ALLIANCE FOR WATER STEWARDSHIP (AWS) CERTIFICATION REQUIREMENTS

ASSESSMENT OF CONFORMITY WITH THE AWS INTERNATIONAL WATER STEWARDSHIP STANDARD V2.0

VERSION 2.0

DECEMBER 2019

Alliance for Water Stewardship (SCIO)
2 Quality Street, North Berwick, Scotland, EH39 4HW
Website: www.a4ws.org Email: info@a4ws.org
AWS is registered as a Scottish Charitable Incorporated Organisation (SCO45894)

CONTENTS

Purpose 3

Responsibility for These Requirements 3

AWS Standard System 4

AWS Standard Normative Documents 4

Scope 5

Normative References 6

Terms and Definitions 6

General Requirements 6

1 Pre-Assessment 6

2 Conformity Assessment 6

3 Surveillance and Certificate Maintenance 15

4 AWS Criteria for Single Site, Multi-Site and Group Operations 20

5 Requirements for Group Operations 24

6 Conformity Assessment of Group Clients 26

7 Use of AWS Assets 30

Appendix 1A. AWS Requirements for Qualifications of Lead AWS Auditors and Local AWS Auditors. 31

Appendix 1B. AWS Requirements for Technical Expertise of the Audit Team. 33

PURPOSE

The purpose of the *AWS Certification Requirements* is to set forth requirements for third-party conformity assessment and certification of clients against the AWS International Water Stewardship Standard v2.0 (“AWS Standard”) and to set forth AWS requirements for the associated processes of pre-assessment, conformity assessment of group operations, and the use of AWS assets and claims. This document is normative and applies to Conformity Assessment Bodies (CABs) that are accredited by AWS to perform conformity assessments of clients against the AWS Standard. AWS reserves the right to change these requirements at any time, in accordance with the review and approval process through the AWS Technical Committee.

RESPONSIBILITY FOR THESE REQUIREMENTS

The AWS Technical Committee (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.

AMENDMENT RECORD

VERSION NO.	DATE OF PUBLICATION	DESCRIPTION OF AMENDMENT
1.0	July 2015	Approved
1.1	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.
2.0	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.

AWS STANDARD SYSTEM

The Alliance for Water Stewardship (AWS) is a global, non-profit organization dedicated to advancing water stewardship around the world. As part of this mission, AWS developed *The AWS International Water Stewardship Standard*. The AWS Standard was the result of an international, four-year, ISEAL compliant, multi-stakeholder process which responded to the growing need for evidence of robust water risk and impact mitigation efforts. The revision of version 1.0 began in 2017 and culminated in the issuance of version 2.0 in March 2019. 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 to work with other water stakeholders to address shared water-related challenges and opportunities. As a full ISEAL member[1], AWS is committed to an equitable, open and transparent approach to setting and maintaining its standard. We are committed to the ISEAL Credibility Principles of sustainability, improvement, relevance, rigor, engagement, impartiality, transparency, accessibility, truthfulness, and efficiency. Accordingly, the AWS Standard System follows ISEAL's *Standard Setting, Assurance, and Impacts Codes*.

AWS has also developed an Assurance System for verifying conformance with the AWS Standard and which is consistent with the ISEAL Assurance Code, providing consistency, rigor, competence, impartiality, transparency, and accessibility. A central feature of the AWS Standard System is the role of independent certification by third-party Conformity Assessment Bodies (CABs). The Assurance system also includes the training and professional credentialing functions.

The AWS Standard Assurance System strives to leverage the competencies of independent third-party entities to assess compliance with the Standard – and draws heavily on existing international norms which apply to conformity assessment bodies (e.g. ISO 17065).

AWS is the standards system owner of *The AWS International Water Stewardship Standard*. As such, AWS is responsible for standard setting, capacity building, assurance and claims, and monitoring and evaluation. These programs 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.

AWS System means the system of standards, policies and procedures established by AWS, including the AWS International Water Stewardship Standard (AWS Standard) and associated guidance, brand, governance structures, training programs, accreditation programs, verification system and conformity assessment program and associated intellectual property.

AWS STANDARD NORMATIVE DOCUMENTS

The AWS Standard System is rooted in four normative documents which comprise the AWS Standard Framework. The scope and interrelationship of these normative documents is shown in Table 1.

[1] The ISEAL Alliance – www.isealalliance.org

TABLE 1. INTERRELATION OF THE FOUR NORMATIVE DOCUMENTS OF THE AWS STANDARD SYSTEM

NORMATIVE DOCUMENT	PURPOSE	AWS LEAD DEPARTMENT	PRIMARY TARGET AUDIENCE
1.AWS Standard v2.0	Defines the Criteria and Indicators for conformance. Supporting the AWS Standard are two other non-normative documents, the General Guidance, and the Scoring Rubric (defining Gold and Platinum level certifications).	Standards and Assurance	Implementers CABs Organizations interested in promoting good water stewardship
2.AWS Certification Requirements	Sets the process for certification to the AWS Standard	Standards and Assurance	CABs Sites seeking information about, or preparing for, Certification
3. AWS Accreditation Requirements	Sets the criteria and the process for accreditation of service providers	Standards and Assurance	Professionally Credentialed individuals CABs Trainers Consultants
4. AWS Professional Credentialing Program Handbook	Describes the training, competency, fee structure, and recordkeeping requirements for those wishing to be AWS professionally credentialed. This status applies at a minimum to individuals working for AWS accredited Service Providers.	Standards and Assurance	Professionally Credentialed individuals, AWS Service Providers, and others seeking to be credentialed

SCOPE

The requirements presented in this document, the *AWS Certification Requirements*, apply to all conformity assessment bodies (CABs) that engage in the provision of conformity assessment services in relation to *The AWS International Water Stewardship Standard v2.0* to sites seeking AWS Certification.

NORMATIVE REFERENCES

AWS Accreditation Requirements: Requirements for Conformity Assessment Bodies, Training Service Providers, and Consultants. Version December 2019

The AWS International Water Stewardship Standard, Version 2.0, March 2019

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

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

AWS Claims Policy and Procedure, Version 1.1 July 2018

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

TERMS AND DEFINITIONS

Relevant Definitions are as noted in Part 3 of ISO 17011:2017.

GENERAL REQUIREMENTS

There are no additional general requirements for CABs beyond those given in *AWS Accreditation Requirements* and ISO 17065:2012.

1 PRE-ASSESSMENT

1.1 Pre-assessment is optional and can be useful to facilitate the implementation process leading to successful certification. AWS does not require clients to have a pre-assessment undertaken. In the event a CAB is retained to do a pre-assessment, they must ensure they do not compromise the required objectivity and avoidance of conflict of interest if they wish to also provide conformity assessment process to the same client and site.

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, and hence is not a conflict as defined in the Accreditation Requirements (2019). However, the individual who leads the pre-assessment cannot also be the lead auditor for the conformity assessment audit. Additionally, the CAB is encouraged to minimize overlap of individuals when performing both pre-assessment and certification audit functions.

2 CONFORMITY ASSESSMENT

2.1 INITIAL ARRANGEMENTS AND CERTIFICATION AGREEMENT

2.1.1 Note: A pre-assessment is not a prerequisite for conformity assessment.

2.1.2 Conformity assessments shall only be performed by CABs holding valid AWS accreditation or applicant CABs which have received prior approval from AWS to initiate such conformity assessments.

2.1.3 CABs shall enter into a certification agreement with the client seeking certification and the costs agreed between both parties. Revenue and fees charged by the CAB to the client seeking certification will be determined directly by the CAB at their discretion.

