ACSSA-200

ISA Security Compliance Institute – Automation and Control System Security Assurance –

Operations and accreditation for conformity assessment bodies

Version 1.2

February 2026

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the SPECIFICATION.

Without limiting the foregoing, ASCI disclaims all liability for harm to persons or property, and users of this SPECIFICATION assume all risks of such harm.

In issuing and making the SPECIFICATION available, ASCI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASCI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this SPECIFICATION should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

To the maximum extent permitted by applicable law, in no event shall ASCI or its suppliers be liable for any special, incidental, punitive, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the SPECIFICATION, the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION, or otherwise under or in connection with any provision of this SPECIFICATION, even in the event of the fault, tort (including negligence), misrepresentation, strict liability, breach of contract of ASCI or any supplier, and even if ASCI or any supplier has been advised of the possibility of such damages.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

Revision history

version	date	changes
1.2	2026.02.08	Initial version available at https://ISASecure.org

Contents

List of ACSSA specific requirements

List of tables

FOREWORD

This is one of a series of documents that defines ISASecure programs that evaluate the conformity of industrial automation and control systems (IACS), to the ISA/IEC 62443 standard. These programs are developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This specification is a document in the series that describes applicable requirements for evaluation of an IACS as deployed for an accountable asset owner, under the ACSSA (Automation and Control System Security Assurance) inspection and certification programs. ISCI also offers programs that evaluate ISA/IEC 62443 conformity for control system products and product suppliers. Further information about ACSSA and all ISASecure conformity assessment programs can be found on the website https://ISASecure.org.

1 Scope

The ISASecure *conformity assessment programs* have been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cybersecurity for *Industrial Automation and Control Systems* (IACS). The ISASecure ACSSA (Automation and Control System Security Assurance) programs evaluate an IACS as deployed for an accountable *asset owner*, for conformity with the ISA/IEC 62443 standards.

There are two ACSSA programs: the ACSSA *inspection* program and the ACSSA *certification* program. See the scheme overview document ACSSA-100 [ACSSA-100] for a detailed comparison of these programs and typical use cases. An organization that performs *evaluations* under the ACSSA inspection program is called an ACSSA *inspection body* (IB). An organization that performs evaluations and grants certifications under the ACSSA certification program is called an ACSSA *certification body* (CB). The term "ACSSA *conformity assessment body*," abbreviated as CAB, is used to refer to both of these types of organizations.

The present document describes how to achieve *accreditation* and operate as an ACSSA IB, CB or both. The document specifies the criteria and processes that define:

- How a CAB is accredited to begin and continue ISASecure ACSSA inspection and certification operations (Sub clause 5.2).
- Requirements on the operations of an ACSSA CAB (Clauses 6 and 7).

Clause 6 provides requirements for CBs and Clause 7 for IBs.

Both ACSSA programs use the same technical evaluation methodology and issue a formal evaluation report. One key difference between the programs is required organization qualifications and ongoing operations requirements for IBs as compared to CBs. These differences are in accordance with the international standards under which these two programs were designed:

- For the inspection program, ISO/IEC 17020, "*Conformity assessment - Requirements for the operation of various types of bodies performing inspection"* [ISO/IEC 17020]
- For the certification program, ISO/IEC 17065, "*Conformity assessment - Requirements for bodies certifying products, processes, and services"* [ISO/IEC 17065].

ISCI has based its program approach on:

- International standards for conformity assessment programs
- ISA/IEC 62443 IACS security standards, specifically 62443-2-1, 62443-2-4, 62443-3-2, and 62443-3-3
- Specifications developed for the ISASecure ACSSA programs.

This document provides a complete reference to these sources, and details ISASecure ACSSA program-specific requirements for conformity to applicable general specifications and standards.

It is anticipated that entities other than CABs will use the ACSSA specifications, such as asset owners, integrators, consultants, and regulators. These entities are not subject to the CAB requirements described in the present specification. However, entities other than CABs may find information in the present document useful as guidance. An example is the description of qualifications for evaluators in 6.4.3.1. Information regarding the purchase and use of ACSSA specifications is found at https://ISASecure.org.

The ISASecure ACSSA program evaluates a deployed IACS, and delivers a report to the asset owner accountable for that IACS. A certificate will be delivered if the IACS *passes* evaluation under the ACSSA

certification program. ISCI also has developed the following certification programs under which a *product* or development process is evaluated and a report delivered to a supplier of IACS *components* or systems:

- For secure product development lifecycle, the ISASecure SDLA program (Security Development Lifecycle Assurance) which evaluates *product supplier* conformity with 62443-4-1 [1] [2]
- For *control system* components, the ISASecure CSA program (Component Security Assurance) and the ISASecure ICSA program (IIoT Component Security Assurance) which evaluate conformity of component products with 62443-4-2 [3] [4], with ICSA exceptions and extensions for the IIoT (Industrial Internet of Things) environment
- For control systems, the ISASecure SSA program (System Security Assurance) which evaluates conformity of system products with 62443-3-3 [IEC 62443-3-3] [ANSI/ISA-62443-3-3].

The separate documents SDLA-200 [5], CSA-200, ICSA-200, and SSA-200 address operations and accreditation topics as they relate to conformity assessment bodies that perform these certifications, respectively. Many requirements for ACSSA CABs found in the present document are identical or parallel to requirements for certification bodies found in these other ISASecure program documents. The Clause 8 Annex in the present document provides a mapping between requirements for a SDLA CB and requirements for an ACSSA CAB. This mapping is intended to assist an entity that has been previously accredited as a certification body for the ISASecure SDLA program, in extending the scope of their existing operating processes to cover accreditation as an ACSSA CAB.

The scheme document ACSSA-100 [ACSSA-100] describes the relationship between ACSSA and other ISA/IEC 62443 certification programs from the perspective of an asset owner.

2 Normative references

2.1 General

NOTE 1 The following is the highest level document that describes the ISASecure ACSSA programs.

[ACSSA-100] *ACSSA-100 ISCI Automation and Control System Security Assurance – ISASecure inspection and certification schemes*, available at https://ISASecure.org

NOTE 2 The following specification lists all document titles and baseline versions that define ACSSA 1.0.0. It is reissued to list any errata or new versions subsequently issued for the baseline documents.

[ACSSA-102] *ACSSA-102 ISCI Automation and Control System Security Assurance – Baseline document versions and errata for ACSSA 1.0.0 specifications,* available at https://ISASecure.org

2.2 Accreditation

NOTE The present document ACSSA-200 falls under this topic category.

[ACSSA-202] *ISCI ISASecure Programs – Application and contract for certification bodies*, internal ISCI document

[ACSSA-212] *ISCI ISASecure Programs – Application and contract for inspection bodies*, internal ISCI document

2.3 ISASecure symbol and certificates

NOTE The following document describes the ISASecure *symbols* and certificates and how they are used within the ISASecure ACSSA programs.

[ACSSA-204] *ACSSA-204 ISCI Automation and Control System Security Assurance – Instructions and policies for use of the ISASecure symbols and certificates*, available at https://ISASecure.org

[ACSSA-205] *ACSSA-205 ISCI Automation and Control System Security Assurance – Certificate Document Format,* available at https://ISASecure.org

2.4 Technical specifications

NOTE 1 This sub clause includes the specifications that define technical criteria for evaluating an asset owner's IACS for ISASecure ACSSA inspection or certification.

NOTE 2 The following document is the overarching technical specification for ISASecure ACSSA evaluation, for inspection or certification.

[ACSSA-300] *ACSSA-300 ISCI Automation and Control System Security Assurance – Inspection and certification requirements, available at* https://ISASecure.org

[ACSSA-303] *ACSSA-303 ISCI Automation and Control System Security Assurance - Sample Report*, *available at* https://ISASecure.org

NOTE 3 The following specification provides the detailed ACSSA technical evaluation methods for a deployed IACS using the ISA/IEC standards 62443-2-1, 62443-2-4, 62443-3-2, and 62443-3-3.

[ACSSA-311] *ACSSA-311 ISCI Automation and Control System Security Assurance – Evaluation methods*, available at https://ISASecure.org

2.5 External references

External references are documents that are used by the ISASecure ACSSA program but maintained outside of the ISASecure program.

2.5.1 IACS security standards

NOTE 1 [ACSSA-300] and [ACSSA-311] describe how ISA/IEC 62443 series standards are used in an ACSSA evaluation.

NOTE 2 The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

[ANSI/ISA-62443-1-1] *ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models*

[IEC 62443-1-1] IEC TS 62443-1-1:2009 *Industrial communication networks – Network and system security - Part 1-1: Terminology, concepts and models*

[ANSI/ISA-62443-2-1] ANSI/ISA 62443-2-1-2024 *Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners*

[IEC 62443-2-1] IEC 62443-2-1:2024 *Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners*

[IEC 62443-2-4] IEC 62443-2-4:2023 *Security for industrial automation and control systems Part 2-4: Security program requirements for IACS service providers*

[ANSI/ISA-62443-3-2] ANSI/ISA-62443-3-2-2020 *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design*

[IEC 62443-3-2] IEC 62443-3-2:2020 *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design*

[ANSI/ISA-62443-3-3] ANSI/ISA−62443−3−3 (99.03.03) - 2013, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

[IEC 62443-3-3] IEC 62443−3−3:2013 *Industrial communication networks - Network and system security Part 3-3: System security requirements and security levels*

2.5.2 International standards for conformity assessment programs

NOTE The following international standards apply to the ISASecure inspection and certification processes.

[ISO/IEC 17020] ISO/IEC 17020, "*Conformity assessment - Requirements for the operation of various types of bodies performing inspection,*" March 1, 2012

[ISO/IEC 17065] ISO/IEC 17065, "*Conformity assessment—requirements for bodies certifying products, processes and services,*" September 15, 2012

2.5.3 International standards for accreditation programs

NOTE The following international standard applies to the ISASecure accreditation process for conformity assessment bodies.

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies,*" November 2017

3 Definitions and abbreviations

3.1 Definitions

For terminology and definitions used in the ACSSA program, see section 3.1 of ACSSA-300 v1.5 [ACSSA-300]. Terms defined in that document are italicized on first use in the text of the present document.

