# CSA-200

# ISA Security Compliance Institute – Component Security Assurance –
**ISASecure CSA chartered laboratory operations and accreditation**

## Version 4.8

October 2021

## 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, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. 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 | 2010.06.07 | Initial version published to http://www.ISASecure.org |
| 1.3 | 2010.09.21 | Table 3 changes for requirement numbers and modified requirements due to revisions to CRT specs EDSA-310 and 401 through 406 |
| 2.1 | 2011.10.13 | Support CRT by organization separate from chartered laboratory |
| 3.3 | 2015.04.22 | Change from Guide 65 to 17065, incorporate ASCI 2009 requirements directly, add VIT to EDSA, all requirements to be met for provisional status except part of technical readiness assessment based on sample device, add SDLPA acronym, no calibration required for CRT tool, update tool versions requirement to include full software version, added GICSP and CSSLP certification, more explanation about 3 vs. 4 levels for EDSA, add EDSA.R38 statement about loss of SDLA cert |
| 3.6 | 2018.01.30 | Alignment with approved ANSI/ISA-62443-4-1: update references, terms, background section, 4.1 discussion of levels, replace section 5.3 with discussion of transition to EDSA 2.1.0; incorporate errata from EDSA-102 v3.1 |
| 3.9 | 2018.10.01 | Update for ANSI/ISA-62443-4-2 alignment for EDSA 3.0.0: update normative references for ISASecure-116, 62443-4-2, and CSA-311, change text in 4.1 about permitting allocation to environment – to *met by integration into system,* in 4.1 change from three to four levels and remove statement that VIT depends upon FSA-E, modify 5.3 for transition to EDSA 3.0.0 |
| 4.2 | 2019.08.03 | Change title from EDSA-200 to CSA-200; clarify definition of term certification level; add definition of security level; modifications to cover all component types; remove CRT, CRT lab and CRT tools; update material related to maintenance of certification; update version of 17025; 17025 scope includes FSA-C testing; add latest version of 17011 |
| 4.8 | 2021.10.26 | Revise 6.4.3.1 personnel qualifications to support substitution of training for some qualifications and increase flexibility of education and experience requirements; add CSA.R11 regarding timeline for chartered lab to have personnel with full professional certifications |
|  |  |  |
|  |  |  |

# Contents

# List of requirements

## List of tables

# FOREWORD

This is one of a series of documents that defines the ISASecure® CSA (Component Security Assurance) certification program for software applications, embedded devices, host devices and network devices. These are the component types defined by the standard IEC 62443-4-2 that are used to build control systems. ISASecure CSA is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). The current list of all ISASecure certification programs and documents related to these programs can be found on the web site http://www.ISASecure.org.

# 1 Scope

The ISASecure® certification programs have been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cyber security for Industrial Automation and Control Systems (IACS). An organization that performs evaluations and grants certifications under the ISASecure CSA (Component Security Assurance) program is referred to as a *ISASecure CSA chartered laboratory*, or (more briefly) a *chartered laboratory.* This document specifies the criteria and processes that define:

- Requirements on the operations of a chartered laboratory (Section 6); and

- How a chartered laboratory shall begin and continue ISASecure component certification operations (Section 7).

ISCI has based its certification program approach on:

- International standards for conformity assessment programs

- IACS security standards IEC 62443-4-1 and IEC 62443-4-2 (also published as ANSI/ISA standards)

- Specifications developed for the ISASecure CSA program.

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

ISASecure CSA is a *product* certification program for IACS components. An IACS component is an entity that is used to build control systems and that exhibits the characteristics of one or more of a software application, embedded device, host device, or network device. These component types are defined in [IEC 62443-4-2] and in 3.1 of the present document. ISCI also has developed *product* certification and *process* certification programs for:

- Control system products, the ISASecure SSA program (System Security Assurance)

- Supplier's secure product development lifecycle process, the ISASecure SDLA program (Security Development Lifecycle Assurance).

The separate documents SSA-200 *ISASecure SSA chartered laboratory operations and accreditation* and SDLA-200 *ISASecure SDLA chartered laboratory operations and accreditation* address these same topics as they relate to chartered laboratories that perform ISASecure SSA and SDLA certifications, respectively.

ISASecure programs support and align with the standards ANSI/ISA/IEC 62443 for IACS security. [CSA-100] discusses the relationship between ISASecure CSA and the ANSI/ISA/IEC 62443 effort.

# 2 Normative references

## 2.1 General

NOTE   The following is the highest level document that describes the ISASecure CSA certification program.

[CSA-100] *ISCI Component Security Assurance – ISASecure Certification Scheme*, as specified at http://www.ISASecure.org

## 2.2 Accreditation

### 2.2.1 Chartered laboratory operations and accreditation

[ISASecure-115] *ISCI ISASecure Certification Programs - Policy for transition to SDLA 2.0.0, EDSA 2.1.0 and SSA 2.1.0*, as specified at http://www.ISASecure.org

[ISASecure-116] *ISCI ISASecure Certification Programs - Policy for transition to EDSA 3.0.0 and SSA 3.0.0*, as specified at http://www.ISASecure.org

[ISASecure-117] *ISCI ISASecure Certification Programs - Policy for transition to CSA 1.0.0 and SSA 4.0.0* as specified at http://www.ISASecure.org

NOTE   The following document can be tailored for chartered laboratories performing CSA, SSA or SDLA certifications, or any combination of these.

[ISASecure-202] *ISCI ISASecure Certification Programs – Application and Contract for Chartered Laboratories*, internal ISCI document

## 2.2.2  Deleted

## 2.2.3  Deleted

## 2.3  ISASecure symbol and certificates

NOTE   The following document describes the ISASecure symbol and certificates and how they are used within the ISASecure CSA programs.

[CSA-204] *ISCI Component Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at http://www.ISASecure.org

[CSA-205] *ISCI Component Security Assurance – Certificate Document Format,* as specified at http://www.ISASecure.org

## 2.4  Technical specifications

## 2.4.1  General technical specifications

NOTE   The following document is the overarching technical specification for ISASecure CSA certification.

[CSA-300] *ISCI Component Security Assurance – ISASecure certification requirements,* as specified at http://www.ISASecure.org

[CSA-301] *ISCI Component Security Assurance – Maintenance of ISASecure certification,* as specified at http://www.ISASecure.org

[CSA-303] *ISASecure CSA Sample Report*, available on request to ISCI

## 2.4.2  Specifications for certification elements

NOTE 1   The following document provides the technical evaluation criteria for the Vulnerability Identification Testing (VIT-C) element of a CSA evaluation.

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Test Specification*, as specified at http://www.ISASecure.org

NOTE 2   The following document provides the technical evaluation criteria for the Functional Security Assessment element (FSA-C) of a CSA evaluation.