2.1.3.1 The portion of the fee charged by the CAB and paid back to AWS, such as fees for use of the AWS Mark and fees for on-product claims, shall be clearly stipulated into the cost structure proposed to the client.

2.1.4 Prior to entering into a certification agreement, the CAB shall confirm with the client the scope of the proposed assessment. The client and site to be certified may be one in the same. However, the client is the entity entering into the certification arrangement with the CAB, and the site (or multiple sites or groups) is where the certificate will be applied.

2.1.4.1 The CAB shall verify that the proposed scope of conformity assessment falls within the CAB's scope of AWS accreditation (i.e., for region and sector, as applicable).

2.1.4.2 The CAB shall require the applicant to disclose in the signed certification agreement any prior involvement with AWS service providers. This disclosure shall include pre-assessment if applicable.

2.1.5 CABs shall inform their clients about the *AWS Comments, Complaints and Appeals Procedure* prior to entering into a certification agreement.

2.1.6 Certification agreements shall be made available to AWS upon request.

2.2 CONFIRMATION OF REGISTRATION

2.2.1 Before proceeding with a conformity assessment, CABs shall contact AWS to confirm that the client has registered with AWS their intent to pursue certification of the proposed site(s) or group and identify the AWS Credentialed Professional who assisted the site with AWS Standard implementation, if any.

2.2.2 At this stage, the CAB shall also communicate with AWS in order to:

2.2.2.1 determine if the client has had any previous AWS certificates suspended or withdrawn within the past two (2) years;

2.2.2.2 verify that the client has not previously received AWS certification for the proposed site(s); and

2.2.2.3 obtain the AWS Reference Number given to the site at registration and to be used for the conformity assessment (see Box 1).

2.2.3 The CAB shall record the AWS Reference Number and include this identifier in certification documents relating to the client (i.e., assessment report, certificate, surveillance report).

BOX 1. AWS REFERENCE NUMBER

AWS assigns a unique AWS Reference Number when a client registers for an assessment as soon as possible. This number is used to track assessments within each catchment over time. AWS Reference Numbers are unique to each site and are autogenerated by the Salesforce system used at AWS. They have the following format: AWS-000001

2.3 AUDIT TEAM

2.3.1 The CAB shall assemble an audit team which, at a minimum, fulfils AWS criteria for qualifications and competencies (Appendix 1).

2.3.1.1 CABs shall retain documentary evidence (i.e. records) to show that each audit team fulfils the criteria given in Appendix 1.

2.3.2 The CAB shall appoint a 'lead AWS auditor' to each audit team.

2.3.3 The CAB shall appoint a 'local AWS auditor' to each audit team.

2.3.3.1 In circumstances where the person appointed as lead AWS auditor is also qualified to function as the local AWS Auditor, the CAB may consider assigning the same person to perform both roles provided that doing so would not compromise the qualifications of the audit team or comprehensiveness of the assessment.

2.3.4 CAB shall assign additional members to the audit team, including technical experts, to assess any specific risk factor(s) and areas of greatest relevance, which is presented by the site and/or the organization under assessment.

2.3.5 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.

2.3.6 Audit Preparation

It is understood that part of the audit may done offsite, such as some document review. In advance of the audit, the lead auditor shall:

2.3.6.1 provide the client with a list of information and other materials which shall be prepared prior to the on-site audit;

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

2.3.6.3 arrange and agree the audit dates with the client;

2.3.6.4 send an audit agenda to the client; and

2.3.6.5 confirm if the audit team will need a translator while on site (e.g., to conduct stakeholder meetings).

2.3.7 Where translators are employed, the translators should be independent of the client under assessment.

2.3.7.1 If the CAB is unable to procure a translator who is independent of the client (e.g., due to logistical difficulties), the CAB shall record the name and affiliation of the translator and justify his or her use in the audit report.

2.3.8 The lead auditor shall provide the client with an estimation of the duration and cost of the site visit.

2.3.9 Prior to going on site, the audit team should complete a document review of information submitted by the client, including as applicable:

2.3.9.1 supplementary materials submitted by the client at the time of or subsequent to application to the CAB for AWS certification;

2.3.9.2 pre-assessment reports or results from pre-assessment work,

2.3.9.3 Any existing self-verification reports (from prior to the discontinuation of the Self Verification option in 2019) or results from internal assessment work, and

2.3.9.4 other relevant information that has been made available to the audit team (e.g., stakeholder submissions).

2.3.10 Where a client has previously undergone a pre-assessment, the audit team may consider those results but shall not be bound by them.

2.3.11 Where a client has previously conducted a self-verification assessment (from prior to the discontinuation of the Self Verification option in 2019), the audit team may consider those results but shall not be bound by them.

2.4 STAKEHOLDER ANNOUNCEMENT

2.4.1 At least thirty (30) days before the on-site audit, the CAB shall release a stakeholder announcement which states the client's intention to pursue AWS certification.

2.4.2 The stakeholder announcement shall be released in at least three outlets. Any circumstances precluding this, a justification must be provided by the CAB, and the CAB is to seek approval from AWS:

2.4.2.1 made available online (e.g., published on the client or CAB's website);

2.4.2.2 submitted to AWS for publication on the AWS website; and

2.4.2.3 published in a local media outlet, if applicable, economical, practical, and available, that is appropriate for the client and the related stakeholders (e.g., local newspaper, radio or websites).

2.4.3 The stakeholder announcement shall invite stakeholders to meet with audit team, or to submit written submissions if preferred.

2.4.4 The audit team shall inform stakeholders that oral and written submissions made in reference to the client's operation should be supported by objective evidence wherever possible.

2.4.5 At a minimum, the stakeholder announcement shall specify:

2.4.5.1 name of the client; site location(s)

2.4.5.2 name of the CAB;

2.4.5.3 name and contact details for the lead AWS auditor

2.4.5.4 date(s) and location(s) of the on-site audit; and

2.4.5.5 a brief outline of the process that stakeholders should follow in order to arrange to meet with the audit team and/or to submit written comments to the audit team.

2.5 CONDUCTING THE AUDIT

The audit team shall fully assess the conformity of the client with each indicator 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 Note that all indicators* are applicable to all clients, and the audit team shall not give a response of “not applicable (NA)” to any indicator.

2.5.2 As part of the audit, the audit team shall conduct interviews with representative stakeholders or stakeholder groups to assess conformity of the client with relevant indicators of the AWS Standard.

2.5.2.1 Interviews shall be conducted with persons or groups representing:

2.5.2.1.1 the catchment authority;

2.5.2.1.2 contract suppliers to the site; and

2.5.2.1.3 other identified stakeholders from within the catchment area.

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

2.5.4 The audit team shall assess: (and where needed and possible, visit):

2.5.4.1 a representative sample of source water locations[2]; and

2.5.4.2 a representative sample of water discharge locations[3] used by the client.

2.5.5 The audit team shall record objective evidence of compliance during the assessment. Audit checklists, prepared against the AWS Standard, may be used.

2.6 GRADING OF AUDIT FINDINGS

2.6.1 Audit findings shall be assigned (or ‘graded’) into one of four categories: conforms, major non-conformity, minor non-conformity, and observation.

2.6.2 Non-conformities, major or minor, shall be raised at indicator level only, with the exception of an audit team raising multiple minor non-conformities to indicators under the same criteria during the same audit. In this exception, the audit team is allowed to raise a Major Non-conformity at Criteria level.