3.2 Abbreviations

The following abbreviations are used in this document.

ACS	automation and control system
ACSSA	Automation and Control System Security Assurance
ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
BS	Bachelor of Science
CAB	conformity assessment body
CACE	Certified Automation Cybersecurity Expert
CACS	Certified Automation Cybersecurity Specialist
CB	certification body
CE	computer engineering
Cert	applies to ACSSA certification program
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CS	computer science
CSA	Component Security Assurance
GICSP	Global Industrial Cyber Security Professional
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
IAF MRA	IAF Multilateral Recognition Arrangement
IB	inspection body
ICSA	IIoT Component Security Assurance
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
ILAC	International Laboratory Accreditation Cooperation
ILAC MRA	ILAC Mutual Recognition Arrangement
Insp	applies to ACSSA inspection program
IRCA	International Register of Certificated Auditors
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISC2	International Information System Security Certification Consortium
ISO	International Organization for Standardization
IT	information technology
PECB	Professional Evaluation and Certification Board
PhD	Doctor of Philosophy
SDL	security development lifecycle
SDLA	Security Development Lifecycle Assurance
SSA	System Security Assurance
TS	technical specification

4 Background

4.1 Technical ISASecure ACSSA certification criteria

An asset owner accountable for an IACS may apply for an evaluation under the ACSSA inspection or certification programs. The IACS for which application is made, must be either in the operation phase of the IACS lifecycle, or near transition to operation. Eligibility criteria are detailed in the specification ACSSA-300 [ACSSA-300].

Whether the asset owner for an IACS elects the ACSSA inspection program or the ACSSA certification program, the IACS will undergo an evaluation to demonstrate conformity to ISA/IEC 62443 standards as follows:

- IACS operations *policies* and *procedures* conformant to 62443-2-1 [IEC 62443-2-1]
- IACS *risk assessment* policies and procedures conformant to 62443-3-2 [IEC 62443-3-2]
- Support from *service providers* for the IACS conformant to 62443-2-4 [IEC 62443-2-4]
- Control system conformant to 62443-3-3 [IEC 62443-3-3].

In order to be eligible for ISASecure ACSSA inspection or certification, an asset owner must maintain their IACS policies and procedures in *security program* documentation under change control.

ACSSA-300 specifies ACSSA evaluation criteria, by reference to the evaluation methods specification ACSSA-311 [ACSSA-311] which describes *validation activities* for each individual ISA/IEC 62443 requirement that is evaluated under ACSSA. Evaluation methods are the same for an ACSSA inspection or an ACSSA certification. ACSSA-300 also describes criteria for granting ACSSA certification, as well as for maintaining that certification over time. Maintenance of ACSSA certification concepts include *surveillance*, expiration of certification, and *recertification*.

The present specification requires that a CAB develop and deliver an evaluation plan to a *client* for an ACSSA inspection or certification (requirement ACSSA.R19). The planning process is described in the evaluation planning specification ACSSA-304 [ACSSA-304]. The form and content for such a plan are provided in the sample evaluation plan ACSSA-305 [ACSSA-305].

4.2 ISASecure ACSSA program implementation

ISCI is organized as an interest area within ASCI (Automation Standards Compliance Institute), a not-for-profit 501 (c) (6) corporation owned by ISA. Descriptions of the governance and organizational structure for ASCI are found on the ISASecure website: https://ISASecure.org.

ASCI ISASecure ACSSA inspection bodies and certification bodies are organizations that are accredited to evaluate an IACS under these ISASecure ACSSA programs. ASCI grants accredited organizations the right to process ISASecure ACSSA applications for accountable asset owners on its behalf. IBs are authorized to issue formal ACSSA inspection reports. CBs are authorized to grant ACSSA certifications and issue ACSSA certification reports and *certificates* when certification criteria are met. Certificate expiration and certificate maintenance are also managed by the CB.

The lists of ASCI ISASecure ACSSA IBs and CBs are posted on the ISCI website at https://ISASecure.org. At the request of an asset owner organization, ISCI will post on its website, the name of the asset owner organization and the information on their ACSSA certificate(s). An asset owner that does not elect that ISCI post this information, may request that ISCI provide the information directly to a specified third party. ISCI will not publish information about IACS and identities of asset owners that have undergone ACSSA evaluation under the ACSSA inspection program.

5 Summary of operations and accreditation requirements

5.1 Overview

ISASecure ACSSA inspection will operate as an internationally recognized inspection program. ISASecure ACSSA certification will operate as an internationally recognized certification program. To meet these standards, IB and CB operations and accreditation requirements are designed to conform to accepted international standards that are applicable, respectively, to inspection and certification programs.

The operations of ISASecure ACSSA IBs SHALL be in conformance with the applicable requirements in ISO/IEC 17020, the international standard that applies to bodies that perform inspections of products, processes, services, or installations.

The operations of ISASecure ACSSA CBs SHALL be in conformance with the applicable requirements in ISO/IEC 17065, the international standard that applies to bodies that certify products, processes or services.

5.2 Accreditation

5.2.1 Inspection body

Accreditation of an inspection body for ACSSA SHALL consist of an *assessment* of the entity against the requirements of ISO/IEC 17020 and ACSSA specific requirements in Clause 7 of the present document.

To be recognized as an inspection body for the ISASecure ACSSA program, an organization SHALL attain the following accreditation, granted by an *accreditation body* that is a signatory to the ILAC Mutual Recognition Arrangement, and based upon such an assessment:

- accredited to ISO/IEC 17020, as either a Type A or C inspection body, with technology scope of accreditation covering ISASecure ACSSA inspection.

5.2.2 Certification body

Accreditation of a certification body for ACSSA SHALL consist of an assessment of the entity against the requirements of ISO/IEC 17065, incorporating ACSSA-specific interpretations of those requirements documented in Clause 6 of the present document, and the requirements in all ACSSA-specific requirement sub clauses in Clause 6.

To be recognized as a certification body for the ISASecure ACSSA program, an organization SHALL attain the following accreditation, granted by an accreditation body that is a signatory to the IAF Multilateral Recognition Arrangement, and based upon such an assessment:

- accredited to ISO/IEC 17065, with technology scope of accreditation covering ISASecure ACSSA certification.

If an ACSSA certification body is also accredited as an ACSSA inspection body, they SHALL BE accredited as a Type A inspection body.

5.2.3 Accreditation process for IB or CB

A candidate entity applies directly to an ACSSA accreditation body for ACSSA IB and/or CB accreditation. The candidate entity will also apply to ASCI for IB and/or CB status, using the application/contract ISASecure-202 [ISASecure-202]. ASCI recognition of IB or CB status is based on a successful assessment result by the accreditation body, and the ISASecure-202 formal agreement with ASCI.

The accreditation body process to accredit an IB or CB consists of two steps. In the first step, an assessor who is qualified with respect to the relevant accreditation will complete an assessment of all accreditation requirements. At this point the accreditation body has not yet formally granted accreditation, which requires as a second step, a review and approval process internal to the accreditation body.

An organization can be accredited as both an IB and a CB. A CB that intends to also be an IB is not "automatically" accredited as an IB, but must have both ISO/IEC 17020 and ISO/IEC 17065 accreditations as listed above. It is intended by design of the ACSSA specifications that an entity that achieves accreditation as an ACSSA CB, will have met requirements for an ACSSA IB. However formal accreditations to both ISO/IEC 17020 (Type A) and ISO/IEC 17065, and ongoing surveillance by the accreditation body of both inspection and certification activities of such an accredited entity, are required for an entity to be both an IB and a CB.

NOTE See 6.4.3.2 for specific ISO/IEC 17020 requirements which have been incorporated as requirements for an ACSSA CB, as well as for an IB.

5.2.4 Provisional conformity assessment body status

As an option during the time period after the accreditation body assessment, and before the accreditation body performs its final review and grants accreditation, the candidate CAB may request that ASCI grant it a temporary *provisional CAB status*. This will be granted if in ISCI's judgement, the accreditation body assessor's report shows that the entity applying for ACSSA IB and/or CB accreditation meets the requirements for formal accreditation defined above, and the formal agreement between the entity and ASCI has been signed. Once an organization has attained provisional CAB status, ASCI grants that organization the right to perform ACSSA evaluations, deliver formal ACSSA evaluation reports and grant ISASecure ACSSA certifications (for CBs). These rights continue as long as the entity receives formal accreditation from an ACSSA accreditation body in a timely manner (the second step), and maintains this status. An internationally recognized accreditation SHALL be obtained by the entity within 18 months of obtaining provisional CAB status.

NOTE Provisional CAB status is typically requested if a delay is anticipated before the accreditation body can perform its final review, for example, due to scheduling issues.

"Provisional certification body" or "provisional inspection body" are terms applied by ASCI/ISCI within the ISASecure program and are not recognized or managed by the accreditation body.

During the period when a CAB is operating in provisional status, ASCI SHALL be made aware of the organization's expectations for receipt of formal internationally recognized accreditation. ASCI SHALL have the option to perform an interim review and update its evaluation for provisional status of the CAB, 6 months after it is received. Once an organization has achieved accreditation by a qualified accreditation body, that accreditation body determines the requirements and frequency for maintenance audits for the CAB to maintain accredited status.

6 Requirements on operations of certification bodies

6.1 Overview

This clause covers scheme-specific ACSSA operation and accreditation requirements for certification bodies. These include scheme references relevant for those ISO/IEC 17065 requirements that explicitly call out possible scheme-specific requirements. The clause is organized using the outline of ISO/IEC 17065. Where required, it interprets requirements in that document for ISASecure ACSSA and adds additional requirements. Of particular note are requirements for:

- publication of certification status (6.2.2);
- organizational and financial affiliations of CABs (6.3.3);
- qualifications for evaluators (6.4.3.1);
- directory listing of certified organizations (6.5.3.3);
- appeals for client complaints (6.5.3.7); and
- managing complaints to certified organizations (6.6.3.6).

This clause provides specific interpretations for ISO/IEC 17065 requirements. It defines further requirements for CBs that are specific to the ISASecure ACSSA certification program.