[CSA-311] *ISCI Component Security Assurance – Functional security assessment for components,* as specified at http://www.ISASecure.org

NOTE 3   The following documents provide the overall technical evaluation criteria for the Security Development Artifacts element (SDA-C) of a CSA product evaluation.  [SDLA-312] also provides the technical evaluation criteria for an ISASecure assessment of supplier secure product development lifecycle process performed for an ISASecure SDLA certification.

[CSA-312] *ISCI Component Security Assurance – Security development artifacts for components,* as specified at http://www.ISASecure.org

[SDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*, as specified at http://www.ISASecure.org

NOTE 4   The following is the highest level document that describes the related ISASecure SDLA certification program for supplier secure product development lifecycle processes.

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme*, as specified at http://www.ISASecure.org

[SDLA-200] *ISCI Security Development Lifecycle Assurance – ISASecure SDLA chartered laboratory operations and accreditation*

## 2.5   External references

External references are documents that are maintained outside of the ISASecure CSA program and are used by the program.

### 2.5.1   IACS security standards

NOTE 1   [CSA-100] describes the relationship of ISASecure CSA to these standards.

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

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

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

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

### 2.5.2   International standards for certification programs

NOTE 1  The following international standards apply to the ISASecure CSA certification and testing processes.

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

NOTE 2  The transition timeline to the later 2017 version of ISO/IEC 17025 below is defined by ISO/ILAC policy.

[ISO/IEC 17025 2005] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories",* 15 May 2005

[ISO/IEC 17025] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories",* November 2017

### 2.5.3   International standards for accreditation programs

NOTE   The following international standard applies to the ISASecure CSA chartered laboratory accreditation process. The transition timeline to the later 2017 version of ISO/IEC 17011 below is defined by ISO/ILAC policy.

[ISO/IEC 17011 2004] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", 01 September 2004

[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

**3.1.1**
**accreditation**
third party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks

NOTE  For the ISASecure CSA certification programs, accreditation is an assessment and recognition process via which an organization is granted chartered CSA laboratory status.

**3.1.2**
**accreditation body**
third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out specific conformity assessment

**3.1.3**
**applicant**
organization that has submitted a product or process to a chartered laboratory for evaluation for ISASecure certification

**3.1.4**
**auditable product**
hardware and/or software product such that the product or its associated development process is subject to audit, in the course of a specific chartered laboratory's planned certification activities

**3.1.5**
**capability security level**
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

**3.1.6**
**certification level**
capability security level for which conformance is demonstrated by a certification

NOTE  It is intended that a product that achieves certification to CSA capability security level $n$ will meet requirements for capability security level $n$ as defined in [IEC 62443-4-2].

**3.1.7**
**component**
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

**3.1.8**
**conformity assessment body**
body that performs conformity assessment services and that can be the object of accreditation

NOTE   Examples are a laboratory, inspection body, product certification body, management system certification body and personnel certification body. This is an ISO/IEC term and concept.

**3.1.9**
**chartered laboratory**
organization chartered by ASCI to evaluate products and/or processes under one or more ISASecure certification programs and to grant certifications under one or more of these programs

NOTE   A chartered laboratory is the conformity assessment body for the ISASecure certification programs.

### 3.1.10
### embedded device
special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE   Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

### 3.1.11
### host device
general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE   Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

### 3.1.12
### industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

### 3.1.13
### major owner
owner of more than two percent (2%) of a business entity

NOTE   This percentage is intended to exclude individuals who are owners via portfolio vehicles, and identify owners that may influence the activities of the business entity.

### 3.1.14
### major user
organization that has or plans purchase of products whose related costs and/or usage is material to the overall operations of that organization

### 3.1.15
### network device
device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

NOTE   Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

### 3.1.16  security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

NOTE   Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

### 3.1.17
### significant financing
financing that is material to the operations of the recipient

### 3.1.18
### significant financial interest
financial interest where the value of this interest is material to the financial position of the entity that has the interest

**3.1.19**
**significant sales**
sales that are material to the operations of the seller

**3.1.20**
**software application**
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

NOTE 1  Software applications typically execute on host devices or embedded devices.

NOTE 2   Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

**3.1.21**
**symbol**
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE    An earlier term for symbol is "mark."

**3.1.22**
**termination**
withdrawal of certification, initiated by the entity that holds the certification

**3.1.23**
**update**
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues

**3.1.24**
**upgrade**
incremental hardware or software change in order to add new features

**3.1.25**
**withdrawal**
cancellation of the statement of conformity

### 3.2 Abbreviations

The following abbreviations are used in this document.

| | |
|---|---|
| ANSI | American National Standards Institute |
| ASCI | Automation Standards Compliance Institute |
| BS | Bachelor of Science |
| CACE | Certified Automation Cyber Security Expert |
| CACS | Certified Automation Cyber Security Specialist |
| CE | computer engineering |
| CISA | Certified Information Systems Auditor |
| CISSP | Certified Information Systems Security Professional |
| CSSLP | Certified Secure Software Lifecycle Professional |
| CS | computer science |
| CSA | component security assurance |
| EDSA | embedded device security assurance |
| FSA-C | functional security assessment for components |
| GICSP | Global Industrial Cyber Security Professional |
| IACS | industrial automation and control system(s) |
| IAF | International Accreditation Forum |
| IEC | International Electrotechnical Commission |
| ILAC | International Laboratory Accreditation Cooperation |
| ISA | International Society of Automation |
| ISCI | ISA Security Compliance Institute |
| ISO | International Organization for Standardization |
| SDA-C | security development artifacts for components |
| SDLA | security development lifecycle assurance |
| SDLPA-C | security development lifecycle process assessment for components |
| VIT-C | vulnerability identification testing for components |

## 4  Background

### 4.1  Technical ISASecure CSA certification elements

ISASecure CSA is a certification program for IACS components. An IACS component is an entity that is used to build control systems and that exhibits the characteristics of one or more of a software application, embedded device, host device, or network device. These component types are defined in the standard [IEC 62443-4-2] and in 3.1 of the present document. CSA certification has the following elements:

- Security Development Lifecycle Process Assessment for components (SDLPA-C);

- Security Development Artifacts for components (SDA-C);

- Functional Security Assessment for components (FSA-C); and

- Vulnerability Identification Testing for components (VIT-C).

SDLPA-C and SDA-C both assess development process. SDLPA-C is an evaluation of the component supplier's secure product development lifecycle process. SDA-C examines the artifacts that are the outputs of the supplier's secure product development lifecycle process for the component to be certified.

FSA-C examines the security capabilities of the component, while recognizing in accordance with [IEC 62443-4-2] that requirements for security functionality differ by component type. The certifier determines all component types applicable to a product; FSA-C then incorporates requirements for all component types applicable to the product. VIT-C scans the component for the presence of known vulnerabilities.

The CSA program defines four certification levels for a component, offering increasing levels of security assurance. Levels offered are capability security levels 1, 2, 3, and 4. The corresponding certifications are called ISASecure CSA Capability Security Level 1, ISASecure CSA Capability Security Level 2, ISASecure CSA Capability Security Level 3, and ISASecure CSA Capability Security Level 4.