2.6.3 Grading of non-conformities shall be based on the audit team’s evaluation of the seriousness of the issue according to the criteria given below (sections 2.7 and 2.8).

2.6.4 For advanced-level indicators, audit teams shall grade all audit findings as either conforms or as observations only.

[2] Definitions and guidance on terminology such as source water areas or discharge locations may be found in the AWS Standard (version 2.0).

[3] Definitions and guidance on terminology such as source water areas or discharge locations may be found in the AWS Standard (version 2.0).

2.6.4.1 Note: Observations are defined as an area of concern regarding a process, document, or activity where there is opportunity for improvement.

2.6.4.2 Failure to meet an advanced-level indicator represents an opportunity for improvement rather than a non-conformity with the AWS Standard. However not meeting an Advanced Indicator means no points are assigned.

2.6.5 For core indicators, audit teams shall grade audit findings using all four categories.

2.7 MAJOR NON-CONFORMITIES

2.7.1 Where the audit team determines that the client does not conform with a core indicator, the audit team shall raise a non-conformity.

2.7.2 The audit team shall grade the audit finding as a major non-conformity if:

2.7.2.1 the issue represents a systematic problem of substantial consequence;

2.7.2.2 the issue is a known and recurring problem that the client has failed to resolve;

2.7.2.3 the issue fundamentally undermines the intent of the AWS Standard; or

2.7.2.4 the nature of the problem may jeopardize the credibility of AWS.

2.7.3 For each major non-conformity identified, the CAB shall require the client to provide a corrective action plan which includes:

2.7.3.1 an analysis of the root cause of the major non-conformity; and

2.7.3.2 the specific corrective action(s) to address the major non-conformity

2.7.4 For applicants, the CAB shall require that all major non-conformities are satisfactorily addressed prior to certification being granted.

2.7.4.1 If an applicant does not address major non-conformities within ninety (90) days of the report being approved by the CAB's internal process (As per the AWS Accreditation Requirements) and the client is notified accordingly, another conformity assessment shall be required.

2.7.5 For certificate holders, the CAB shall require that all major non-conformities are satisfactorily addressed by the client within ninety (90) days of the report being approved by the CAB's internal process (As per the AWS Accreditation Requirements) and the client is notified accordingly.

2.7.5.1 If a major non-conformity is not addressed by a certificate holder within this period of 90 days of the report being approved by the CAB's internal process (As per the AWS Accreditation Requirements) and the client notified accordingly, the CAB shall suspend or withdraw the certificate and reinstatement shall not occur before another conformity assessment has been successfully completed.

2.7.5.1.1 Note that no AWS assets (e.g. logos or claims) may be used by any client with a suspended certificate.

2.7.6 The CAB shall review objective evidence for the effectiveness of the client's corrective actions before closing out or downgrading a major non-conformity.

2.8 MINOR NON-CONFORMITIES

2.8.1 Where the audit team has evaluated an audit finding and determines that the seriousness of the issue does not meet any of the criteria outlined in section 2.7.2, the audit team shall grade the finding as a minor non-conformity.

2.8.2 For applicants, the audit team may recommend the client for certification once the client has submitted an acceptable corrective action plan to address all minor non-conformities.

2.8.2.1 The corrective action plan shall include:

2.8.2.1.1 an analysis of the root cause of the minor non-conformity;

2.8.2.1.2 the specific corrective action(s) to address the minor non-conformity; and

2.8.2.1.3 an appropriate timeframe to implement corrective action(s).

2.8.3 For certificate holders, the CAB shall require that minor non-conformities are satisfactorily addressed by the next surveillance audit.

2.8.4 If corrective actions are inadequate to resolve a minor non-conformity, the CAB shall upgrade the audit finding to a major non-conformity.

2.8.5 If an unusually large number of minor non-conformities are detected for indicators falling under the same criterion during the course of a single audit, the audit team may at their discretion raise a major non-conformity at the criterion level to reflect a systematic failure of the client's management system to deliver conformity with the AWS Standard to that criterion.

2.9 ALLOCATION OF POINTS

2.9.1 Where a client has one or more unresolved major non-conformity, the audit team shall not allocate points to any advanced-level indicators.

2.9.2 The audit team shall complete the allocation of points within thirty (30) days of completion of the on-site audit and, in any event, before finalizing the assessment report (section 2.11).

2.9.3 Prior to allocating points, the audit team shall review the assessment results to confirm that the client has met all core indicators.

2.9.3.1 Note: where one or more minor non-conformity has been raised against core indicators, the audit team should consider the adequacy of corrective action plans submitted by the client when applying clause 2.10.3.

2.9.4 Audit teams shall award points in accordance with the indicator-specific point allocation system given in the AWS Standard. Where a range of points is provided for an indicator, the points awarded are at the discretion of the auditor.

2.9.5 Certification level shall be determined based on the total sum of points awarded, in any combination, to all advanced-level indicators.

2.9.6 Thresholds for the three (3) AWS certification levels against the AWS Standard v2.0 are given in Table 2. Note that points thresholds may change as a result of periodic reviews of the AWS Standard. The point ranges are above and beyond the core indicators. In other words, a site would need to achieve at least 40 advanced indicator points in addition to meeting all core indicators before they would be considered AWS Gold Certified.

TABLE 2. THRESHOLDS FOR AWS CERTIFICATION LEVELS.

POINT TOTAL	AWS CERTIFICATION LEVEL
0 to 39	AWS Core Certified
40 to 79	AWS Gold Certified
80 or greater	AWS Platinum Certified

2.10 AUDIT REPORT

2.10.1 The audit team shall prepare a draft audit report within thirty (30) days of completing the on-site audit. The audit report shall be considered as final once it is reviewed and approved by the CABs internal process. However, no certificate can be issued until major non-conformities are resolved in accordance with 2.7. The specific format of the audit report is at the discretion of the CAB, but it must contain the elements in 2.10.2 through 2.10.8.

2.10.2 The audit report shall contain an introductory section which covers the following information:

2.10.2.1 client name and contact details of the person responsible to liaise with AWS;

2.10.2.2 scope of the assessment including all locations and facilities that were visited;

2.10.2.3 a description of the catchment in which the client operates; and

2.10.2.4 a summary of shared water challenges.

2.10.3 The audit report shall contain a section about the audit findings which includes:

2.10.3.1 a checklist or table of all AWS indicators detailing the objective evidence that was reviewed by the audit team for each indicator;

2.10.3.2 a description of all major non-conformities that were raised;

2.10.3.3 a description of all minor non-conformities that were raised; and

2.10.3.4 a description of any observations that were raised, as applicable.

2.10.3.4.1 Note: the CAB shall request that the client responds within an agreed upon time period to all audit findings by providing root cause analyses and corrective actions, and the client’s responses shall be incorporated into the final version of the assessment report.

2.10.4 The audit report shall contain a section summarizing AWS indicators. The section shall present a concise summary of the client’s conformity or non-conformity with:

2.10.4.1 all core indicators; and

2.10.4.2 all advanced-level indicators if the site is seeking a Gold or Platinum level status.

2.10.4.2.1 Note: point values for each advanced-level indicator may be included in the summary.

2.10.5 The audit report shall contain a section summarizing any identified areas of weakness or opportunities for improvement.

2.10.5.1 Note: the audit team shall not make specific recommendations to the client about how to resolve an identified area of weakness. However, the audit team may refer the client to AWS for additional information about programs for capacity-building or training in water stewardship.