Requirement titles for requirements unique to ACSSA include for convenience the notations *Insp* or *Cert* or both, to indicate whether a requirement on CBs listed in this clause is also applicable for IBs. Clause 7 provides the full list of requirements applicable to IBs.

Clause 6 is organized as follows:

- The sub clauses at numbering level 2 (6.2, 6.3, 6.4, 6.5, 6.6) each correspond to a clause in ISO/IEC 17065, covering in turn clauses 4-8 in that document.
- Each of these sub clauses in the present document has three further sub clauses as follows:
    - *Overview* - provides a list of the topics covered in the corresponding clause of ISO/IEC 17065
    - *Scheme references for standard requirements* - A number of ISO/IEC 17065 requirements provide the option for the scheme owner to require conformity with unique requirements specified by their *certification scheme*. This sub clause in the present document provides a table that lists each such ISO/IEC 17065 requirement and provides references, if any, to documentation for the ISASecure ACSSA certification scheme where the unique scheme requirements are found. These references may refer to ISASecure ACSSA scheme documents that are listed in Clause 2 of the present document, or may refer to the present document itself, in particular to requirements in the sub clauses in the present document described next.
    - *ISASecure ACSSA specific requirements* - This sub clause lists additional scheme specific requirements, beyond those derived directly from ISO/IEC 17065 together with the other documents of the ISASecure ACSSA certification scheme.

6.2 General requirements

6.2.1 Overview

Clause 4 *General requirements* in ISO/IEC 17065 covers the following topics in associated sub clauses of that document:

- Legal and contractual matters (4.1)
- Management of *impartiality* (4.2)
- Liability and financing (4.3)
- Non-discriminatory conditions (4.4)
- Confidentiality (4.5)
- Publicly available information (4.6).

6.2.2 Scheme references for standard requirements

The following table provides ACSSA scheme references, for ISO/IEC 17065 requirements in Clause 4 of that document that refer to certification scheme requirements.

Table 1. Scheme references for ISO/IEC 17065 Clause 4

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ACSSA reference
4.1.2 *Certification agreement*	4.1.2.2 h	Certification scheme requirements regarding client references to their certification	Requirement ISASecure_ACS.R5 in [ACSSA-300], and [ACSSA-204]
4.1.2 *Certification agreement*	4.1.2.2 f, g	Certification scheme requirements on actions taken by a client upon loss of certification, and on reproduction of certification documents	No unique requirements specified by scheme
4.1.2 *Certification agreement*	4.1.2.2 j	Certification scheme requirements on certification body to verify tracking of complaints received by client	[ACSSA-200] ACSSA.R46
4.1.3 *Use of license, certificates and marks of conformity*	4.1.3.1	Control by the certification body, as specified by the certification scheme, of mechanisms for indicating an entity is certified	Requirements on mechanisms are in [ACSSA-204]
4.2 *Management of impartiality*	4.2.10	Period of time between performing *consultancy* and certification services	[ACSSA-200] Requirement ACSSA.R4
4.6 *Publicly available information*	4.6 c)	Certification scheme requirements regarding client references to their certification	[ACSSA-300] requirement ISASecure_ACS.R5 in 4.1, and [ACSSA-204]
4.6 *Publicly available information*	4.6 a)	Certification scheme requirements related to granting certification	[ACSSA-300]

6.2.3 ISASecure ACSSA specific requirements

This sub clause lists additional scheme specific requirements related to Clause 4 *General requirements* in ISO/IEC 17065, beyond those derived from ISO/IEC 17065 together with the other documents of the ISASecure ACSSA certification scheme.

Requirement ACSSA.R1 – Confidentiality for ASCI and ISCI (Insp, Cert)
ASCI and ISCI SHALL NOT have access to information generated during ISASecure evaluations, except by permission of the *applicant*, or as required to fulfill ISCI's oversight role as scheme owner.

Requirement ACSSA.R2 – Handling of inspection and certification data (Insp, Cert)
Procedures for document distribution internal to the CAB SHALL limit copies of an inspection or certification report or *certification scoping detail* only to those that the CAB determines need the information to fulfill their work responsibilities. Procedures for external distribution SHALL require that any external disclosure of an ACSSA certificate, certification scoping detail, or inspection or certification report be approved by the asset owner, other than as required to ISCI under requirements ACSSA.R26 and ACSSA.R48. If approved by the asset owner, a CAB MAY publish in a public venue a certificate or an inspection report cover letter. The asset owner MAY request that the CAB provide this information directly to a specified third party. The legal ACSSA agreement between the CAB and the client SHALL require the CAB to carry out confidentiality procedures for all data disclosed to the CAB under the program, as agreed in the client evaluation plan to be approved per requirement ACSSA.R19.

Requirement ACSSA.R3 – Public availability of ISCI complaint escalation process (Insp, Cert)
The ISO/IEC 17065 requirement 4.6 d) in the sub clause 4.6 *Publicly available information* refers to procedures for handling complaints and appeals. Likewise, ISO/IEC 17020 in 7.5.2 requires an IB to make available such a description upon request. This information SHALL include the information about complaints to ASCI/ISCI in clause 6.5.3.7 of this document.

Requirement ACSSA.R4 – Time delay from provision of consultancy (Cert)
The ISO/IEC 17065 requirement 4.2.10 refers to the period of time between personnel having provided consultancy for an IACS and reviewing or making a certification decision. The minimum time period SHALL be two years.

NOTE The definition for consultancy in ACSSA-300 is “participation in the designing, implementing, operating or maintaining of a certified entity or an entity to be the subject of conformity assessment.”

Requirement ACSSA.R5 – Client facility access (Insp, Cert)
Appropriate contracts, covenants, or agreements SHALL include provision(s) for access to the client's IACS facility, in accordance with the client's standard visit procedures.

6.3 Structural requirements

6.3.1 Overview

Clause 5 *Structural requirements* in ISO/IEC 17065 covers the following topics in associated sub clauses of that document:

- Organizational structure and top management (5.1)
- Mechanism for safeguarding impartiality (5.2).

6.3.2 Scheme references for standard requirements

The following table provides ACSSA scheme references, for ISO/IEC 17065 requirements in Clause 5 of that document that refer to certification scheme requirements.

Table 2. Scheme references for ISO/IEC 17065 Clause 5

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ACSSA reference
5.2 *Mechanism for safeguarding impartiality*	5.2.1 (Notes 2 and 3)	Certification scheme owner participation in mechanism for impartiality	No unique requirements specified by scheme
5.2 *Mechanism for safeguarding impartiality*	5.2.4 (Note 2)	Certification scheme requirements on interests represented by mechanism for safeguarding impartiality	No unique requirements specified by scheme

6.3.3 ISASecure ACSSA specific requirements

This sub clause lists additional scheme specific requirements related to Clause 5 *Structural requirements* in ISO/IEC 17065, beyond those derived from ISO/IEC 17065 together with the other documents of the ISASecure ACSSA certification scheme.

Additional requirements on financial and other organizational affiliations of CABs are defined as follows, to further safeguard impartiality.

Requirement ACSSA.R6 – Organizational affiliations (Insp, Cert)

When a legal entity is a *major client* of an applicant for ACSSA, personnel from this entity SHALL NOT be involved in management of a CAB concerned with this application. For a CAB that is a CB, such personnel SHALL NOT be involved in certification review or certification decisions for this certification applicant.

NOTE ISO/IEC 17065 4.2.8 addresses the case of personnel from a legal entity that produces a product to be certified or provides consultancy. This requirement adds the case of a legal entity that is a major client of the organization to be inspected or certified.

Requirement ACSSA.R7 – Financial affiliations (Insp, Cert)

The following requirements apply to a CAB regarding its financial affiliations with clients or with major users of products produced by clients.

- A CAB or a *major owner* of the CAB SHALL NOT:
    - provide *significant financing* to a client asset owner or to a *major user* of such an asset owner's products;
    - be a major owner of a client asset owner or of a major user of such an asset owner's products;
- A CAB SHALL NOT:

- receive significant financing from a client asset owner or from a major user of such an asset owner's products, or their major owners;

- have as a major owner, an organization that is a client asset owner or a major user of such an asset owner's products, or a major owner of such an organization;

- A person involved in the management of the CAB SHALL NOT have a *significant financial interest* in a client asset owner or major user of such an asset owner's products. For a CAB that is a CB, such a person SHALL not be involved in the certification review or certification decision for such an asset owner.

Requirement ACSSA.R8 – CAB sales and purchases (Insp, Cert)

The following requirements apply to IBs and CBs as stated, regarding sales and purchase activities:

- A CB, Type A IB, or any part of the same legal entity, SHALL NOT have *significant sales* of any products or services to client asset owners, other than inspection or certification services. This includes but is not limited to consulting, design, implementation, integration, operation or maintenance for elements of the IACS to be evaluated under ACSSA, or for a similar IACS for the same client (noting this condition does not apply for TYPE C IBs);

- For any CB or IB (Type A or Type C), a person who participates in or benefits from sales of products or services to a client of this CAB other than inspection or certification services, regardless of the legal entity making such sales, cannot participate in client application, evaluation, certification review, or the certification decision under the ACSSA programs for a period of two years. In particular, a person involved in sales, consulting, design, implementation, integration, operation or maintenance for elements of the IACS to be evaluated, or for a similar IACS for the same client, cannot participate in client application to, or evaluation under, the ACSSA inspection program for two years;

- A CB, IB, or any part of the same legal entity, SHALL NOT sell products produced by client asset owners;

- Prices and agreements related to any products or services that a CB, IB or any part of the same legal entity purchases from a client asset owner SHALL NOT have dependencies on related inspection or certification activity.

6.4 Resource requirements

6.4.1 Overview

Clause 6 *Resource requirements* in ISO/IEC 17065 covers the following topics in associated sub clauses of that document:

- Certification body personnel (6.1)

- Resources for evaluation (6.2)

6.4.2 Scheme references for standard requirements

The following table provides scheme references, for ISO/IEC 17065 requirements in Clause 6 of that document that refer to certification scheme requirements.