All levels of certification include the certification elements defined in Section 1. SDLPA-C does not have an associated level. SDA-C and VIT-C assessments are the same for all certification levels with the exception of allowable residual risk for known security issues. FSA-C incorporates more requirements at higher levels, aligned with the requirements assigned to each capability security level in [IEC 62443-4-2].

NOTE  In SDLA-312 v5.5, the treatment of residual risk related to known security issues is found in SDLA requirement SDLA-DM-4.

## 4.2  ISASecure CSA certification program implementation

ISCI is organized as an interest area within ASCI (Automation Standards Compliance Institute), a not-for-profit 503 (c) (6) corporation owned by ISA. Descriptions of the governance and organizational structure for ASCI are found on the ISASecure website: http://www.ISASecure.org.

ASCI CSA chartered laboratories are organizations that are accredited to evaluate components under the ISASecure CSA programs. ASCI grants accredited laboratories the right to process ISASecure CSA certifications for components on its behalf. A chartered laboratory will issue an ISASecure CSA certificate for a component that meets the CSA certification requirements for its applicable component type(s), as determined by the chartered laboratory. Compliance with component certification requirements is determined based upon process audits, functional audits, and tests, which measure adherence to the ISASecure CSA requirements for SDLPA-C, SDA-C, FSA-C, and VIT-C.

A supplier meets the SDLPA-C criteria by holding the ISASecure SDLA process certification described in [SDLA-100]. This prerequisite for a CSA product certification is further detailed in [CSA-300].

All evaluations defined by the CSA specifications are conducted directly by a chartered laboratory or its subcontractors.

The list of ASCI CSA chartered laboratories is posted on the ISCI website at http://www.ISASecure.org. At the request of a component supplier, components that are issued certifications are registered on this same ISCI website.

[SSA-420] requires a specific tool to be used by a chartered laboratory to perform VIT-C.

## 5  Summary of operations and accreditation requirements

### 5.1  Overview

ISASecure CSA will operate as an internationally recognized certification program. To meet this standard, the chartered laboratory operations and accreditation requirements are designed to comply with accepted international standards applicable to product certification and testing.

The operations of ISASecure CSA chartered laboratories shall be in compliance with the applicable requirements in:

- [ISO/IEC 17065], the international standard that applies to bodies that certify products, processes or services, and

- [ISO/IEC 17025 2005], the international standard that applies to test organizations, and which is updated to [ISO/IEC 17025] in a timeframe determined by ILAC/ISO policy.

The present document is organized using the outline of [ISO/IEC 17065]. Where required, it interprets requirements in that document for ISASecure CSA and adds additional requirements. Of particular note are requirements for:

- Organizational and financial affiliations of chartered laboratories (6.3.3);

- Qualifications for chartered laboratory personnel (6.4.3.1);

- Content of chartered laboratory application and evaluation procedures (6.5.3.1.2 and 6.5.3.2.3)

- Directory listing of certified products (6.5.3.3);

- Appeals for client complaints (6.5.3.7); and

- Managing complaints to suppliers regarding certified products (6.6.3.6).

## 5.2 Accreditation process

Accreditation of a chartered laboratory consists of an assessment of the organization against the general requirements in ISO/IEC 17025, 17065 and the specific requirements in Section 6 of this document, together with an assessment of technical readiness for performing ISASecure CSA evaluations. Technical readiness assessment is based upon review of laboratory processes and procedures as well as review of artifacts from SDA-C, FSA-C and VIT-C evaluations carried out by the laboratory on a component. To be recognized as a chartered laboratory for the ISASecure CSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC accreditation body:

- Accredited to ISO/IEC 17065, with technology scope of accreditation covering ISASecure CSA certification; and

- Accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure FSA-C and VIT-C specifications.

The laboratory accreditation process consists of two steps. In the first step, an IEC assessor who is qualified with respect to the above two accreditations will complete an evaluation of all accreditation requirements. Provisional chartered status is granted if ISCI's analysis of the assessor's report following this evaluation, shows that the laboratory meets the requirements for formal accreditation and technical readiness assessment defined in 7.2 of the present document. At this point the accreditation body has not yet formally granted accreditation, which requires a review and approval process internal to the accreditation body.

Once a laboratory has attained provisional chartered status, ASCI grants that laboratory the right to perform component evaluations and grant ISASecure CSA certifications. These rights continue as long as the laboratory receives formal accreditation from a CSA accreditation body in a timely manner (the second step) and maintains this status.

## 5.3 Transition to CSA 1.0.0

The approved standard [IEC 62443-4-2] defines technical security requirements for the four IACS component types: software applications, embedded devices, host devices, and network devices. Previously, the ISASecure EDSA 3.0.0 certification program certified one of these component types, embedded devices, to that standard. The release of ISASecure CSA 1.0.0 subsumes the former EDSA program, and defines certification criteria for the remaining three component types in [IEC 62443-4-2]. Accordingly, ISCI has defined a policy for chartered laboratories to follow in transitioning certification activities from EDSA 3.0.0 to CSA 1.0.0. This policy is defined in the document [ISASecure-117]. [ISASecure-117] also defines the transition policy for related changes to the separate ISASecure SSA certification program for control systems.

CSA 1.0.0 also incorporates by reference an update to the ISASecure [SDLA-312] specification, however that update does not change the SDLA certification version. SDLA v2.0.0 remains the most current version of that certification, so no transition policy for that program is needed or described in [ISASecure-117]. This is because the update to [SDLA-312] required for the CSA program, modifies material in [SDLA-312] that defines certifier validations for the element Security Development Artifacts for components (SDA-C) of CSA 1.0.0, but does not modify the material that defines certifier validations toward SDLA certification.

## 6 Requirements on operations of chartered laboratories

### 6.1 Overview

Section 6 of the present document specifies all requirements on the operation of CSA chartered laboratories. It provides specific interpretations for ISO/IEC 17065 requirements, and defines further requirements that are specific to the ISASecure CSA program.

Section 6 is organized as follows:

- The sub sections 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 sections in the present document has three further sub sections as follows:

    o *Overview* - provides a list of the topics covered in the corresponding clause of [ISO/IEC 17065]

    o *Scheme references for standard requirements* - A number of ISO/IEC 17065 requirements refer in turn to compliance with requirements specified by a certification scheme. This sub section in the present document provides a table that lists each such ISO/IEC 17065 requirement and provides a reference to the documentation in the ISASecure CSA scheme where the relevant scheme requirements are found. These references may refer to ISASecure CSA scheme documents that are listed in section 2 of the present document, or may refer to the present document itself, in particular to requirements in the sub sections in the present document described next.

    o *ISASecure CSA specific requirements* - This sub section lists additional scheme specific requirements, beyond those derived directly from [ISO/IEC 17065] together with the other documents of the ISASecure CSA 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 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 CSA reference |
|---|---|---|---|
| 4.1.2 *Certification agreement* | 4.1.2.2 h | Certification scheme requirements regarding client references to their certification | [CSA-300] 5.1 requirement C.R3, and [CSA-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 | [CSA-200] 6.6.3.6 |
| 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 a device is certified | Requirements on mechanisms are in [CSA-204], which include updating CSA certificates after supplier SDLA recertification (see CSA.R38) |
| 4.2 *Management of impartiality* | 4.2.10 | Period of time between performing consultancy and certification services | [CSA-200] Requirement CSA.R5 |
| 4.6 *Publicly available information* | 4.6c) | Certification scheme requirements regarding client references to their product certification | [CSA-300] 5.1 requirement C.R3, and [CSA-204] |
| 4.6 *Publicly available information* | 4.6a) | Certification scheme requirements related to granting certification | [CSA-300] |

### 6.2.3  ISASecure CSA specific requirements

This sub section 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 CSA certification scheme.