2.10.6 The audit report shall specify audit team's overall recommendation to the CAB reviewer(s) whether or not to issue certification and if so, clearly identify the certification level to be awarded (AWS Core, AWS Gold, or AWS Platinum Certified).

2.10.7 The audit team shall recommend a surveillance schedule for the client, including any sampling that is recommended.

2.10.7.1 AWS considers the surveillance audit frequency to be minimum one annual on-site audit. Any longer time period for surveillance frequency must be first approved by AWSW, but at no time will it exceed 18 months.

2.10.8 For re-assessments, in addition to the foregoing reporting requirements, the (re-)assessment report shall also contain a review of non-conformities raised at the previous surveillance audit, including an evaluation of:

2.10.8.1 the current status of each non-conformity;

2.10.8.2 the site's analysis of root cause; and

2.10.8.3 the effectiveness of corrective action(s) taken.

2.11 ADDITIONAL REPORTING

2.11.1 In addition to the audit report, the CAB will prepare a more summarized version called a Certification Report. This document will be posted on the AWS website and should not contain proprietary information as it is available to the public. The Certification Report is intended to provide more transparency into the performance of a certified site(s). The template for these reports is provided by AWS.

2.11.1.1 AWS may also request additional information to support the Monitoring and Evaluation efforts of progress towards the Standard's outcomes, and in accordance with the ISEAL Impacts Code of Practice.

2.11.1.2 The Certification Report template and any additional information requests in accordance with 2.11.1.1 will be posted on the AWS website (a4ws.org) and the Service Providers will be notified.

2.12 CERTIFICATION

2.12.1 The CAB shall retain records to demonstrate that it has reviewed audit documents and has taken the certification decision in accordance with Part 2 of the Accreditation Requirements v 2.0 (December 2019.

2.12.2 AWS will not acknowledge a site as being certified until a Certification Report is submitted to AWS for posting on the AWS website.

2.12.3 A certificate of conformity shall only be awarded when all core indicators have been met to the satisfaction of the CAB.

2.12.3.1 AWS Gold or AWS Platinum certification levels may also be attached to the certificate if:

2.12.3.1.1 the CAB is satisfied that all core indicators have been met; and

2.12.3.1.2 the CAB is satisfied that the total number of points awarded to advanced-level indicators meets the respective threshold for the assigned certification level (section 2.9.6).

2.12.4 AWS certificates shall indicate the following:

2.12.4.1 name and address of client (or certificate holder if for some reason it is not the client or the site (2.11.3.2);

2.12.4.2 name and location of the site (if different from above);

2.12.4.3 catchment and industry sector;

2.12.4.4 name of CAB;

2.12.4.5 version of AWS Standard that was used;

2.12.4.6 date of certificate issuance, period of validity and date of expiry;

2.12.4.7 certificate scope (single site, multi-site, or group operation); and

2.12.4.8 AWS Reference Number.

2.12.5 Certificates shall be valid for a period of three (3) years.

2.12.6 Upon awarding a certificate, the CAB shall inform the client of their eligibility to use specific AWS assets which may include claims about AWS certification and the use of AWS certification logos (see section 7.

3 SURVEILLANCE AND CERTIFICATE MAINTENANCE

3.1 SURVEILLANCE FREQUENCY AND SCOPE

3.1.1 The frequency and scope of surveillance (i.e., frequency and intensity of monitoring) may vary for different types of clients. It is a function of risk factors such as the size, complexity, scope, certification level, industry sector, region and prior audit history of the client.

3.1.2 The following requirement shall apply to the determination of surveillance level:

3.1.2.1 For each certificate issued, the CAB shall conduct monitoring (i.e., surveillance audits) of the certificate holder throughout the lifetime of the certificate in accordance with the frequency as determined using the conditions noted in 2.10.7.1 and 3.1.1.).

3.1.2.2 The audit team shall produce an annual surveillance schedule for the client, including any specific sampling that is recommended.

3.1.2.3 The audit frequency may change if the CAB concludes that more frequent surveillance is necessary to address observed patterns of nonconformance.

3.1.2.4 Surveillance audits shall be conducted preferable onsite, however offsite audits maybe conducted if all of the following apply:

3.1.2.4.1 There are no open major non conformities and any that were closed previously have been verified by at least one onsite surveillance

3.1.2.4.2 There are no active minor non conformities that involve an onsite aspect where the corrective action can only be verified as closed by an onsite visit

3.1.2.4.3 Previous audits have revealed a high level of commitment and robustness for water stewardship and have demonstrated a proven pattern of continual improvement

3.1.2.4.4 At least one surveillance audit within a certificate cycle must be onsite

3.1.2.4.5 There may be other extenuating circumstance (size and complexity of site, access, affordability, or other) that may justify offsite surveillance audits. These will be presented to, and pre-approved by, AWS Standards and Assurance.

3.1.2.4.6 Note: the audit team may use a document review to supplement but not to replace the on-site audit.

3.1.2.5 Surveillance audits shall be performed by an audit team which fulfills the requirements of Appendix 1.

3.1.2.6 Scope of surveillance audits shall meet or exceed the requirements given in section 3.2.

3.2 SCOPE OF SURVEILLANCE AUDITS

3.2.1 Scope of surveillance audits shall include, at a minimum:

3.2.1.1 review and follow-up on all non-conformities raised at the previous audit;

3.2.1.2 evaluation of known areas of weakness (i.e., risk factors);

3.2.1.3 a review of shared water challenges; and

3.2.1.4 additional areas for review at the audit team's discretion such that after the 3-year period of the certificate, all requirements are evaluated at least once.

3.2.2 During each surveillance audit, the audit team shall review, at a minimum, objective evidence for conformity in the following areas:

3.2.2.1 Leadership commitment;

3.2.2.2 Prioritized list of shared water challenges and how these issues are currently being addressed;

3.2.2.3 Implementation of the water stewardship plan and performance disclosure;

3.2.2.4 Documentation demonstrating legal, regulatory and rights compliance;

3.2.2.5 Water balance performance;

3.2.2.6 Water quality performance;

3.2.2.7 Performance against the site's Important Water-Related Areas;

3.2.2.8 Participation in catchment governance;

3.2.2.9 Provision of WASH;

3.2.2.10 Stakeholder commentary on performance; and

3.2.2.11 Transparency of communications relative to water-related legal compliance.

3.3 RE-EVALUATION OF CERTIFICATION LEVEL

3.3.1 CABs shall consider all reasonable requests from clients to re-evaluate the certification level (AWS Core, AWS Gold, or AWS Platinum) which is attached to the client's certificate.

3.3.2 An 'upgrade' of certification level (e.g., from Core to Gold, from Gold to Platinum) is contingent on successful completion of an audit that covers all core indicators and advanced-level indicators implemented by the client.

3.3.3 Because re-evaluation is minimally different from re-assessment, CABs may handle such requests as a re-assessment (i.e., in accordance with the requirements given in section 3.6) provided that the timing of re-assessment would fit within the certification cycle.

3.3.4 Where timing does not allow for a re-assessment approach, the CAB may schedule the re-evaluation to coincide with a surveillance audit.

3.3.4.1 Surveillance audit scope shall be expanded to reflect the new audit objective(s) which shall include assessment of all core indicators and advanced-level indicators selected by the client.

3.3.5 CABs shall not upgrade a client's certification level based exclusively on results from a surveillance audit, i.e. re-evaluation is required for certificate upgrades.

3.3.5.1 Note that the CAB may downgrade a client's certification level based on results from a surveillance audit if there is objective evidence supporting such a determination (e.g. major non-conformities).