Table 3. Scheme references for ISO/IEC 17065 Clause 6

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ACSSA reference
6.1 *Personnel*	6.1.1.3	Certification scheme requirements to release information created during an evaluation	[ACSSA-200] requirements ACSSA.R1 and ACSSA.R2
6.1.2 *Management of competence for personnel involved in the certification process*	6.1.2.1 a	Certification scheme requirements for competency of personnel involved in certification	[ACSSA-200] sub clause 6.4.3.1
6.1.2 *Management of competence for personnel involved in the certification process*	6.1.2.1 b	Certification scheme requirements for training of personnel involved in certification	[ACSSA-200] sub clause 6.4.3.1
6.2.1 *Internal resources* 6.2.2 *External resources*	6.2.1, 6.2.2.1	Applicable requirements from other standards	[ACSSA-200] sub clause 6.4.3.2

6.4.3 ISASecure ACSSA specific requirements

This sub clause lists additional scheme specific requirements related to Clause 6 *Resource requirements* in ISO/IEC 17065, beyond those derived from ISO/IEC 17065 together with the other documents of the ISASecure ACSSA certification scheme.

6.4.3.1 Personnel qualifications

Requirement ACSSA.R9 – Evaluator minimum qualifications (Insp, Cert)

The ISO/IEC 17065 requirement 6.1.2.1 a) in the sub clause 6.1.1 *Management of competence for personnel involved in the certification process* refers to competencies of personnel involved in the certification process. Likewise ISO/IEC 17020 in sub clause 6.1.3 refers to appropriate qualifications, training, experience, and a satisfactory knowledge of the requirements of the inspections to be carried out The minimum qualifications for personnel that are responsible for evaluation of an IACS to ACSSA requirements under the ACSSA inspection or certification program SHALL include those specified in Table 4.

The minimum level of knowledge required for ISA/IEC 62443 as indicated in the last row of Table 4, MAY be demonstrated by passing the examinations for ISA course offerings on ISA/IEC 62443 numbered IC32, IC33, IC34, and IC37, or by holding a valid “ISA/IEC 62443 Cybersecurity Expert certificate” issued by ISA. A CAB MAY also determine that a candidate evaluator has adequate knowledge based upon an evaluation of the candidate’s experience using the standard.

The minimum level of knowledge required for ISO/IEC 27001, SHALL be sufficient for the individual to prepare and present a one hour overview on the scope of application and contents of the standard, and be capable of

quickly finding the answers to questions about what the standard requires on a particular topic, if given access to the text of the standard.

Table 4. ACSSA evaluator qualifications

Category of qualification / experience	Baseline evaluator qualifications	Unique qualifications for evaluator roles
ACSSA training program	• Successful completion and maintenance of training certificate under ISCI approved ACSSA training program	• None
Formal education	• BS Electrical Engineering **OR** • BS Computer Engineering (CE) **OR** • BS Computer Science (CS) **OR** • BS Chemical Engineering with CE or CS minor **OR** • BS Cybersecurity or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR** • Equivalent science or engineering degree **OR** • Bachelor's or equivalent level degree in other subject, if individual has sufficient experience in computer technology field as specified below **OR** • Degree as described above, higher than BS **OR** • Otherwise, exceed minimum criterion stated below. Specifically, where a minimum of four or six years experience is specified under "Relevant work experience in ACS environment," the minimum is increased to ten years.	• None
Professional certification	• One of the following credentials is in valid/active status • CISA, CISSP, GICSP, CACE, CACS, or equivalent **OR** • For individuals that meet all qualifications in this column that use the term "control systems," a professional certification equivalent to one in the above list, except for any required duration of cybersecurity experience, together with a plan to achieve a full certification. See text following table for details **OR** • ISO 27001 Lead Auditor personnel certification issued by a certification body that is accredited by an accreditation body that is an IAF member (e.g. consider certifications issued by IRCA or PECB).	• None
Work experience in field	• Minimum four years of work experience in computer technology field, if individual has	• For evaluator responsible for 62443-3-2 evaluation, work

Category of qualification / experience	Baseline evaluator qualifications	Unique qualifications for evaluator roles
	degree in one of the specific subjects identified above, or has an equivalent science or engineering degree **OR** • Minimum eight years of work experience in computer technology field, if individual has a bachelor's or equivalent level degree in other subject **OR** • Minimum three years of work experience in computer technology field, if individual has Master's Degree in Cybersecurity or equivalent **OR** • Minimum two years of work experience in computer technology field if individual has PhD in Cybersecurity or equivalent	experience demonstrating use of cyber risk management concepts in operational setting (may be IT application)
Relevant work experience in ACS environment	• Minimum four years of systems integration, *commissioning*, operations, or maintenance experience for control systems **OR** • Minimum three year systems integration, commissioning, operations, or maintenance experience for control systems if individual has Master's Degree in Cybersecurity or equivalent **OR** • Minimum two year systems integration, commissioning, operations or maintenance experience for control systems if individual has PhD in Cybersecurity or equivalent **AND** • Experience includes two years with security-related responsibilities **OR** • Other experience requiring interaction with any of these activities for 6 years total with 2 years security responsibilities	• For evaluator responsible for evaluation of 62443-3-3 requirements, permit alternative experience: Minimum six years system level product test of control systems
Relevant auditing work experience	• Minimum three years experience performing cybersecurity audit (organizational) **OR** • Minimum three years in position in organization which has been audited for cybersecurity as an organization, with significant role in interaction with auditors **OR** • Industry-recognized training in IT cybersecurity auditing	• For lead evaluator role, or for evaluator responsible for evaluation of 62443-3-2 requirements, or if meet professional certification requirement with 27001 lead auditor certification, minimum three years experience performing organizational cybersecurity audit as an external auditor, is required
Relevant industry specific knowledge	• General knowledge of cyber risk management (possibly for IT) **AND** • General knowledge of at least two different control systems **AND** • General knowledge of application of control systems and roles and duties of employees at sites using control systems **AND**	• For evaluator responsible for evaluation of 62443-3-3 requirements, able to independently read and understand user installation and configuration documents for control systems products also required

Category of qualification / experience	Baseline evaluator qualifications	Unique qualifications for evaluator roles
	• Moderate level knowledge of networking and communication protocols **AND** • Moderate level knowledge of virtualization • Able to independently read and interpret requirement specifications for control systems products	
Knowledge of security standards	• ISA/IEC 62443 • ISO/IEC 27001	

If the individual meets all qualifications for an evaluator role that use the term “control systems,” then the professional certification qualification may be initially met if the individual achieves the equivalent of a professional certification from list shown in the first bullet for “Professional certification” in above table, with the exception of any certification qualification for a minimum duration of cybersecurity experience. If the chosen certification offers formal recognition for individuals meeting all certification criteria, but without sufficient experience to achieve the full certification (for example as "Associate of ISC2" for CISSP), the individual SHALL obtain this recognition to initially satisfy this professional certification qualification.

In all cases, to remain qualified after this initial qualification is achieved, the CAB SHALL plan and monitor the individual’s progress toward a full professional certification equivalent to one on the specified list. Several of these professional certification programs offer a “starter” credential that does not require experience, where the full credential may be earned later. Other programs do not have an experience requirement.

NOTE 1 If a candidate for auditor meets all qualifications in a column of Table 4 that use the term “control systems,” then GICSP or a similar control system focused professional certification is recommended.

Requirement ACSSA.R10 – Currency of skills and knowledge (Insp, Cert)

Staff training SHALL BE kept up-to-date and staff SHALL stay up-to-date of current normative specification issues (includes participation in technical groups or committees). All evaluators SHALL attend at a minimum, an annual update of ISCI approved ACSSA training.

NOTE 2 The annual ACSSA training update is expected to be at most a half day in duration.

6.4.3.2 Other standards

The ISO/IEC 17065 requirements 6.2.1 *Internal resources* and 6.2.2 *External resources* in the sub clause 6.2 *Resources for evaluation* refer to conformance to applicable requirements in ISO/IEC 17025, ISO/IEC 17020, and ISO/IEC 17021. A number of requirements from ISO/IEC 17020 are incorporated explicitly into the present specification as written in ISO/IEC 17020. These are listed under requirement ACSSA.R11 below. For other requirements in ISO/IEC 17020, detail is provided that is specific to ACSSA, elsewhere in the ACSSA specifications. These requirements are listed in Table 6 following.

Requirement ACSSA.R11 – ISO/IEC 17020 requirements (Insp, Cert)

ACSSA CBs SHALL conform to the following requirements in ISO/IEC 17020, where “inspection body,” “inspector,” and “inspection” are replaced by “certification body,” “evaluator,” and “evaluation” for consistency with terminology used elsewhere in the ACSSA specifications.

NOTE These requirements also apply to ACSSA inspection bodies since ACSSA inspection bodies are required to be accredited to the ISO/IEC 17020 standard, which is the source of the requirements in Table 5.

Table 5. ISO/IEC 17020 requirements applicable for ACSSA certification scheme (no scheme-specific detail)

17020 requirement	17020 text of requirement
5.1.3	The inspection body shall have documentation which describes the activities for which it is competent.
6.1.6	The documented procedures for training (see 6.1.5) shall address the following stages: a) an induction period; b) a mentored working period with experienced inspectors; c) continuing training to keep pace with developing technology and inspection methods.
6.1.9	Each inspector shall be observed on-site, unless there is sufficient supporting evidence that the inspector is continuing to perform competently.
6.2.13	If the inspection body uses computers or automated equipment in connection with inspections, it shall ensure that: a) computer software is adequate for use; NOTE This can be done by the following: — validation of calculations before use; — periodic revalidation of related hardware and software; — revalidation whenever changes are made to related hardware or software; — software updates implemented as required. b) procedures are established and implemented for protecting the integrity and security of data; c) computer and automated equipment is maintained in order to ensure proper functioning.
6.2.15	Relevant information on the equipment, including software, shall be recorded. This shall include identification and, where appropriate, information on calibration and maintenance.
7.1.5 (a-b are covered by 17065)	The inspection body shall have a contract or work order control system which ensures that: c) work being undertaken is controlled by regular review and corrective action; d) the requirements of the contract or work order have been met.
7.1.6	When the inspection body uses information supplied by any other party as part of the inspection process, it shall verify the integrity of such information
7.1.7	Observations or data obtained in the course of inspections shall be recorded in a timely manner so as to prevent loss of relevant information.
7.3.2	The inspection report or certificate shall be internally traceable to the inspector(s) who performed the inspection.