**Requirement CSA.R1 – Confidentiality for ASCI and ISCI**
The general confidentiality requirement in [ISO/IEC 17065] 4.5.1 SHALL be interpreted to include the requirement that neither ASCI nor ISCI shall 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 EDSA.R2 – Deleted**

**Requirement CSA.R3 – Internal distribution for assessment reports**
Procedures for report distribution internal to the chartered laboratory SHALL limit copies of test and assessment reports only to those that the chartered laboratory determines need the information to fulfill their work responsibilities.

**Requirement CSA.R4 – Public availability of ISCI complaint escalation process**
The [ISO/IEC 17065] requirement 4.6d) in the sub clause 4.6 *Publicly available information* refers to procedures for handling complaints and appeals. This information SHALL include the information about complaints to ASCI/ISCI in 6.5.3.7 of this document.

**Requirement CSA.R5 – Time delay from provision of consultancy**
The [ISO/IEC 17065] requirement 4.2.10 refers to the period of time between personnel having provided consultancy for a product and reviewing or making a certification decision. The minimum time period SHALL be two years.

**Requirement CSA.R6 – Notification of changes to certification requirements**

The chartered laboratory SHALL have processes to keep interested parties informed of changes to certification requirements (such as changes to legal agreements associated with the certification process). Since the supplier must maintain an SDLA certification in order to maintain an existing CSA certification over time, the certification body SHALL inform the holder of a CSA certification regarding changes to the SDLA certification criteria, as also required by the SDLA scheme in [SDLA-200]. The certification body SHALL also inform the supplier of changes to other CSA certification criteria, as these changes will affect certification of upgrades (as defined in 3.1.24) of a certified component in accordance with [CSA-301], so will be required by the supplier for planning purposes.

## 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 scheme references, for [ISO/IEC 17065] requirements in clause 5 of that document that refer to certification scheme requirements.

**Table 2 – Scheme reference for ISO/IEC 17065 clause 5**

| ISO/IEC 17065 sub clause | ISO/IEC 17065 requirement reference | Scheme topic referenced | ISASecure CSA 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 CSA specific requirements

This sub section 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 CSA certification scheme.

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

**Requirement CSA.R7 – Organizational affiliations**

When the separate legal entity as in [ISO/IEC 17065] 4.2.7 is a major user of certified products, the personnel of the separate legal entity shall not be involved in the management of the certification body, the review, or the certification decision.

**Requirement CSA.R8 – Financial affiliations**

The following requirements apply to a chartered laboratory regarding its financial affiliations with suppliers and users of auditable products. The term "auditable product" is defined in 3.1.4. A supplier of auditable products is typically a certification client of the chartered laboratory. However, other organizations could also sell these products, and these cases are covered in this requirement as well.

- A chartered laboratory or a major owner of the chartered laboratory SHALL NOT:

    o provide significant financing to a supplier or to a major user of auditable products;

    o be a major owner of a supplier or of a major user of auditable products;

- A chartered laboratory SHALL NOT:

    o receive significant financing from a supplier or from a major user of auditable products, or their major owners;

      o   have as a major owner, an organization that is a supplier or a major user of auditable products, or a major owner of such an organization;

- A person involved in the management of the certification body, the review, or the certification decision for the chartered laboratory SHALL NOT have a significant financial interest in a supplier or major user of auditable products.

### Requirement CSA.R9 – Chartered laboratory sales and purchases

The following requirements apply to a chartered laboratory regarding its sales and purchase activities:

- A chartered laboratory SHALL NOT have significant sales of any products or services to suppliers of auditable products, other than certification services;

- A chartered laboratory SHALL NOT sell auditable products;

- Prices and agreements related to any products or services that a chartered laboratory purchases from a supplier of auditable products SHALL NOT have dependencies on related 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 CSA reference |
|---|---|---|---|
| 6.1 *Personnel* | 6.1.1.3 | Certification scheme requirements to release information created during an evaluation | [CSA-200]   Requirement CSA.R1 |
| 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 | [CSA-200] 6.4.3.1 |

| ISO/IEC 17065 sub clause | ISO/IEC 17065 requirement reference | Scheme topic referenced | ISASecure CSA reference |
|---|---|---|---|
| 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 | [CSA-200] 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 | [CSA-200] 6.4.3.2 |

### 6.4.3  ISASecure CSA specific requirements

This sub section 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 CSA certification scheme.

#### 6.4.3.1  Personnel qualifications

For the purposes of this section, the term "control system" refers to not only industrial discrete and process control systems, but systems in other domains of cyber-physical control such as building automation, medical devices, and automobiles and encompasses any components (network devices, embedded devices, software applications, host devices) commonly used in a control system.

**Requirement CSA.R10 – FSA-C and SDA-C auditor minimum qualifications**
The [ISO/IEC 17065] requirement 6.1.2.1a) 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. The minimum qualifications for personnel that are responsible for evaluation to FSA-C and SDA-C requirements SHALL include those specified in Table 4.

The level of knowledge required for IEC 62443 as indicated in the last row of Tables 4-5, SHALL at a minimum 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. For the other security standards and practices listed in the table, the level of knowledge required SHALL at a minimum be equivalent to 8 hours of training on the standard or practice.