3.4 SURVEILLANCE AUDIT REPORT

3.4.1 The audit team shall prepare a draft surveillance audit report within thirty (30) days of completing the audit. The audit report shall be considered as final once it is reviewed and approved by the CABs internal process. The surveillance audit report shall cover, at a minimum, the information specified in section 3.2.

3.4.1.1 Note: the CAB shall request that the client responds promptly to all non-conformities by providing root cause analyses and corrective actions and developing an agreed-upon timeline for resolution.

3.4.2 The surveillance report shall clearly specify the audit team's overall recommendation as to:

3.4.2.1 whether or not the certificate should be maintained (i.e., continuing certification); and

3.4.2.2 if applicable, the certification level (AWS Core, AWS Gold, or AWS Platinum Certified) which should be attached to the certificate.

3.4.3 Where the audit team recommends that the certification level should be different from the level that was determined at the previous assessment, the audit team shall include a section in the surveillance report which justifies the change.

3.4.3.1 A recommendation for an 'upgrade' in certification level (i.e., from Core to Gold; from Gold to Platinum) shall be accompanied by a summary of the objective evidence which led to improved scoring of the relevant advanced-level indicators (note that certificate upgrades resulting from a surveillance audit require a re-evaluation to take place as described in 3.3.5 above).

3.4.3.2 A recommendation for a 'downgrade' in certification level (i.e., from Gold to Core; from Platinum to Gold) shall be accompanied by a summary of:

3.4.3.2.1 observations on those advanced-level indicators which had been met by the client at the previous audit; and

3.4.3.2.2 any major non-conformities that were raised (if applicable).

3.4.4 The audit team shall include the surveillance schedule developed in 3.1.2.2 in the report.

3.5 CERTIFICATE TRANSFER

3.5.1 CABs shall have procedures to handle certificate transfers to other CABs including:

3.5.1.1 the outbound transfer of their own clients to a different CAB; and

3.5.1.2 the inbound transfer of clients from a different CAB.

3.5.2 Note: AWS considers transfer of ownership (i.e. due to mergers or acquisitions) of a certificate to be a contractual matter between CAB and client that should be handled in accordance with the certification agreement.

3.5.3 Should a client opt to change CABs at any point after certification (i.e. transfer of certificate during surveillance) the client shall:

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

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

3.5.3.3 provide the new CAB with a copy of their last assessment report and surveillance report.

3.5.4 Prior to accepting a client transfer, the new CAB shall review all available information regarding previous conformity assessments and surveillance audits.

3.5.5 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 conformity assessments, the client shall authorize the previous CAB to share additional audit history information with the new CAB in order to ensure that all outstanding non-conformities are resolved.

3.5.5.1 Note: The new CAB may determine, after having completed a document review of the information in 3.5.5, that it is necessary to perform a surveillance audit or conformity assessment of the transferring client before issuing a certificate.

3.6 RE-ASSESSMENT

3.6.1 CABs shall conduct a re-assessment of the client before the certificate can be re-issued or the period of validity extended.

3.6.1.1 Note that a re-assessment is a ‘full' conformity assessment.

3.6.2 The process for re-assessment shall follow all steps for conformity assessment as described in Section 2 with the exception of sections 2.1 and 2.2 which are not repeated.

3.6.3 Re-assessment should be completed before the certificate expires (i.e., before the end of the third year of certification) in order to ensure continuity of certification. However, if a major non-conformity is identified during the re-assessment, the renewal is delayed until the issue is resolved and closed.

3.7 SUSPENSION

3.7.1 Should a client fail to resolve non-conformities within required time period, the CAB shall:

3.7.1.1 suspend the certificate;

3.7.1.1.1 Note that no AWS assets (e.g. claims, logos) may be used by any client with a suspended certificate.

3.7.1.2 inform AWS within two (2) working days so that AWS may publish a notice of suspension on the AWS website; and

3.7.1.3 prepare a suspension report and submit it to AWS within five (5) working days.

3.7.1.3.1 The suspension report shall give a rationale for suspension and provide a description of all unresolved non-conformities.

3.7.1.3.2 AWS may publish the suspension report on the AWS website.

3.7.2 Suspended clients shall be given twelve (12) months to address the cause for suspension.

3.7.3 The CAB shall not reinstate a suspended certificate until the client has successfully undergone another conformity assessment.

3.7.4 Note: Clients with suspended certificates will be treated as high-risk sites when determining surveillance level, and they will remain high-risk until the next conformity assessment shows otherwise.

3.7.5 AWS reserves the right to suspend the certificate of any client who violates the spirit and intent of the AWS Standard or who goes directly against AWS's organizational mission.

3.7.5.1 Note: In respect of 3.7.5, clients shall assume responsibility for all sites named on the certificate whose actions may discredit AWS, including the actions of a facility which may be added to the certificate through change of ownership, merger or acquisition.

3.8 TERMINATION

3.8.1 If the client has not resolved the cause of suspension within twelve (12) months, the CAB shall:

3.8.1.1 terminate the certificate;

3.8.1.2 notify the client that they are ineligible to apply for AWS certification for a period of no less than 36 months;

3.8.1.3 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

3.8.1.4 prepare a termination report and submit it to AWS within five (5) working days.

3.8.1.4.1 The termination report shall give a rationale for termination.

3.8.1.4.2 AWS may publish the termination report on the AWS website.

4 AWS CRITERIA FOR SINGLE SITE, MULTI-SITE AND GROUP OPERATIONS

4.1 ELIGIBILITY CRITERIA

4.1.1 A client with sites that occupies more than one catchment may be considered based on how the criteria and indicators would be addressed to account for the multiple catchments.

4.1.1.1 For those clients occupying two catchments, CABs may consider an allowance for the client to use supplemental water resources from a second catchment, or activities that can affect water quality in the catchment or other catchments, provided that inclusion would not undermine the intent of the AWS Standard.

4.1.1.2 Clients may contact a CAB or AWS to discuss how catchment area boundaries might be used to delineate sub-units of the enterprise which are (or may be) eligible for AWS certification when assessed as separate units.

4.1.2 The scope of the proposed certification should be under the control of a single management system in accordance with Part 5.

4.1.3 The scope of the proposed certification should be homogeneous with respect to primary production system, water management, product or service range, and the main market.