Requirements from ISO/IEC 17020 which apply to the ACSSA certification scheme to which additional scheme-specific information has been added, have been incorporated in ACSSA specifications as shown in Table 6.

Table 6. ISO/IEC 17020 requirements applicable for ACSSA certification scheme (with scheme specific detail)

ISO/IEC 17020 requirement	Topic	ACSSA-200 requirement
6.1 6c	Continuing training	ACSSA.R10
7.1.2	Planning and Sampling	ACSSA.R19, ACSSA.R20
7.1.9	Safety of inspection	An evaluation plan is required for each client per ACSSA.R19; the plan template includes the topic of meeting requirements for personnel access to sites, and provides examples of following safety rules and safety training as needed, in the example plan [ACSSA-305]

6.5 Process requirements

6.5.1 Overview

Clause 7 *Process requirements* in ISO/IEC 17065 covers the following topics in associated sub clauses of that document:

- General (7.1)
- Application (7.2)
- Application review (7.3)
- Evaluation (7.4)
- Review (7.5)
- Certification decision (7.6)
- Certification documentation (7.7)
- Directory of certified products (7.8)
- Surveillance (7.9)
- Changes affecting certification (7.10)
- *Termination*, reduction, *suspension* or *withdrawal* of a certification (7.11)
- Records (7.12)
- Complaints and appeals (7.13)

6.5.2 Scheme reference for standard requirements

The following table provides scheme references, for ISO/IEC 17065 requirements in Clause 7 of that document that refer to certification scheme requirements.

In Clause 7, per the *informative* guidance in Annex B of ISO/IEC 17065, the following substitutions are made when interpreting requirements for application to processes rather than products:

- replace “product(s)” with “process(es)”;
- replace “production” with “operation”;
- replace “produced” with “operated”;
- replace “producing” with “operating.”

Table 7. ACSSA certification scheme references for ISO/IEC 17065 Clause 7

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ACSSA reference
7.1 *General*	7.1.1	Certification scheme used by an ACSSA certification body	Defined in [ACSSA-100]
7.1 *General*	7.1.2	Refers to normative documents against which an asset owner’s IACS is evaluated	Documents are [ACSSA-300] and [ACSSA-311]
7.1 *General*	7.1.3	Person or committee to provide explanations per application of normative documents	ISCI Technical Steering Committee, as stated in [ACSSA-200] requirement ACSSA.R12
7.2 *Application*	7.2	Information that scheme requires for client application	[ACSSA-300] sub clause 4.2
7.4 *Evaluation*	7.4.4	Evaluation performed to scope of certification and requirements specified in scheme	Scope of an ACSSA certification is defined in [ACSSA-300] sub clause 4.1. Requirements are in [ACSSA-300] and [ACSSA-311]
7.7 *Certification documentation*	7.7.1 f	Information scheme requires on the document signifying certification	Certificate format and content specified in [ACSSA-204]

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ACSSA reference
7.8 *Directory of certified products*	7.8 last paragraph	Information about certified entities made available to a directory	[ACSSA-200] clause 6.5.3.3
7.9 *Surveillance*	7.9.1	Surveillance when specified by certification scheme	Surveillance requirements in [ACSSA-300] Clause 5
7.10 *Changes affecting certification*	7.10.1	Actions required by scheme for changes to certification criteria	[ACSSA-200] sub clause 6.5.3.4
7.11 *Termination, reduction, suspension or withdrawal of certification*	7.11.3	Actions required when a certification is terminated, suspended or withdrawn	For suspension, withdrawal, and termination, see [ACSSA-300] ISASecure_ACS.R23, [ACSSA-200] ISASecure_ACSSA.R29, and ISASecure_ACSSA.R30. Reduction is not defined for ACSSA certification
7.11 *Termination, reduction, suspension or withdrawal of certification*	7.11.4, 7.11.5	Scheme requirements related to suspension	[ACSSA-300] ISASecure_ACS.R23
7.12 Records	7.12.1	Retain records to demonstrate all certification process requirements for scheme have been effectively fulfilled	[ACSSA-200] ISASecure_ACSSA.R31
7.12 *Records*	7.12.3	Require retaining records for two cycles if scheme requires complete re-evaluation of process on a predetermined cycle	Required, in accordance with [ACSSA-300] requirement ISASecure_ACS.R27 regarding expiration and recertification

6.5.3 ISASecure ACSSA specific requirements

This sub clause lists additional scheme specific requirements related to Clause 7 *Process requirements* in ISO/IEC 17065, beyond those derived from ISO/IEC 17065 together with the other documents of the ISASecure ACSSA certification scheme.

6.5.3.1 Application

6.5.3.1.1 Process requirements

Requirement ACSSA.R12 – Determining application of specifications (Insp, Cert)
The ISO/IEC 17065 requirement 7.1.3 in Clause 7 *Process requirements* refers to persons or committees who provide the CAB with explanations as to the application of the ISASecure specifications. This role SHALL be fulfilled by the ISCI Technical Steering Committee.

Requirement ACSSA.R13 – Determining applicant eligibility (Insp, Cert)
The CAB SHALL be responsible for determining whether a potential client meets the scope for the ACSSA programs. The CAB MAY request guidance from ISCI in this matter. If the client does not concur with the decision of the CAB, they MAY use the conformant escalation process described in requirements ACSSA.R32 and ACSSA.R33.

6.5.3.1.2 Content of procedures

Requirement ACSSA.R14 – Application steps procedure (Insp, Cert)
Procedures for processing an inspection or certification application SHALL identify the steps for the application, administrative/technical processing of the investigation including typical and any required chronological order, personnel responsible for each stage of the process (possibly by job role or position), and records maintained at various steps of the process.

Requirement ACSSA.R15 – Maintenance of procedure for application (Insp, Cert)
Procedures for developing and maintaining inspection and certification application processing procedures SHALL identify personnel responsible for developing, reviewing and maintaining the procedures, the frequency for review, and personnel responsible for verifying that the procedures are being followed.

6.5.3.2 Evaluation

6.5.3.2.1 Process requirements

Requirement ACSSA.R16 – Evaluation report (Insp, Cert)
The ISO/IEC 17065 requirement 7.4.9 in sub clause 7.4 *Evaluation*, refers to documentation of evaluation results prior to review. The ISO/IEC 17020 requirements 7.4.1 and 7.4.2 refer to an inspection report that covers the work carried out by an IB. This documentation for an ACSSA inspection or certification SHALL at a minimum include an evaluation report following the content and format of [ACSSA-303], the ACSSA evaluation report sample. [ACSSA-303] specifies tailoring of the report for an inspection vs. a certification. A report following this template SHALL also be provided to the client. An inspection client will also receive a summary cover letter following the format in [ACSSA-204]. If a client applied for certification and certification criteria are not met, the certification body SHALL, unless waived by the client, issue a cover letter and a report with the same content as if the evaluation been performed under the ACSSA inspection program.

Requirement ACSSA.R17 – Use of inspection program results for certification (Cert)
If an ACSSA CB relies upon an inspection report submitted by an internal or external accredited ACSSA IB as evidence of evaluation results, as part of the basis upon which to grant an ACSSA certification, then at a minimum the CB SHALL:

- Perform the activity described in ACSSA-300 requirement ISASecure_ACS.R25 a) to determine changes to the IACS since the date of inspection

- Consider the outcome of this activity, and the time elapsed since the inspection, in its determination to accept responsibility for all or part of the inspection results in accordance with ISO/IEC 17065 requirement 7.4.5, including determination of additional verifications needed
- Verify ongoing practice of *security policies* and *procedures* during the time period since the inspection, by performing the activity "Process updates for time period of conformity" described in ACSSA-300 requirement ISASecure_ACS.25 e), for ten high risk 62443-2-1 requirements as described in ACSSA-300 requirement ISASecure_ACS.25 b), that also meet the criteria of ACSSA-300 requirement ISASecure_ACS.25 e)
- Perform all activities of annual surveillance as specified in ACSSA-300, if the application for certification is made more than one year from the date of the inspection report.

The CB MAY at their sole discretion determine to accept or not to accept the inspection report or any portion of it as evidence toward a certification, and may perform further verifications. The CB MAY determine not to accept the report in part, or in full, if one or more *major nonconformities* are found during the CAB's process to determine acceptance of inspection report results.

If a client of a CAB that is both an IB and a CB initially applies for an inspection, and elects during or after the evaluation process to modify their application to apply for a certification, all evaluation activities performed while under the inspection program, will thereafter be identified by the CAB as associated with their ACSSA certification program, for the purposes of audits performed by the accreditor for maintaining ISO/IEC 17065 accreditation.

NOTE The ISO/IEC 17065 requirement 7.4.5 applies in the first case described. It places conditions on CB reliance upon external evaluation results. That requirement incorporates other ISO/IEC 17065 requirements found in ISO/IEC 17065 6.2.2 about any CB use of external resources.

6.5.3.2.2 Content of procedures

Requirement ACSSA.R18 – Content of evaluation instructions or procedures (Insp, Cert)
Each evaluation instruction or procedure SHALL have sufficiently detailed instructions that assure reasonable repeatability of the evaluation and include or address the: title, effective date, evaluation data to be obtained and recorded, objective acceptance criteria for results, evaluation techniques, where additional information to that in [ACSSA-311] is required to meet these goals.

Requirement ACSSA.R19 – Evaluation planning (Insp, Cert)
The CAB SHALL have and SHALL use adequately documented instructions for planning an ACSSA evaluation in accordance with [ACSSA-304] and SHALL deliver an evaluation plan to the client in accordance with the ACSSA evaluation plan template [ACSSA-305]. The plan SHALL be approved by the CAB and the client. Evaluation SHALL commence after the CAB and the asset owner have approved the plan, though minor open issues in that plan may remain.