**Table 4 – FSA-C and SDA-C auditor qualifications**

| Category of qualification / experience | FSA-C auditor | SDA-C auditor |
|---|---|---|
| Formal education | <ul><li>BS Electrical Engineering **OR**</li><li>BS Computer Engineering (CE) **OR**</li><li>BS Computer Science (CS) **OR**</li><li>BS Chemical Engineering with CE or CS minor **OR**</li><li>BS Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR**</li><li>Equivalent science or engineering degree **OR**</li><li>Bachelors or equivalent level degree in other subject, if individual has sufficient experience in computer technology field as specified below **OR**</li><li>Degree as described above, higher than BS **OR**</li><li>Exceed minimum criterion stated below under "Relevant development work experience." Specifically, where a minimum of 4 or 6 years experience is specified there, the individual shall have ten or more years.</li></ul> | <ul><li>BS Electrical Engineering **OR**</li><li>BS Computer Engineering **OR**</li><li>BS Computer Science **OR**</li><li>BS Chemical Engineering with CE or CS minor **OR**</li><li>BS Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR**</li><li>Equivalent science or engineering degree **OR**</li><li>Bachelors or equivalent level degree in other subject, if individual has sufficient experience in computer technology field as specified below **OR**</li><li>Degree as described above, higher than BS **OR**</li><li>Exceed minimum criterion stated below under "Relevant development work experience." Specifically, where a minimum of 4 or 6 years experience is specified there, the individual shall have ten or more years.</li></ul> |
| Professional certification | <ul><li>CISA, CISSP, GICSP, CACE, CACS, or equivalent **OR**</li><li>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.</li></ul> | <ul><li>CISA, CISSP, GICSP, CSSLP, CACE, CACS, or equivalent **OR**</li><li>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.</li></ul> |

| Category of qualification / experience | FSA-C auditor | SDA-C auditor |
|---|---|---|
| Work experience in field | • Minimum four years of work experience in computer technology field, if individual has degree in one of the specific subjects identified above, or has an equivalent science or engineering degree **OR**<br>• Minimum eight years of work experience in computer technology field, if individual has a bachelors or equivalent level degree in other subject<br>• Minimum three years of work experience in computer technology field if individual has Master's Degree in Cybersecurity or equivalent **OR**<br>• Minimum two years of work experience in computer technology field if individual has PhD in Cybersecurity or equivalent | • Minimum four years of work experience in computer technology field, if individual has degree in one of the specific subjects identified above, or has an equivalent science or engineering degree **OR**<br>• Minimum eight years of work experience in computer technology field, if individual has a bachelors or equivalent level degree in other subject **OR**<br>• Minimum three years of work experience in computer technology field if individual has Master's Degree in Cybersecurity or equivalent **OR**<br>• Minimum two years of work experience in computer technology field if individual has PhD in Cybersecurity or equivalent |

| Category of qualification / experience | FSA-C auditor | SDA-C auditor |
| --- | --- | --- |
| Relevant development work experience | • Min 4 year detailed product development involvement for control systems **OR**<br>• Min 4 years of systems integration, commissioning, or maintenance experience for control systems **OR**<br>• Min 3 year detailed product development involvement, systems integration, commissioning or maintenance experience for control systems if individual has Master's Degree in Cybersecurity or equivalent **OR**<br>• Min 2 year detailed product development involvement, systems integration, commissioning or maintenance experience for control systems if individual has PhD in Cybersecurity or equivalent **OR**<br>• Min 6 years system level product test of control systems<br>• Experience includes 2 years with security-related responsibilities **OR**<br>• Same minimums for above activities and security responsibilities for electronic hardware/software non-control systems and pass specified ISCI-approved training **OR**<br>• Other experience requiring interaction with any of these activities for 6 years total with 2 years security responsibilities, and pass specified ISCI-approved training, unless four years involved control systems | • Min 4 years electronic hardware or software development experience for control systems, or for non-control systems and pass specified ISCI-approved training **OR**<br>• Other experience requiring interaction with electronic hardware or software development, integration, commissioning, maintenance for 6 years total with 2 years security responsibilities and 2 years of product development responsibilities, and pass specified ISCI-approved training, unless four years involved control systems<br>• Demonstrates understanding and experience with defining and implementing product lifecycle process improvements<br>• Experience includes 2 years with security-related responsibilities |
| Relevant auditing work experience | • Min 1 year experience performing technical product audit **OR**<br>• 2 years in position with significant role in interaction with auditors **OR**<br>• Min 3 years experience performing cybersecurity audit (organizational) **OR**<br>• Min 3 years in position in organization which has been audited for cybersecurity, with significant role in interaction with auditors **OR**<br>• Industry-recognized training in IT cybersecurity auditing **AND**<br>• Pass specified ISCI-approved training, if qualifying based on organizational audit or IT audit training | • Min 1 year experience performing software process audit OR 2 years in position with significant role in interaction with auditors |

| Category of qualification / experience | FSA-C auditor | SDA-C auditor |
|---|---|---|
| Relevant industry specific knowledge | • General knowledge of at least two different control systems or pass specified ISCI approved training **AND**<br>• General knowledge of application of control systems and roles and duties of employees at sites using control systems or pass specified ISCI approved training **AND**<br>• Moderate level knowledge of networking and communication protocols **AND**<br>• Able to independently read and interpret requirement specifications for control systems products, or for other computer technology products and pass specified ISCI approved training **AND**<br>• Able to independently read and understand user installation and configuration documents for control systems products, or for other computer technology products and pass specified ISCI approved training **AND**<br>• Knowledge of methods used to protect communications and detect / prevent communication attacks | • General knowledge of end-end electronic hardware or software development life cycle **AND**<br>• General knowledge of control systems architectures or pass specified ISCI-approved training |
| Knowledge of security standards | • IEC 62443 Standard plus at least one of:<br>   ○ Common Criteria<br>   ○ ISO/IEC 27001<br>   ○ IEC 61508 **AND**<br>• If have not met a cybersecurity experience requirement under professional certification, also pass specified ISCI-approved training. | • IEC 62443 Standard plus at least one of:<br>   ○ Common Criteria<br>   ○ ISO/IEC 27001<br>   ○ IEC 61508 **AND**<br>• If have not met a cybersecurity experience requirement under professional certification, also pass specified ISCI-approved training. |

If the individual meets all qualifications for an auditor 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 lists shown in the 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 chartered lab SHALL plan and monitor the individual's progress toward a full professional certification equivalent to one on the specified lists. 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 If a candidate for auditor meets all qualifications in a column of Table 4 or Table 5 that use the term "control systems," then GICSP or a similar control-system focused professional certification is recommended.

**Requirement EDSA.R11 – Deleted**

**Requirement CSA.R11 – Chartered laboratory requirement for personnel with full professional certifications**

Two years after a chartered laboratory receives initial CSA accreditation, all CSA certification evaluations toward CSA certificates issued by the chartered laboratory SHALL be performed under the technical oversight of individuals holding a relevant professional certification as specified in the second row of Table 4 or Table 5.

NOTE    The requirements CSA.R10 and CSA.R12 imply that a chartered laboratory may initiate certification operations before their auditors/evaluators have met the experience requirement for a full professional certification listed under those requirements. CSA.R11 requires that ultimately, lead auditors/evaluators must meet these experience requirements and fully achieve one of these professional certifications.

**Requirement CSA.R12 – VIT-C lead evaluator minimum qualifications**

The [ISO/IEC 17065] requirement 6.1.2.1a) 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. The minimum qualifications for personnel that that are responsible for the technical aspects of V IT testing and interpretation of results shall include those specified in Table 5.