4.2 CLASSIFICATION CRITERIA

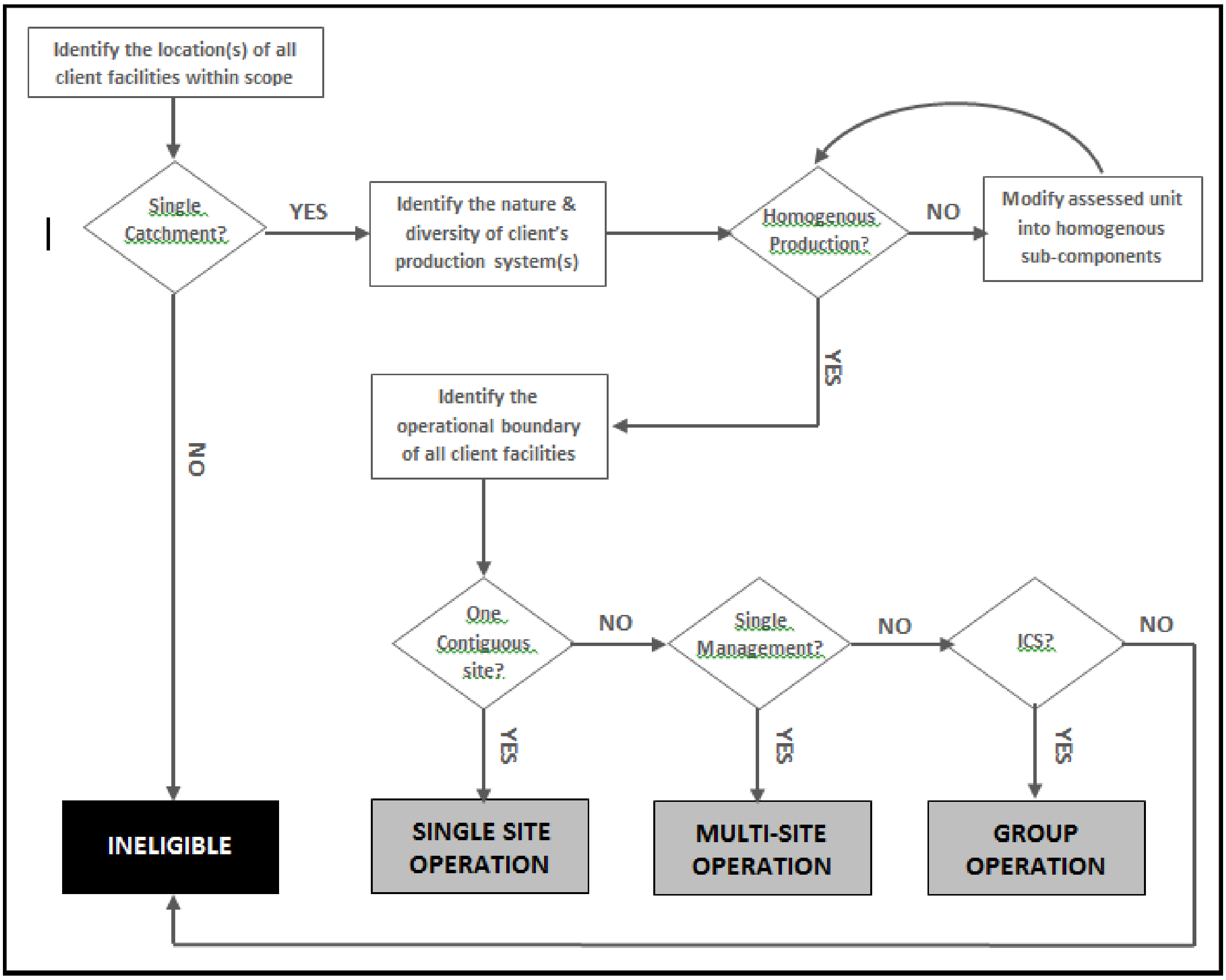
4.2.1 For the purposes of certification, AWS distinguishes three types of operation:

4.2.1.1 single site operation;

4.2.1.2 multi-site operation; and

4.2.1.3 group operation.

4.2.2 Figure 2 summarizes key steps in classifying the scope of the certificate as either a single site operation, a multi-site operation, or a group operation.



Identify the location(s) of all client facilities within scope
Single Catchment?
YES
Identify the nature & diversity of client's production system(s)
Homogenous Production?
NO
Modify assessed unit into homogenous sub-components
YES
Identify the operational boundary of all client facilities
NO
One Contiguous site?
NO
Single Management?
NO
ICS?
NO
YES
YES
YES
INELIGIBLE
SINGLE SITE OPERATION
MULTI-SITE OPERATION
GROUP OPERATION

Figure 2. Decision tree as a guideline for CABs in determining the client's type of operation.

4.2.3 CABs should use the decision tree (Figure 2) and the following section (section 4.3) as a guideline for classifying the client's type of operation.

4.2.4 Where the CAB has good reason to deviate from AWS guidelines for classifying the type of operation of a client, the CAB shall justify that determination in the assessment report.

4.2.5 Clients may direct questions to AWS regarding the application of criteria for single site, multi-site, and group operations.

4.3 CLASSIFICATION OF TYPE OF OPERATION

4.3.1 For the purposes of AWS assessment, the scope proposed for certification should be defined as a single site operation if it meets the following definition:

4.3.1.1 A single location, including the building(s) and the property over which the client has control, which is using or managing water.

4.3.2 Where the scope proposed for certification does not meet the above definition for a single site operation, it should be assessed as either:

4.3.2.1 a multi-site operation; or

4.3.2.2 a group operation.

4.3.3 The CAB should assess the scope proposed for certification as a group operation if:

4.3.3.1 all sites within the proposed group operate an internal control system (ICS);

4.3.3.2 all sites within the proposed group have entered into a Group Member Agreement with management to pursue AWS certification as a group operation;

4.3.3.3 the proposed group has nominated an AWS Group Representative; and

4.3.3.4 the client for certification has requested to be assessed as a group operation.

4.3.3.4.1 Note: the CAB shall ensure that the client understands the applicable AWS group certification requirements (sections 5 and 6) before entering into a certification agreement to assess the scope proposed for certification as a group operation.

4.3.4 In addition to the requirements of the AWS Standard, group operations shall meet the requirements as specified in section 5.

4.3.5 In addition to the requirements of the AWS Standard, CABs shall assess the conformity of group operations against the requirements of section 5 as set forth in section 6.

4.3.6 If the scope proposed for certification does not meet the criteria in 4.3.3 for a group operation, nor the criteria in 4.3.1 for a single site operation, the CAB should assess as a multi-site operation as outlined in section 4.4.

4.4 REQUIREMENTS FOR ASSESSMENT OF MULTI-SITE OPERATIONS

4.4.1 Requirements for conformity assessment and surveillance of multi-site operations are similar to those for single site operations, as specified in sections 2 and 3, respectively, with the following exceptions:

4.4.1.1 The CAB shall require the client to nominate an AWS Group Representative.

4.4.1.2 The CAB shall identify the name and location of each site within the scope proposed for certification and shall assign a unique code to each.

4.4.1.3 For conformity assessment of multi-site operations, the CAB shall conduct an on-site audit at each site.

4.4.1.4 For surveillance of multi-site operations, the CAB shall conduct an on-site audit at each site.

4.4.1.5 CABs may consolidate the results from all site audits into a single assessment report.

4.4.1.6 CABs should issue a single certificate for the multi-site operations.

4.4.1.7 Certificates for a multi-site operation shall incorporate a register of all sites included in the scope of the certificate.

4.4.2 Where a client requests to add a new site to a multi-site certificate, the CAB shall conduct an on-site audit of the site proposed for inclusion before adding that site to the certificate register.

4.4.3 The CAB shall ensure that all AWS claims made by the client are managed through the AWS Group Representative.

4.4.4 Table 3 summarizes some of the similarities and key differences between multi-site certification, single site certification and group certification.