Requirement ACSSA.R20 – Sampling and evaluation techniques (Insp, Cert)
The CAB SHALL have and SHALL use adequate documented instructions on sampling and evaluation techniques, where the absence of such instructions could jeopardize the effectiveness of the evaluation process. Selection of representative sample sets of *systems under consideration*, *zones,* or *conduit*s for evaluation of conformity with ISA/IEC 62443 requirements SHALL be in accordance with sampling requirements in [ACSSA-300].

Requirement ACSSA.R21 – Content of evaluation data sheet (Insp, Cert)
Evaluation data sheets or similar paper or electronic records SHALL include the evaluation procedure and specification used, date of the evaluation, evaluation report number, signature of the personnel performing the evaluation, and evaluation results.

Requirement ACSSA.R22 – Content of procedure maintenance procedures (Insp, Cert)
Procedures for developing and maintaining evaluation instructions and procedures SHALL identify the personnel (possibly by job role or position) responsible for developing, reviewing and maintaining the procedures, specify frequency of review by management, ensure consistency with recognized specifications,

ensure that deviations still assure the process conforms with the specification, and ensure modifications are reviewed by personnel who are familiar with the specification.

Requirement ACSSA.R23 – Content of procedures for evaluation (Insp, Cert)
Procedures for evaluation SHALL require the investigator to: verify and use a current ACSSA specification edition, provide written justification of how a process conforms with each section of the specification (including a reference to an evaluation procedure). Current specification editions are identified based upon the document version listing in the publicly posted documents titled ACSSA-102 *Baseline document versions and errata for ACSSA x.y.z specifications*, together with any posted transition policies that state the current *ISASecure version(s)* for the ACSSA program. Versions are identified using the notation *x.y.z*, as in the example ACSSA 1.0.0.

NOTE An ACSSA-102 document could be posted for both ACSSA 1.0.0 and ACSSA 1.0.1, for example. More than one version of ACSSA could be considered current based upon a transition policy.

Requirement ACSSA.R24 – Content of policy for evaluation (Insp, Cert)
Policies on evaluation SHALL identify personnel responsible for technical decisions on the specification, how to decide which section of a specification applies, how to handle newly developed technologies when the specification does not apply; require that interpretations of the specifications are documented and made readily available for the appropriate evaluators; and require explanation of *nonconformities* in regard to the ISASecure specification without the CAB engaging in the redesign of the entity under evaluation.

Requirement ACSSA.R25 – Content of procedures for preparing technical reports (Insp, Cert)
Procedures for preparing technical reports SHALL BE written and SHALL:

- Identify personnel responsible for preparation, review of technical content, and initial or revision approval;
- Require the appropriate evaluation procedures; and
- Ensure that technical corrections involve qualified personnel.

6.5.3.3 Directory of certified IACS

The ISO/IEC 17065 requirement 7.8 refers to certification information to be published in a directory of certifications granted by a certification body.

Requirement ACSSA.R26 – Input to scheme directory (Cert)
The certification body SHALL inform ISCI of each certification granted and provide a copy of the certificate, to support ISCI's central directory of ISASecure certifications.

NOTE 1 From specification ACSSA-100 sub clause 4.6: "At the request of an asset owner organization, ISCI will post on its website https://ISASecure.org, the name of the asset owner organization and the information on their certificate(s). An asset owner that does not elect that ISCI post this information, may request that ISCI provide the information directly to a specified third party."

NOTE 2 The case of a report provided to a certification client where certification criteria have not been met, is not reported to the scheme directory. (See ACSSA.R16.)

NOTE 3 If approved by the asset owner, the certification body may provide public access to the certificate, see requirement ACSSA.R2.

Requirement ACSSA.R27 – Accuracy of certification status (Cert)
Proper controls SHALL be in place to assure accuracy of information on the certificate and in certification body records of certified entities.

6.5.3.4 Changes affecting certification

The ISO/IEC 17065 requirement 7.10.2 in sub clause 7.10 *Changes affecting certification*, refers to certification body actions required by the scheme when certification criteria change. Under the requirements in [ACSSA-300], conformity of a client to scheme changes is audited at the next recertification time for that client, prior to certification expiration. The following related requirement also applies.

Requirement ACSSA.R28 – Intermediate audit for changed certification criteria (Cert)
Upon request of the client, the CB SHALL audit conformity to a changed requirement, prior to its next recertification cycle. The outcome SHALL NOT negatively impact certification status. However, it MAY support the update of the client's current certification, to a more recent ISASecure ACSSA version.

6.5.3.5 Termination, reduction, suspension or withdrawal of certification

The ISO/IEC 17065 sub clause 7.11 refers to termination, reduction, suspension or withdrawal of certification. Reduction is not defined for ACSSA certification. The following requirements apply to the remaining actions.

Requirement ACSSA.R29 – Termination of certification (Cert)
Termination before expiration of a certification SHALL be supported by the CB.

The following requirement defines actions as referenced in ISO/IEC 17065 sub clause 7.11.3, that are required by the scheme upon termination, reduction, suspension or withdrawal.

Requirement ACSSA.R30 – Notification of certification status change (Cert)
The CAB SHALL inform ISCI of any suspension, restoral, withdrawal or termination of an ACSSA certification at the time it occurs.

NOTE It is permitted but not required for the CB to update the certificate itself to show suspended, withdrawn, terminated, or expired status.

6.5.3.6 Records

Requirement ACSSA.R31 – Evidence records (Insp, Cert)

The ISO/IEC 17065 requirement 7.12.1 under 7.12 *Records*, requires a certification body to retain records to demonstrate that all certification process requirements for the scheme have been effectively fulfilled. Likewise, ISO/IEC 17020 in the sub clause 7.3.1 requires an inspection body to maintain a record system to demonstrate fulfilment of inspection procedures and enable an evaluation of the inspection.

To support such demonstration, during the course of an ACSSA evaluation, the CAB SHALL maintain a record of evidence presented for evaluation under the criteria in ACSSA-311, including but not limited to:

- requirement(s) for which the evidence item is presented
- an identifier or short description for each evidence item including date or revision where applicable, and key confirmations
- source organization for item (e.g. asset owner, product supplier, integrator, maintenance service provider)
- source contact that provided the item (name and/or role)
- role of individual and scope of zones(s) or conduit(s), for interview or questionnaire evidence (see requirement ACSSA-300 ISASecure_ACS.R10)

- method of acquisition (e.g. contract deliverable, formal request, asset owner developed)
- CAB evaluator who reviewed the item
- method of access or delivery (e.g. live screen share, document portal, on-site observation, interview, questionnaire)

These records SHALL be maintained after the evaluation in accordance with CAB data retention procedures.

NOTE Data retention procedures are required under sub clauses 7.12.3 and 8.4.2 in ISO/IEC 17065, and 8.4 in ISO/IEC 17020.

6.5.3.7 Complaints and appeals

The ISO/IEC 17065 requirement 17.13.1 under 17.13 *Complaints and appeals*, refers to the certification body process related to complaints and appeals.

Requirement ACSSA.R32 – Escalation for complaints and appeals (Insp, Cert)
The published CAB process for handling complaints SHALL include the provision that complaints may be appealed to ISCI by the party bringing the complaint, if the internal CAB resolution procedure does not offer a resolution satisfactory to them. Appealed complaints SHALL first go to the ISCI Technical Steering Committee. They MAY be further appealed to the ISCI governing board, then to the ASCI board of directors.

Requirement ACSSA.R33 – Escalation for complaints and appeals related to application of specifications (Insp, Cert)
An appealed complaint may request a ruling on whether the ISASecure specifications were correctly applied in a specific instance. Such a complaint SHALL NOT be escalated to the ASCI board of directors, but is resolved within ISCI. This ruling could impact:

- Whether the ACSSA inspection or certification process is applicable to a particular organization that has applied for that program;
- The nature of inspection results and whether or not a certification was granted; or
- Adequacy of the ACSSA evaluation process by the CAB.

NOTE ISCI or ASCI does not accept inspection or certification applications, nor process, grant, or revoke certifications or inspection reports. This is the role of a CAB. ISCI can assist in interpretation of the ISASecure ACSSA specifications.

6.6 Management system requirements

6.6.1 Overview

Clause 8 *Management system requirements* in ISO/IEC 17065 covers the following topics in associated sub clauses. Sub clause 8.1 describes two options open to certification bodies to meet the ISO/IEC 17065 management system requirements. Option A is the option for a certification body to conform to the management system requirements listed in sub clauses 8.2-8.8 of ISO/IEC 17065. Option B is the option for a certification body to conform to ISO 9001 [7] requirements. Option B does not require that the certification body be certified to ISO 9001.

- Options (8.1)
- General management system documentation (Option A) (8.2)
- Control of documents (Option A) (8.3)
- Control of records (Option A) (8.4)
- Management review (Option A) (8.5)

- Internal audits (Option A) (8.6)
- Corrective actions (Option A) (8.7)
- Preventative actions (Option A) (8.8)

6.6.2 Scheme references for standard requirements

No requirements in ISO/IEC 17065 Clause 8 refer to scheme specific requirements.

6.6.3 ISASecure ACSSA specific requirements

This sub clause lists additional scheme specific requirements related to Clause 8 *Management system requirements* in ISO/IEC 17065, beyond those derived from ISO/IEC 17065 together with the other documents of the ISASecure ACSSA certification scheme. They apply whether the certification body elects Option A or Option B to fulfill the management system requirements.

6.6.3.1 General management system documentation

Requirement ACSSA.R34 – Scope of procedures under management system (Insp, Cert)
CAB procedures SHALL cover the entire "quality loop" from application for services to final evaluation report and listing of certification status (where applicable), including follow-up services.

Requirement ACSSA.R35 – Responsibility for quality (Insp, Cert)
The CAB SHALL:

- identify the personnel responsible for quality, other general and the specific responsibilities for quality, and the authority delegated to each activity;
- specify the coordination necessary between different activities; and
- identify the control over activities that affect quality.