**Table 5 – VIT-C lead evaluator qualifications**

| Category of qualification / experience | VIT-C lead evaluator |
|---|---|
| Formal education | • BS Electrical Engineering **OR**<br>• BS Computer Engineering **OR**<br>• BS Computer Science **OR**<br>• BS Chemical Engineering with CE or CS minor **OR**<br>• BS Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR**<br>• Equivalent science or engineering degree **OR**<br>• 4 years work experience in testing of control systems may be substituted for degree<br>• 4 years work experience in known vulnerability testing may be substituted for degree |
| Professional certification | • CISA, CISSP, GICSP, CACE, CACS, or equivalent **OR**<br>• For individuals that meet all other qualifications for this role, 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 4 for details. |
| Work experience in field | • Min 4 years work experience in computer technology field |
| Relevant development work experience | • Min 4 year detailed product development involvement for computer technology systems **OR**<br>• Min 4 years of systems integration, commissioning, or maintenance experience for computer technology systems **OR**<br>• Min 3 years System Level Product Test for computer technology systems<br>• Experience includes 1 year with software security-related responsibilities<br>• Experience includes 2 years involvement with networking technologies |
| Relevant test work experience | • Min 1 year experience performing testing on computer technology systems |
| Relevant industry specific knowledge | • Successful completion of training class or 1 year experience in job demonstrating proficiency with VIT tool to be used **AND** |

| Category of qualification / experience | VIT-C lead evaluator |
|---|---|
| | • Moderate level knowledge of networking and communication protocols **AND**<br>• Able to independently read and understand user installation and configuration documents for control systems products |
| Knowledge of security standards | IEC 62443 Standard plus at least one of:<br>• Common Criteria<br>• ISO/IEC 27001<br>• IEC 61508 |

**Requirement CSA.R13 – Currency of skills and knowledge**

Staff training SHALL BE kept up-to-date and staff SHALL keep up-to-date of current normative specification issues (includes participation in technical groups or committees).

### 6.4.3.2 Other standards

The [ISO/IEC 17065] requirements 6.2.1 *Internal resources* and 6.2.1 *External resources* in the sub clause 6.2 *Resources for evaluation* refer to compliance with applicable requirements in ISO/IEC 17025, 17020, and 17021. Accreditation to ISO/IEC 17025 is required for a CSA chartered laboratory. Requirements from ISO/IEC 17020 which apply to inspection activities, have been adapted and incorporated in this document as follows and hence are noted but not repeated here:

**Table 6 – ISO/IEC 17020 requirements specified**

| ISO/IEC 17020 requirement | Topic | CSA-200 requirement |
|---|---|---|
| 6.1 6c | Continuing training | CSA.R13 |
| 7.4.2 | Test and assessment records<br><br>("Inspection records" in 17020) | CSA.R31 |

## 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.

**Table 7 – Scheme reference for ISO/IEC 17065 clause 7**

| ISO/IEC 17065 sub clause | ISO/IEC 17065 requirement reference | Scheme topic referenced | ISASecure CSA reference |
|---|---|---|---|
| 7.1 *General* | 7.1.1 | Certification scheme used by a CSA chartered laboratory | Defined in [CSA-100] |
| 7.1 *General* | 7.1.2 | Refers to normative documents against which a component is evaluated | For initial certifications, documents are [CSA-300] and its normative references; for products with a version previously certified, documents are [CSA-301] and its normative references; [CSA-200] CSA.R18 specifies current versions of these documents |
| 7.1 *General* | 7.1.3 | Person or committee to provide explanations per application of normative documents | ISCI Technical Steering Committee, as stated in [CSA-200] requirement CSA.R14 |

| ISO/IEC 17065 sub clause | ISO/IEC 17065 requirement reference | Scheme topic referenced | ISASecure CSA reference |
|---|---|---|---|
| 7.2 *Application* | 7.2 | Information that scheme requires for client application | [CSA-300] 5.1 and 5.2 requirements C.R1, R2 and R4 in for initial certification; requirements for products with a version previously certified are in [CSA-301] |
| 7.4 *Evaluation* | 7.4.4 | Evaluation of device to scope of certification and requirements specified in scheme | Certification requirements for initial certification are listed in [CSA-300] requirement C.R5; certification requirements for products with a version previously certified are in [CSA-301] |
| 7.4 *Evaluation* | 7.4.9 Note 2 | Whether certification scheme requires certification body to perform evaluation under its responsibility after application | Yes, per [CSA-300] 5.2 |
| 7.7 *Certification documentation* | 7.7.1 f | Information scheme requires on the document signifying certification | Certificate format and content specified in [CSA-204] and [CSA-205] |
| 7.8 *Directory of certified products* | 7.8 last paragraph | Information about certified products made available to a directory | [CSA-200] 6.5.3.3 |
| 7.9 *Surveillance* | | | Not applicable, see [CSA-200] 6.5.3.4 |
| 7.10 *Changes affecting certification* | 7.10.1 | Actions required by scheme for changes to certification criteria | [CSA-200] Inform clients per CSA.R6, update processes per CSA.R18 |
| 7.11 *Termination, reduction, suspension or withdrawal of certification* | 7.11.3 | Actions required when a certification is terminated, suspended or withdrawn | For withdrawal and termination, see [CSA-200] 6.5.3.6. Other actions are not defined for CSA certification |

| ISO/IEC 17065 sub clause | ISO/IEC 17065 requirement reference | Scheme topic referenced | ISASecure CSA reference |
|---|---|---|---|
| 7.11 *Termination, reduction, suspension or withdrawal of certification* | 7.11.4, 7.11.5 | Scheme requirements related to suspension | Not applicable. Suspension is not defined for CSA certification |
| 7.12 *Records* | 7.12.3 | Whether scheme requires complete re-evaluation of product on a predetermined cycle | No, as explained in [CSA-200] 6.5.3.4 |

### 6.5.3 ISASecure CSA specific requirements

This sub section 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 CSA certification scheme.

#### 6.5.3.1 Application

#### 6.5.3.1.1 Process requirements

**Requirement CSA.R14 – Determining application of specifications**
The [ISO/IEC 17065] requirement 7.1.3 in clause 7 Process *requirements* refers to persons or committees who provide the chartered laboratory with explanations as to the application of the ISASecure specifications. This role SHALL be fulfilled by the ISCI Technical Steering Committee.

**Requirement CSA.R15 – Determining applicant eligibility**
The chartered laboratory SHALL be responsible for determining whether a product presented by a potential client meets the scope for a CSA certification, and which component type(s) apply to the product (software application, embedded device, host device, network device). The chartered laboratory MAY request guidance from ISCI in this matter. If the client does not concur with the decision of the chartered laboratory, they MAY use the compliant escalation process described in Requirements CSA.R41 and CSA.R42.

#### 6.5.3.1.2 Content of procedures

**Requirement CSA.R16 – Application steps procedure**
Procedures for processing a certification application SHALL identify the steps for the application, administrative/technical processing of the investigation in chronological order, personnel responsible for each stage of the process, and records maintained at various steps of the process.