TABLE 3. SOME KEY DIFFERENCES BETWEEN CERTIFICATION OF SINGLE SITE, MULTI-SITE AND GROUP OPERATIONS

	SINGLE SITE CERTIFICATION	MULTI-SITE CERTIFICATION	GROUP CERTIFICATION
NUMBER OF CATCHMENTS	One (exceptions as per 4.1)	One (exceptions as per 4.1)	One (exceptions as per 4.1)
NUMBER OF MANAGEMENT SYSTEMS	One	One	Multiple
PRODUCTION SYSTEM	Homogeneous	Homogeneous	Homogeneous
OWNERSHIP	Single or Multiple	Single or Multiple	Single or Multiple
PHYSICAL ARRANGEMENT OF FACILITIES	Contiguous (1 site)	Discontiguous (> 1 site)	Discontiguous (> 1 site)
AWS GROUP REPRESENTATIV E	No	Yes	Yes
CENTRALIZED GROUP STRUCTURE (E.G. ICS)	No	No (not required)	Yes
INTERNAL AUDITS	No	No (not required)	Yes
EXTERNAL AUDITS (BY THE CAB)	One annual audit	One annual audit at each site	One annual audit at group headquarters; annual audits at a sample of member sites
ASSESSMENT AND SURVEILLANCE REPORTS	One	One report to cover all sites	One report for the group
CERTIFICATES	One	One certificate to cover all sites	One certificate to cover all members

5 REQUIREMENTS FOR GROUP OPERATIONS

5.1 GROUP MANAGEMENT

5.1.1 The management of the group must be clearly defined.

5.1.2 The group shall identify the person with overall management responsibility for the group.

5.1.3 The group shall nominate an 'AWS Group Representative' who assumes overall responsibility for the group's implementation of and compliance with the AWS Standard and AWS certification requirements and serves as the primary contact for AWS communications.

5.1.3.1 Note: the AWS Group Representative may or may not be the person identified in 5.1.2.

5.1.4 Group management shall be responsible for:

5.1.4.1 Establishing a common management framework which explicitly adopts the objective of responsible water stewardship;

5.1.4.2 Ensuring 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;

5.1.4.3 Ensuring that all members within the group operation are in conformity with the AWS Standard;

5.1.4.4 Providing evidence to show that all members within the group operation are in conformity with the AWS Standard;

5.1.4.5 Ensuring that records for all member sites are maintained up to date;

5.1.4.6 Preparing and approving documents, processes and procedures to be used by all sites within the scope;

5.1.4.7 Ensuring that all members have an adequate understanding of the AWS Standard;

5.1.4.8 Carrying out yearly internal audits at all sites within the scope;

5.1.4.9 Following up on non-conformities raised during internal audits; and

5.1.4.10 Following up on non-conformities raised during external audits (i.e. during third-party conformity assessments).

5.2 GROUP INTERNAL CONTROL SYSTEM

5.2.1 The group shall operate an Internal Control System (ICS) which meets the requirements of the AWS Standard and AWS certification requirements.

5.2.2 At a minimum, the ICS shall include or incorporate each of the following:

5.2.2.1 a documented set of procedures covering group processes;

5.2.2.2 a detailed description of how production units are structured;

5.2.2.3 appropriate procedures for maintenance of records;

5.2.2.4 records from internal audits of production units; and

5.2.2.5 a description of the responsibilities of staff of production units and ICS.

5.2.3 In addition to the foregoing, the ICS shall identify the applicable AWS Standard and how non-conformities from internal audits are dealt with according to a set of procedures and sanctions.

5.3 HOMOGENEITY OF GROUP PRODUCTION SYSTEMS

5.3.1 Group members shall be homogeneous regarding their main production systems, their water management, their product or service range, and their main market structures.

5.4 GROUP MEMBERSHIP AGREEMENT

5.4.1 Each group member shall indicate, by way of signature or practical alternative (e.g., in the case of illiterate members), their entry into a contract or agreement with group management to coordinate and pursue AWS certification as a group operation, known as the 'Group Membership Agreement'.

5.4.2 Group management shall make sure that each group member understands the implications of entering into the Group Membership Agreement.

5.4.3 The Group Membership Agreement shall contain at least the following:

5.4.3.1 a commitment by the group member to fulfil the requirements of the AWS Standard and applicable AWS Certification Requirements;

5.4.3.2 a commitment by the group member to provide the group management with required information per the needs of the ICS in a timely manner;

5.4.3.3 acceptance by the group member of internal and external audits;

5.4.3.4 an obligation for the group member to report non-conformities; and

5.4.3.5 the rights of group management to terminate the membership of any member if continued participation by that member threatens the credibility of the group.

5.5 GROUP MEMBER REQUIREMENTS

5.5.1 Group management shall ensure that all members shall have an adequate understanding of the AWS Standard as well as a copy of, or at least access to, the specified requirements determined by the group (Standard and certification requirements). Where appropriate, this can include diagrams or pictures that explain the requirements. Depending on the needs of the group, the document can be an internal standard developed by the group or the (external) AWS Standard in its entirety. The documents such as contracts and internal standards which the group members need to understand shall be written in a way that is adapted to their local language and knowledge.

5.5.2 Records covering the relationship between the group management and group members shall be maintained and kept up to date.

5.5.3 The AWS Group Manager shall keep the following information up to date:

5.5.3.1 Copies of contracts between the group and individual group members;

5.5.3.2 group member list;

5.5.3.3 maps of sites and property areas;

5.5.3.4 internal audit reports;

5.5.3.5 non-conformities (both minor and major), sanctions and follow-up action arising from both internal audits and external audits; and

5.5.3.6 complaints and appeals (to group management, the CAB, or AWS directly).

5.5.4 The internal audits shall be conducted with sufficient scope and detail to provide group management with a robust appraisal of whether or not each group member continues to maintain conformity with the AWS Standard and certification requirements.

5.5.5 Each member of the group shall be internally audited on at least once per year.

5.5.6 New or proposed group members shall always be subject to an internal audit before they may be added to the list of group members (5.3.13).

5.5.7 The AWS Group Representative shall perform an annual review of the status of all members of the group and shall take a decision as to continuing membership of each member. This decision shall be based on internal audits and other information. Safeguards shall be in place to ensure that internal auditors are not unduly influenced in their findings by group management or group members.

5.5.8 Group members should have the right to appeal internal audit findings of non-conformity.

5.5.9 Group management may assume the responsibility of maintaining the operational records on behalf of individual members.

5.5.10 All group members shall be recorded on a list. The list of group members shall be updated annually or more often if necessary and shall include at least the following information for each member:

5.5.10.1 name of the member or code assigned to the member;

5.5.10.2 location

5.5.10.3 the nature (product types) and volume of production (units);

5.5.10.4 volume of water use (inputs and outputs) specify units;

5.5.10.5 Group membership status (including any non-conformities and corrective action plans);

5.5.10.6 date(s) of most recent internal audit;

5.5.10.7 date(s) of most recent external audit; and

5.5.10.8 any other group-specific information as may be needed.

6 CONFORMITY ASSESSMENT OF GROUP CLIENTS

6.1 GENERAL

6.1.1 The CAB shall ensure that the client is informed about the AWS Standard and AWS certification requirements for group operations before entering into a certification agreement.

6.1.2 Where certification of a client group is sought, the CAB shall:

6.1.2.1 perform an assessment of the client group against the AWS Standard and the AWS group certification requirements outlined in section 6;

6.1.2.2 Conduct a risk assessment of the client group to ensure that a representative sample (quantity and type) of group members are assessed;

6.1.2.3 Perform an audit of the group entity (i.e., the central or head office of the group operation); and

6.1.2.4 Audit of a sample of group members to assess the accuracy of the results of the ICS. The audit sample shall conform to AWS sampling requirements (Table 4).

TABLE 4. AWS GROUP SAMPLING REQUIREMENTS

NUMBER OF GROUP MEMBERS	MINIMUM NUMBER OF SITES TO SAMPLE
2-10	2
11-15	3
16-20	4
21-30	6
31-40	8
41-50	10
51+	15

6.1.3 Sites for sampling should be selected at random from the pool of client group members, with the exception of the following:

6.1.3.1 Audit teams may select up to one-third of the sites using targeted sampling.

6.1.3.1.1 Note: When using targeted sampling, auditors should focus on known areas of weakness or non-conformity.

6.1.3.2 The CAB shall use targeted sampling to select at least one group member for audit.

6.1.3.3 Where targeted sampling has been applied, the audit team shall provide an explicit rationale for selection of sites in the assessment report or surveillance report.