Requirement ACSSA.R36 – Housekeeping (Insp, Cert)
Adequate measures SHALL be taken to ensure good housekeeping at the CAB facilities where evaluation activities are performed.

Requirement ACSSA.R37 – Artifact inventory (Insp, Cert)
CAB procedures for handling of *artifact* samples SHALL address item inventory.

Requirement ACSSA.R38 – Facility security (Insp, Cert)
CAB measures and procedures related to security SHALL include provisions for: controlling access, off hours security, and fire protection for the facility; informing all personnel of security policies; limiting distribution of confidential information; limiting access to and safe storage of records (including certificates and reports); back-up or off-site storage; and designate personnel responsible for monitoring security.

6.6.3.2 Control of documents

Requirement ACSSA.R39 – Processing for revisions to normative specifications (Insp, Cert)
Policies and procedures for distribution & control of *normative* specifications SHALL identify the personnel responsible for maintaining and distributing revised specifications, and a method to notify all relevant locations, including clients and agents, about modifications or amendments.

Requirement ACSSA.R40 – Archival of superseded specifications (Insp, Cert)
Superseded normative specifications SHALL be archived.

6.6.3.3 Control of records

Requirement ACSSA.R41 – Maintenance of records (Insp, Cert)
Records maintained for evaluation, inspection, and certification SHALL identify the personnel responsible for maintaining records and how to correct or modify information on a record.

6.6.3.4 Management review

Requirement ACSSA.R42 – Management follow-up review for deficiencies (Insp, Cert)
Internal quality audit policies and procedures SHALL specify the management review of reasons for deficiencies, conclusions, recommendations on corrective actions, and the effectiveness of corrective actions.

6.6.3.5 Internal audits

Requirement ACSSA.R43 – Basis for internal audits (Insp, Cert)
Internal quality audit policies and procedures SHALL specify the basis for conducting audits.

Requirement ACSSA.R44 – Contents included in internal audit reports (Insp, Cert)
Audit reports SHALL include the name(s) of the auditor(s), the areas audited, the dates of the audit and the signature of the auditor(s), the discrepancies encountered, corrective action plan (including time for completion and evidence of implementation), and review by upper management.

Requirement ACSSA.R45 – Internal audits of satellite facilities (Insp, Cert)
Quality assurance oversight of company owned satellite facilities SHALL include routine and documented internal audits of satellite facility personnel, regular headquarters review and audit of the quality assurance program and audits conducted by satellite personnel, and consistency of technical records and interpretations among all facilities.

Requirement ACSSA.R46 – Implementation for permanent corrective actions (Insp, Cert)
Internal quality audit policies and procedures SHALL specify how permanent changes resulting from corrective actions are recorded in standard operating procedures, instructions, manuals and specifications.

6.6.3.6 Complaints to ACSSA certified clients

Requirement ACSSA.R47 – Asset owner process for disclosure of complaints related to nonconformities (Cert)
A certification body SHALL include the following in its signed agreement with the client organization: that the client organization has a documented process for meeting the requirements regarding complaints they receive related to conformity to ACSSA requirements, that are found in ISO/IEC 17065 4.1.2.2j. These requirements address handling and disclosure to the certification body of such complaints known to the certified organization.

7 Requirements on operations of inspection bodies

7.1 Overview

Requirements for ACSSA IBs consist of requirements unique to the IBs participating in the ACSSA inspection program, and requirements in common with those for ACSSA CBs. These requirements are enumerated in the following two sub clauses.

7.2 Unique requirements for IBs

The following ACSSA-specific requirements SHALL apply to ACSSA IBs, in addition to the ACSSA requirements in common for IBs and CBs, which are specified in 7.3.

Requirement ACSSA.R48 – Inspection scheme and methods (Insp)

ISO/IEC 17020 requirement 7.1.1 requires an IB to “use methods and procedures for inspection which are defined in the requirements against which inspection is to be performed.” The methods and procedures used for an IACS evaluation under the ACSSA inspection program SHALL BE as defined in the specifications [ACSSA-300] and [ACSSA-311].

Requirement ACSSA.R49 – Input to scheme records (Insp)

The inspection body SHALL inform ISCI of each inspection report delivered to a client, and provide a copy of the cover letter described in requirement ACSSA.R16 of the present document.

NOTE 1 Access to these records is restricted to ISCI, for use in managing the ACSSA inspection program. ISCI will not publish or otherwise make available to third parties, any information about IACS and identities of asset owners that have undergone ACSSA evaluation under the ACSSA inspection program. Requirement ACSSA.R2 addresses disclosure by the IB of inspection information.

Requirement ACSSA.R50 – Asset owner references to inspection results (Insp)

Asset owner references to the results of an evaluation under the ACSSA inspection scheme SHALL BE in accordance with the specification [ACSSA-204]. The inspection body SHALL exercise control of such references as governed by that specification over ownership, use and display of licenses, marks of conformity, and any other mechanisms that refer to ACSSA inspection activities in which an asset owner has participated. Incorrect references to the inspection scheme, or misleading use of licenses, marks, or statements found in documentation or other publicity, SHALL be dealt with by suitable action.

NOTE 2 This requirement is adapted from the similar requirement for CBs, ISO/IEC 17065 4.1.3.

7.3 Common CAB requirements

The following requirements found in Clause 6 for ACSSA certification bodies, SHALL also apply for ACSSA inspection bodies:

Requirement ACSSA.R1 – Confidentiality for ASCI and ISCI (Insp, Cert)

Requirement ACSSA.R2 – Handling of inspection and certification data (Insp, Cert)

Requirement ACSSA.R3 – Public availability of ISCI complaint escalation process (Insp, Cert)

Requirement ACSSA.R5 – Client facility access (Insp, Cert)

Requirement ACSSA.R6 – Organizational affiliations (Insp, Cert)

Requirement ACSSA.R7 – Financial affiliations (Insp, Cert)

Requirement ACSSA.R8 – CAB sales and purchases (Insp, Cert)

Requirement ACSSA.R9 – Evaluator minimum qualifications (Insp, Cert)

Requirement ACSSA.R10 – Currency of skills and knowledge (Insp, Cert)

Requirement ACSSA.R11 – ISO/IEC 17020 requirements (Insp, Cert)

Requirement ACSSA.R12 – Determining application of specifications (Insp, Cert)

Requirement ACSSA.R13 – Determining applicant eligibility (Insp, Cert)

Requirement ACSSA.R14 – Application steps procedure (Insp, Cert)

Requirement ACSSA.R15 – Maintenance of procedure for application (Insp, Cert)

Requirement ACSSA.R16 – Evaluation report (Insp, Cert)

Requirement ACSSA.R18 – Content of evaluation instructions or procedures (Insp, Cert)

Requirement ACSSA.R19 – Evaluation planning (Insp, Cert)

Requirement ACSSA.R20 – Sampling and evaluation techniques (Insp, Cert)

Requirement ACSSA.R21 – Content of evaluation data sheet (Insp, Cert)

Requirement ACSSA.R22 – Content of procedure maintenance procedures (Insp, Cert)

Requirement ACSSA.R23 – Content of procedures for evaluation (Insp, Cert)

Requirement ACSSA.R24 – Content of policy for evaluation (Insp, Cert)

Requirement ACSSA.R25 – Content of procedures for preparing technical reports (Insp, Cert)

Requirement ACSSA.R31 – Evidence records (Insp, Cert)

Requirement ACSSA.R32 – Escalation for complaints and appeals (Insp, Cert)

Requirement ACSSA.R33 – Escalation for complaints and appeals related to application of specifications (Insp, Cert)

Requirement ACSSA.R34 – Scope of procedures under management system (Insp, Cert)

Requirement ACSSA.R35 – Responsibility for quality (Insp, Cert)

Requirement ACSSA.R36 – Housekeeping (Insp, Cert)

Requirement ACSSA.R37 – Artifact inventory (Insp, Cert)

Requirement ACSSA.R38 – Facility security (Insp, Cert)

Requirement ACSSA.R39 – Processing for revisions to normative specifications (Insp, Cert)

Requirement ACSSA.R40 – Archival of superseded specifications (Insp, Cert)

Requirement ACSSA.R41 – Maintenance of records (Insp, Cert)

Requirement ACSSA.R42 – Management follow-up review for deficiencies (Insp, Cert)

Requirement ACSSA.R43 – Basis for internal audits (Insp, Cert)

Requirement ACSSA.R44 – Contents included in internal audit reports (Insp, Cert)

Requirement ACSSA.R45 – Internal audits of satellite facilities (Insp, Cert)

Requirement ACSSA.R46 – Implementation for permanent corrective actions (Insp, Cert)

NOTE The following are not required for IBs under the ACSSA inspection program:

Requirement ACSSA.R4 – Time delay from provision of consultancy (Cert)

Requirement ACSSA.R17 – Use of inspection program results for certification (Cert)

Requirement ACSSA.R26 – Input to scheme directory (Cert)

Requirement ACSSA.R27 – Accuracy of certification status (Cert)

Requirement ACSSA.R28 – Intermediate audit for changed certification criteria (Cert)

Requirement ACSSA.R29 – Termination of certification (Cert)

Requirement ACSSA.R30 – Notification of certification status change (Cert)

Requirement ACSSA.R47 – Asset owner process for disclosure of complaints related to nonconformity (Cert)

8 Annex A: ACSSA-specific CAB requirements mapped to SDLA-specific CB requirements

The table below shows ACSSA-specific CAB requirements from the present document, for which there are similar or identical SDLA-specific requirements in the specification SDLA-200 [5] for the ISASecure SDLA certification program. The purpose of the mapping is to assist an entity that holds accreditation as an ISASecure SDLA CB, in extending the scope of their processes to support ACSSA accreditation.