**Requirement CSA.R17 – Maintenance of procedure for application**
Procedures for developing and maintaining 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  General Process requirements

**Requirement CSA.R18 – Current ISASecure specifications**

[ISO/IEC 17025] 7.2.1.3 on selection of test methods, specifies using the latest valid version of the standards upon which tests are based, where appropriate. The appropriate versions of ISASecure specifications to use for a certification SHALL be identified in accordance with transition policies and specification listings found on the ISASecure web site at http://www.ISASecure.org.

**Requirement EDSA.R19 – Deleted**

**Requirement EDSA.R20 – Deleted**

**Requirement CSA.R21 – VIT-C report**

Detailed reporting on VIT-C results for a component SHALL be carried out in accordance with the requirements on VIT-C reporting in the technical specification for VIT-C, which is listed in the normative references for [CSA-300].

**Requirement CSA.R22 – Assessment report**
The [ISO/IEC 17065] requirement 7.4.9 in sub clause 7.4 *Evaluation*, refers to documentation of evaluation results prior to review. This documentation SHALL at a minimum include an assessment report following the content and format of [CSA-303], the CSA assessment report sample. A report following this template SHALL also be provided to the client.

#### 6.5.3.2.2  Deleted

**Requirement EDSA.R23 – Deleted**

**Requirement EDSA.R24 – Deleted**

**Requirement EDSA.R25 – Deleted**

**Requirement EDSA.R26 – Deleted**

**Requirement EDSA.R27 – Deleted**

#### 6.5.3.2.3  Content of procedures

**Requirement CSA.R28 – Equipment calibration**
Persons responsible for the calibration of equipment (where applicable) and authorized to perform each type of calibration SHALL be identified. Records for each calibration SHALL contain sufficient information to permit their repetition.

**Requirement CSA.R29 – Content of test or assessment methods or procedures**
Each test or assessment method or procedure SHALL have sufficient detail instructions that assure reasonable repeatability of the test or assessment and include or address the: title, effective date, assessment or test data to be obtained and recorded, objective acceptance criteria for results, test or assessment techniques, where additional information to that required by the CSA technical specifications is required to meet these goals. In addition, test procedures SHALL include or address: specific test equipment to use and instructions for handling the equipment.

**Requirement EDSA.R30 – Deleted**

**Requirement CSA.R31 – Content of test or assessment data sheet**
Each test or assessment data sheet or similar document SHALL include the test or assessment procedure and specification used, date of the test or assessment, test or assessment report number, signature of the personnel performing the test or assessment, and test or assessment results. In addition, test data sheets shall include the product or component tested and test equipment used.

**Requirement CSA.R32 – Content of procedure maintenance procedures**
Procedures for developing and maintaining test or assessment methods and procedures SHALL identify the personnel 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 product, component or process conforms with the specification, and ensure modifications are reviewed by personnel who are familiar with the specification.

**Requirement CSA.R33 – Content of procedures for evaluating test or assessment data**
Procedures for evaluating test or assessment data SHALL require the investigator to: verify and use a latest appropriate specification edition (per CSA.R18), provide written justification of how a product, component or process complies with each section of the specification (including a reference to a test or assessment procedure), and address components not listed by the supplier.

**Requirement CSA.R34 – Content of policy for evaluation of test or assessment data**
Policies on evaluation of test or assessment data 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 investigators; and require the resolution of product, component or process discrepancies without the laboratory engaging in the redesign, except to explain the failures in regard to the ISASecure specification.

**Requirement CSA.R35 – Content of procedures for preparing technical reports**
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 test and evaluation procedures; and

- Ensure that technical corrections involve qualified personnel.

### 6.5.3.3  Directory of certified products

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

**Requirement CSA.R36 – Input to scheme directory**
With permission of the certification client, the chartered laboratory SHALL inform ISCI of each certification granted and provide a copy of the certificate, to support ISCI's central directory of ISASecure certifications.

**Requirement CSA.R37 – Accuracy of certification status**
Proper controls SHALL be in place to assure accuracy of information on the certificate and in chartered laboratory records of certified entities.

### 6.5.3.4  Surveillance

The ISASecure CSA certification scheme does not require surveillance, where that term refers to inspection of samples of actual shipped product for compliance with certification requirements. ISCI does not require a

chartered laboratory to verify periodically that components shipped by the supplier that are labeled with a version number that has been certified, are in fact that version. However, ISO/IEC 17065 requires that the chartered laboratory monitor the use of the ISASecure symbol. This includes proper symbol use as it relates to product version. Certification of updated and upgraded product versions (as defined in 3.1.23 and 3.1.24), and certification to updated ISASecure versions, are covered in [CSA-301]. As required by CSA.R38 and described in [CSA-301], maintaining CSA certification for updates of a certified product requires maintenance by the supplier of a SDLA process certification, which in turn requires periodic recertification audits under the SDLA scheme, as described in [SDLA-300].

### 6.5.3.5  Deleted


### 6.5.3.6  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 and suspension are not defined for CSA certification. The following requirements apply to withdrawal and termination.

#### Requirement CSA.R38 – Withdrawal or termination of certification
An ISASecure product certification SHALL be withdrawn if any of the following conditions for validity of the certificate are NOT met:

- The product remains in a support status such that an SDLA certified SDL process still applies to the product;

- The supplier retains their SDLA certification, or if their SDLA certification is lost, reinstates it within a year grace period; AND

- The supplier participated in good faith in the certification process.

The certification body SHALL terminate the certification if the supplier reports to them that the product has left support status under the certified SDL process, or if the supplier otherwise requests termination of the certification for any reason.

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 CSA.R39 – Notification of withdrawal or termination of certification
The chartered laboratory SHALL inform ISCI of any withdrawal or termination of an ISASecure product certification at the time it occurs.

### 6.5.3.7  Complaints and appeals

The [ISO/IEC 17065] requirement 7.13.1 under 7.13 *Complaints and appeals*, refers to the certification body process related to complaints and appeals.

#### Requirement CSA.R40 – Complaints regarding evaluations or certifications

A chartered laboratory SHALL be responsible for managing the resolution of complaints related to any aspect of compliance for a product it evaluated or certified.

#### Requirement CSA.R41 – Escalation for complaints and appeals
The published chartered laboratory process for handling complaints SHALL include the provision that complaints may be appealed to ISCI by the party bringing the complaint, if the internal chartered laboratory 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 CSA.R42 – Escalation for complaints and appeals related to application of specifications**
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 certification process is applicable to a particular product that has applied for certification;

- Whether or not a certification was granted; or

- Adequacy of the product evaluation process by the chartered laboratory.

NOTE Neither ISCI nor ASCI accept certification applications, nor process, grant, or revoke certifications. This is the role of a chartered laboratory. ISCI can assist in interpretation of the ISASecure 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 comply with 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 comply with ISO 9001 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] Section 8 refer to scheme specific requirements.

### 6.6.3 ISASecure CSA specific requirements

This sub section 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 CSA certification scheme. They apply whether the chartered laboratory elects Option A or Option B to fulfill the management system requirements.

