence in areas relevant to the AWS Standard and site context to assess specific risk factors and areas of greatest relevance. Technical subject areas are:

TECHNICAL SUBJECT AREA	A. BACKGROUND EDUCATION	B. WORK EXPERIENCE, TRAINING OR CERTIFICATION	REQUIREMENT
Water Resource Management (general background)	Water resource management, business, economics, environmental science or any one of the subject areas listed below	Five (5) or more years of work experience in water resource management relating to one or more of the outcomes of the AWS Standard	A or B
AWS Standard	-	AWS Standard System Training to Specialist Level	B
Water Governance	-	Five (5) or more years of work experience with water governance (planning, regulation, policy, law or permitting)	B
Water Balance	Civil engineering, hydrology	AWS training in water balance evaluation	A and B
Environmental Impact Assessment	Environmental science, civil engineering, ecology	Two (2) or more years of work experience with environmental impact assessments	A or B
Water, Sanitation and Hygiene	Environmental science, civil engineering, water resources management, international development	One (1) or more year of work experience with WASH-related issues	A and B
Water Quality	Environmental science, civil engineering, ecotoxicology, water resource management	Two (2) or more years of work experience with water quality analysis, monitoring, or modeling	A and B
Freshwater Ecology	Environmental science, ecology, biology, limnology	Two (2) or more years of work experience in an environmental field involving aquatic studies	A and B
Laws and Regulations (applicable to the catchment)	-	One (1) or more year of experience working in the environmental sector in the country where the catchment is located	B
Language and culture applicable to the catchment	-	Knowledge of context of the site location, gained through work experience or education; working knowledge of primary language used at the site, either through Lead or Local Auditors, or via translators	B

ANNEX 3 - REQUIREMENTS FOR INTERNAL AUDITORS (GROUP OPERATIONS)

Subject area	A. Degree, training, or certification	B. Previous experience	Requirement
Water Resource Management (general background)	Water resource management or environmental sciences	A minimum of two (2) years of work experience in water resource management relating to one or more of the outcomes of the AWS Standard	A or B
Auditing	AWS Internal Auditor Training for AWS Standard Certification	--	A
AWS Standard	New AWS Standard System Training to Specialist Level taken from Oct 2023	--	A
Laws and Regulations (applicable to the catchment)	-	A minimum of one (1) year of experience working in relation with sector of the scope and awareness on the applicable laws and regulations applicable in the country/countries where the catchment is located	B
Language and culture applicable to the catchment	-	Knowledge of context of the sites' location, gained through work experience or education; working knowledge of primary language used at the sites	B