Table 8. ACSSA-specific and SDLA-specific CB requirements

ACSSA-200 requirement ID	ACSSA-200 requirement title	SDLA-200 requirement ID	SDLA-200 requirement title	Modification to SDLA requirement for ACSSA
ACSSA.R1	Confidentiality for ASCI and ISCI (Insp, Cert)	SDLA.R1	Confidentiality for ASCI and ISCI	Identical requirement
ACSSA.R2	Handling of inspection and certification data (Insp, Cert)	SDLA.R2	Internal distribution for assessment reports	Change chartered laboratory to CAB; add concept of certification scoping detail and requirements on external distribution; add adherence to confidentiality procedures in evaluation plan to CAB/client legal agreement
ACSSA.R3	Public availability of ISCI complaint escalation process (Insp, Cert)	SDLA.R3	Public availability of ISCI complaint escalation process	Add reference to 17020 and IB
ACSSA.R4	Time delay from provision of consultancy (Cert)	SDLA.R4	Time delay from provision of consultancy	Consultancy for IACS instead of product
ACSSA.R5	Client facility access (Insp, Cert)	SDLA.R5	Client facility access without prior notification	Modified for IACS facility vs. development facility
ACSSA.R6	Organizational affiliations (Insp, Cert)	SDLA.R6	Organizational affiliations	Modified for asset owner vs. product supplier; add reference to inspection

ACSSA-200 requirement ID	ACSSA-200 requirement title	SDLA-200 requirement ID	SDLA-200 requirement title	Modification to SDLA requirement for ACSSA
ACSSA.R7	Financial affiliations (Insp, Cert)	SDLA.R7	Financial affiliations	Modified for asset owner vs. product supplier; change chartered laboratory and certification body to CAB
ACSSA.R8	CAB sales and purchases (Insp, Cert)	SDLA.R8	CAB sales and purchases	Modified for asset owner vs. product supplier and exception for Type C IB
ACSSA.R9	Evaluator minimum qualifications (Insp, Cert)	SDLA.R9	Evaluator minimum qualifications	Modified for unique roles and qualifications for ACSSA evaluators
---	---	SDLA.R9A	Chartered laboratory [timeline] requirement for personnel with full professional certifications	---
ACSSA.R10	Currency of skills and knowledge (Insp, Cert)	SDLA.R10	Currency of skills and knowledge	Add required annual training update
ACSSA.R11	ISO/IEC 17020 requirements (Insp, Cert)	---	---	---
ACSSA.R12	Determining application of specifications (Insp, Cert)	SDLA.R11	Determining application of specifications	Change chartered laboratory to CAB
ACSSA.R13	Determining applicant eligibility (Insp, Cert)	SDLA.R12	Determining applicant eligibility	Change chartered laboratory to CAB and SDLA to ACSSA

ACSSA-200 requirement ID	ACSSA-200 requirement title	SDLA-200 requirement ID	SDLA-200 requirement title	Modification to SDLA requirement for ACSSA
ACSSA.R14	Application steps procedure (Insp, Cert)	SDLA.R13	Application steps procedure	Certification changed to inspection or certification; specify typical chronological order and any required chronological order
ACSSA.R15	Maintenance of procedure for application (Insp, Cert)	SDLA.R14	Maintenance of procedure for application	Certification changed to inspection and certification
ACSSA.R16	Evaluation report (Insp, Cert)	SDLA.R15	Assessment report	Define both inspection and certification reports; adds cover letter for inspection reports; report issued whether or not certification passed
ACSSA.R17	Use of inspection program results for certification (Cert)	---	---	---
ACSSA.R18	Content of evaluation instructions or procedures (Insp, Cert)	SDLA.R16	Content of assessment methods or procedures	Change term assessment to evaluation; evaluation methods to evaluation instructions; SDLA to ACSSA
ACSSA.R19	Evaluation planning (Insp, Cert)	---	---	---
ACSSA.R20	Sampling and evaluation techniques (Insp, Cert)	SDLA.R17	Sampling	Adds references to requirements and guidance in [ACSSA-300]

ACSSA-200 requirement ID	ACSSA-200 requirement title	SDLA-200 requirement ID	SDLA-200 requirement title	Modification to SDLA requirement for ACSSA
ACSSA.R21	Content of evaluation data sheet (Insp, Cert)	SDLA.R18	Content of assessment data sheet	Change term assessment to evaluation; add reference to electronic records
ACSSA.R22	Content of procedure maintenance procedures (Insp, Cert)	SDLA.R19	Content of procedure maintenance procedures	Change term assessment to evaluation, and evaluation methods to evaluation instructions
ACSSA.R23	Content of procedures for evaluation (Insp, Cert)	SDLA.R20	Content of procedures for evaluating assessment data	Change term assessment to evaluation, refer to current rather than latest specifications; add method to determine current specifications
ACSSA.R24	Content of policy for evaluation (Insp, Cert)	SDLA.R21	Content of policy for evaluation of assessment data	Remove term assessment and phrase assessment data; remove requiring resolution of discrepancies; change term failures to nonconformities
ACSSA.R25	Content of procedures for preparing technical reports (Insp, Cert)	SDLA.R22	Content of procedures for preparing technical reports	Removed reference to test
ACSSA.R26	Input to scheme directory	SDLA.R23	Input to scheme directory	Add note referencing policy in [ACSSA-300] regarding disclosure/posting of certificates
ACSSA.R27	Accuracy of certification status (Cert)	SDLA.R24	Accuracy of certification status	Identical requirement

ACSSA-200 requirement ID	ACSSA-200 requirement title	SDLA-200 requirement ID	SDLA-200 requirement title	Modification to SDLA requirement for ACSSA
ACSSA.R28	Intermediate audit for changed certification criteria (Cert)	SDLA.R25	Intermediate audit for changed certification criteria	Change chartered laboratory to CB; SDLA to ACSSA
ACSSA.R29	Termination of certification (Cert)	SDLA.R26	Termination of certification	Change chartered laboratory to CB
ACSSA.R30	Notification of certification status change (Cert)	SDLA.R27	Notification of termination of certification	Change chartered laboratory to CB; add additional types of status changes other than termination, which are to be reported to ISCI
ACSSA.R31	Evidence records (Insp, Cert)	---	---	---
ACSSA.R32	Escalation for complaints and appeals (Insp, Cert)	SDLA.R28	Escalation for complaints and appeals	Change chartered laboratory to CAB
ACSSA.R33	Escalation for complaints and appeals related to application of specifications (Insp, Cert)	SDLA.R29	Escalation for complaints and appeals related to application of specifications	Add reference to inspection; change SDL evaluation to ACSSA evaluation
ACSSA.R34	Scope of procedures under management system (Insp, Cert)	SDLA.30	Scope of procedures under management system	Change chartered laboratory to CAB; change assessment to evaluation report
ACSSA.R35	Responsibility for quality (Insp, Cert)	SDLA.R31	Responsibility for quality	Change chartered laboratory to CAB
ACSSA.R36	Housekeeping (Insp, Cert)	SDLA.R32	Housekeeping	Change chartered laboratory to CAB
ACSSA.R37	Artifact inventory (Insp, Cert)	SDLA.R33	Artifact inventory	Change laboratory to CAB
ACSSA.R38	Facility security (Insp, Cert)	SDLA.R34	Facility security	Change chartered laboratory to CAB

ACSSA-200 requirement ID	ACSSA-200 requirement title	SDLA-200 requirement ID	SDLA-200 requirement title	Modification to SDLA requirement for ACSSA
ACSSA.R39	Processing for revisions to normative specifications (Insp, Cert)	SDLA.R35	Processing for revisions to normative specifications (Insp, Cert)	Identical requirement
ACSSA.R40	Archival of superseded specifications (Insp, Cert)	SDLA.R36	Archival of superseded specifications	Identical requirement
ACSSA.R41	Maintenance of records (Insp, Cert)	SDLA.R37	Maintenance of records (Insp, Cert)	Add reference to inspection
ACSSA.R42	Management follow-up review for deficiencies (Insp, Cert)	SDLA.R38	Management follow-up review for deficiencies	Identical requirement
ACSSA.R43	Basis for internal audits (Insp, Cert)	SDLA.R39	Basis for internal audits	Identical requirement
ACSSA.R44	Contents included in internal audit reports (Insp, Cert)	SDLA.R40	Contents included in internal audit reports	Identical requirement
ACSSA.R45	Internal audits of satellite facilities (Insp, Cert)	SDLA.R41	Internal audits of satellite facilities	Identical requirement
ACSSA.R46	Implementation for permanent corrective actions (Insp, Cert)	SDLA.R42	Implementation for permanent corrective actions	Identical requirement
ACSSA.R47	Asset owner process for disclosure of complaints related to nonconformity (Cert)	SDLA.R43	Supplier process for disclosure of complaints related to nonconformity	Asset owner instead of supplier
---	---	SDLA.R44	Supplier process for disclosure of complaints related to security development process effectiveness	---

ACSSA-200 requirement ID	ACSSA-200 requirement title	SDLA-200 requirement ID	SDLA-200 requirement title	Modification to SDLA requirement for ACSSA
---	---	SDLA.R45	Disclosure to ISCI of complaints related to security development lifecycle effectiveness	---
ACSSA.R48	Inspection scheme and methods (Insp)	---	---	---
ACSSA.R49	Input to scheme records (Insp)	SDLA.R23	Input to scheme records	Applies to inspection report cover letters instead of certificates
ACSSA.R50	Asset owner references to inspection results (Insp)	---	---	---

BIBLIOGRAPHY

The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC. These 62443 standards that apply to a product supplier, are not in scope for an ACSSA evaluation. However, asset owners that use suppliers who hold certifications demonstrating conformance to these standards, will find this practice beneficial for achieving conformance to ACSSA requirements and for demonstrating that conformance. Section 4.7 of [ACSSA-100] discusses the relationship between ACSSA and other ISA/IEC 62443 certifications such as ISASecure CSA, ISASecure SSA, and ISASecure SDLA.

[1] ANSI/ISA-62443-4-1-2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[2] IEC 62443-4-1:2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[3] ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[4] IEC 62443-4-2:2019 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[5] SDLA-200 *ISCI Security Development Lifecycle Assurance – ISASecure SDLA chartered laboratory operations and accreditation v1.9,* available at https://ISASecure.org

[6] [ACSSA-101] *ISCI Automation and Control System Security Assurance – Evaluation planning for asset owners, available at* https://ISASecure.org

[7] ISO 9001:2015 *Quality management systems – Requirements*