6.1.4 The selection of group members for audit should vary from one year to another with at least half of the group members being different from the previous audit.

6.1.5 Where new members have joined the group since the previous audit, CABs shall stratify them separately from the original pool of members at the next audit (i.e., 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.

6.1.6 The audit team shall review the documentation of the ICS to ensure internal audits have been carried out, records are complete and non-conformities are resolved.

6.1.6.1 The major aim of the CAB audit is to evaluate the quality and effectiveness of the internal audits. If internal audits are weak, the whole idea of an internal control system instead of effective external control is at risk.

6.1.6.2 Audit teams shall place a greater emphasis on assessing the effectiveness of the ICS (e.g., by reviewing implementation of policies and procedures at all sites) than would normally be done when assessing a single site enterprise.

6.1.7 CABs shall reserve the right to audit any other findings at their discretion should anomalous information be found by any of the given group members.

6.2 NON-CONFORMITIES IN GROUP OPERATIONS

6.2.1 Non-conforming members within a group operation signify a systemic problem with the group's ICS. AWS requires CABs to take immediate action if a significant number of non-conforming individual group members are found during their assessments.

6.2.2 AWS sets a threshold of 5% for the observed non-conformity rate of members within a group operation, rounded to the nearest whole number. If the thresholds are exceeded (i.e., the number of non-conforming individual members is equal to, or greater than, this number), then it signifies a systemic problem with the group's internal control system (see Table 5).

TABLE 5. EXAMPLES OF THRESHOLD FOR NON-CONFORMITY RATE.

EXAMPLE 1. GROUP OPERATION #1
13 member sites were sampled, and 1 major non-conformity was identified. Non-conformity rate: 1 NC per 13 sites = 7.7% (rounded up to 8%) Observed rate (8%) is greater than threshold (5%) Conclusion: Systemic problem with the group's ICS.
EXAMPLE 2. GROUP OPERATION #2
24 member sites were sampled, and 1 major non-conformity was identified. Non-conformity rate: 1 per 24 sites = 4.2% (rounded down to 4%), Observed rate (4%) is less than threshold (5%) Conclusion: Not a systematic problem with the group's ICS.

6.2.3 If a systemic problem with the ICS is found, the CAB shall raise a major non-conformity against group management.

6.2.4 If the major non-conformity is not addressed by a certificate holder within 30 days, the CAB shall suspend the certificate until such time as:

6.2.4.1 the group has addressed non-conforming individual members;

6.2.4.2 the group manager documents the actions being undertaking to rectify the systemic problem; and

6.2.4.3 the group undergoes a re-assessment that includes a follow up on non-conforming members plus another randomly selected site, based upon the audit team's discretion.

6.2.4.4 Note that no AWS assets may be used by any client with a suspended certificate.

6.3 ASSESSMENT REPORT

6.3.1 The reporting requirements for single sites (section 2.11) shall apply to conformity assessments of group operations.

6.3.2 In addition to single site reporting requirements, group assessment reports shall contain the following information:

6.3.2.1 Name and contact details of the Group Manager responsible to liaise with AWS;

6.3.2.2 A description of the group structure and relationships; and

6.3.2.3 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.

6.3.3 The assessment report for group operations shall also contain:

6.3.3.1 Commentary on the audit team's assessment of the competency and impartiality of the group to maintain conformance with the AWS Standard and AWS group requirements;

6.3.3.2 Commentary on the audit team's perception of the competency of the internal auditors to undertake internal audits as part of a group operation;

6.3.3.3 Commentary on the reliance that can be placed upon the internal auditor's finding of conformance / non-conformance of the group;

6.3.3.4 A comparison of the audit team's findings with the findings made by the group entity, and the reliance that can be placed upon the group entity's findings of conformance / non-conformance;

6.3.3.5 A copy of the sampling plan used with a justification for use;

6.3.3.6 Recommendations for subsequent surveillance audits or training, including any sampling that is recommended.

7 USE OF AWS ASSETS

7.1 GENERAL

7.1.1 AWS assets consist of all trademarks, logos, claims and other intellectual property associated with or developed by AWS, and this shall include the assets described in the AWS Claims Policy and Procedure.

7.1.1.1 AWS may impose a fee for use of the AWS Mark on certificates (for site certifications and on-product claims)

7.1.2 CABs shall review their client's use of AWS assets at all main assessments, surveillance audits, and re-assessments in line with the requirements of the AWS Claims Policy and Procedure.

7.1.3 Continuing certification shall be conditional upon clients demonstrating control over all communications referring to conformance with the AWS Standard and the AWS Assurance System, including the use of all AWS assets. This control must cover:

7.1.3.1 business-to-business correspondence and sales documentation;

7.1.3.2 all use of AWS assets off-product (e.g., in promotional material, annual reports or to media; social media); and

7.1.3.3 all on-product use of AWS Assets, where applicable

7.1.3.4 any approved AWS assets that are developed in the future.

7.1.4 The CAB shall issue non-conformities to their clients should any inconsistencies with these requirements be identified.

APPENDIX 1A. AWS REQUIREMENTS FOR QUALIFICATIONS OF LEAD AWS AUDITORS AND LOCAL AWS AUDITORS.

SUBJECT AREA	A. DEGREE, TRAINING OR CERTIFICATION	B. PREVIOUS EXPERIENCE	REQUIREMENT
Lead AWS Auditor			
Education	Degree in a relevant discipline (e.g., hydrology, environmental engineering, agriculture, forestry, water-related relevant social and economic issues)	Five (5) or more years of experience in the industry sector to be audited	A or B
AWS Standard	AWS water stewardship training course to Specialist level; AWS Professionally Credentialed Specialist Auditor	-	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 (e.g., RSPO, FSC); and - ISO 14001; and/or - an equivalent standard;	A and B
Auditing, AWS-Specific	AWS water stewardship training course to Specialist level;	Team member in at least two (2) AWS conformity assessments or surveillance audits within the last five (5) years.	A and B
CAB Internal Approval	Review, approval and assignment as lead AWS auditor by the AWS Program Manager of the CAB and part of the AWS Professional Credentialing system at Specialist level.	-	A
Local AWS Auditor			
Communication & Stakeholder Facilitation Skills	Training in Social Impact Assessment, SA 8000, or an equivalent program or certification scheme	Three (3) or more years applying stakeholder interview and facilitation techniques	A or B
Language, culture and local water knowledge applicable to the catchment	Fluency in the local language and knowledge of the local culture	One (1) or more year living and working in the region where the catchment is located	A or B

AWS Standard	AWS water stewardship specialist training course; and part of the AWS Professional Credentialing system at Specialist level.	-	A
CAB Internal Approval	Review, approval and assignment as local AWS auditor by the AWS Program Manager of the CAB	-	A

APPENDIX 1B. AWS REQUIREMENTS FOR TECHNICAL EXPERTISE OF THE AUDIT TEAM

TECHNICAL SUBJECT AREA	A. COLLEGE OR UNIVERSITY DEGREE PROGRAM (OR EQUIVALENT) IN ONE OF THE FOLLOWING SUBJECT AREAS:	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 and B
AWS Standard	-	AWS Specialist training course and relevant credentials	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	-	One (1) or more year living and working in the region where the catchment is located	B