### 6.6.3.1  General management system documentation

#### Requirement CSA.R43 – Scope of procedures under management system
Chartered laboratory procedures SHALL cover the entire "quality loop" from application for services to final assessment or listing of certification status, including follow-up services.

#### Requirement CSA.R44 – Responsibility for quality
The chartered laboratory 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 CSA.R45 – Housekeeping
Adequate measures SHALL be taken to ensure good housekeeping at the chartered laboratory facilities where evaluation activities are performed.

#### Requirement CSA.R46 – Item inventory
Laboratory procedures for handling of artifacts, or customer or laboratory equipment to be tested or used in tests, SHALL address item inventory.

#### Requirement CSA.R47 – Facility security
Chartered laboratory measures and procedures related to security SHALL include provisions for: controlling access, off hours security, and fire protection for the facility; informing all personnel 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 CSA.R48 – Processing for revisions to normative specifications
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 CSA.R49 – Archival of superseded specifications
Superseded normative specifications SHALL be archived.

### 6.6.3.3  Control of records

#### Requirement CSA.R50 – Maintenance of records
Records maintained for evaluation 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 CSA.R51 – Management follow-up review for deficiencies
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 CSA.R52 – Basis for internal audits**
Internal quality audit policies and procedures SHALL specify the basis for conducting audits.

**Requirement CSA.R53 – Contents included in internal audit reports**
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 CSA.R54 – Internal audits of satellite facilities**
QA 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 CSA.R55 – Implementation for permanent corrective actions**
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 suppliers of CSA certified products

**Requirement CSA.R56 – Supplier process for disclosure of complaints related to noncompliance**
A chartered laboratory 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 compliance with ISASecure product certification requirements, that are found per [ISO/IEC 17065] 4.1.2.2j. These requirements address handling and disclosure to the chartered laboratory of such complaints known to the certified organization, to the chartered laboratory.

The intent of the following broader provision is to improve the ISASecure product certification programs.

**Requirement CSA.R57 – Supplier process for disclosure of complaints related to security of ISASecure certified product**
The signed agreement between the chartered laboratory and the client SHALL include the following provision. Any complaint regarding its certified product that is known to the supplier organization and that is determined to affect product security shall be brought to the attention of the chartered laboratory that granted the product certification.  The laboratory shall evaluate the impact on the product conformance to the ISASecure CSA requirements.

**Requirement CSA.R58 –  Disclosure to ISCI of complaints related to ISASecure certified product**
The chartered laboratory process for handling a report under Requirement CSA.R57 SHALL include a process to advise ISCI if a modification to the ISASecure specifications should be considered based upon this event. This process SHALL be contingent upon approval from the client making the report, to disclose to ISCI any information concerning their product, whether or not it is attributed to their product.

## 7  Accreditation of chartered laboratories

### 7.1  Overview

Accreditation of a chartered laboratory involves an assessment of the organization against the requirements in the following documents:

- ISO/IEC 17065 [ISO/IEC 17065]

- ISO/IEC 17025 [ISO/IEC 17025 2005], updated to [ISO/IEC 17025]

- Section 6 this document, all ISASecure specific requirements subsections

- Section 7 of this document, which describes technical readiness assessment.

Technical readiness assessment is based upon review of documented laboratory processes and procedures as well as review of artifacts from sample audits carried out by the laboratory on a component, as described in Section 7.3. To be recognized as a chartered laboratory for the ISASecure CSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC recognized accreditation body:

- Accredited to IAF ISO/IEC 17065, with technology scope of accreditation covering ISASecure CSA certification; and

- Accredited to ISO/IEC 17025, with technology scope of accreditation covering ISASecure CSA FSA-C and VIT-C specifications.

This internationally recognized accreditation shall be obtained by a laboratory within 18 months of obtaining a provisional chartered laboratory status, as described in Section 5. The following section discusses requirements for attaining provisional chartered laboratory status.

## 7.2  Provisional chartered laboratory status

Provisional chartered laboratory status allows an organization to begin certification activities before accreditation has been formally granted by a CSA accreditation body. Formal granting of the accreditation can occur several months after the evaluation of the laboratory has taken place and results submitted by the evaluators to the board within the CSA accreditation body that makes the final accreditation decision.

ASCI will grant a laboratory provisional chartered status based on the results of an evaluation of the laboratory by qualified assessors for ISO/IEC 17065 and ISO/IEC 17025.   Provisional chartered status is granted if the evaluation shows that the organization complies with:

- All ISO/IEC 17065 and ISO/IEC 17025 requirements;

- All numbered ISASecure specific requirements in the present document; and

- Those technical readiness criteria in Table 8 that may be verified based upon process and procedure documentation evidence. These criteria are in rows 1-3 Table 8.

The accreditation body will assess the remaining technical readiness criteria once the chartered laboratory is operating and has examples of product evaluation results available.

The evaluation for a candidate chartered laboratory is performed by an assessor that has been qualified by an IAF/ILAC recognized accreditation body. A candidate organization shall apply for accreditation as required by the accreditation body. A candidate chartered laboratory also applies to ASCI using the form [ISASecure-202]. "Provisional" chartered laboratory status is a term applied by ASCI/ISCI within the ISASecure program and is not recognized or managed by the accreditation body.

During the period when a chartered laboratory is operating in provisional status, ASCI shall be made aware of the laboratory's expectations for receipt of formal internationally recognized accreditation by an IAF/ILAC organization. ASCI shall have the option to perform an interim review and update its evaluation for provisional status of the chartered laboratory 6 months after it is received. Once a chartered laboratory has achieved accreditation by an IEC 17011 accreditation body, that accreditation body determines the requirements and frequency for maintenance audits to maintain accredited status.

## 7.3 Technical readiness assessment

The technical readiness assessment for CSA accreditation focuses on SDA-C, FSA-C, and VIT-C. The evaluation consists of assessment of evidence supplied by the candidate laboratory per the evaluation criteria in Table 8. The requirements numbered VIT-C.Rnn or VIT.Rnn are from [SSA-420].

**Table 8 – Evidence for technical readiness**

| ID | Evidence supplied by candidate laboratory | Evaluation criteria |
|---|---|---|
| 1 | Organization statement of test tool and version in use for VIT-C | • ISCI-specified tool is in place as specified for VIT per VIT-C.R1 |
| 2 | VIT-C processes/procedures | • Comply with VIT-C.R2 and on VIT testing configuration<br><br>• Comply with VIT-C.R3 regarding the Nessus policy to be used and modes of the product to be tested<br><br>• Comply with VIT-C.R4 on interfaces to test under VIT-C<br><br>• Comply with VIT-C.R5 on criteria for VIT-C pass<br><br>• Instructions for VIT evaluation report creation comply with VIT.R14-23 |
| 3 | Application form and instructions to be given to suppliers submitting components | • Application requests all items required per [CSA-300] Requirement ISASecure_C.R4 |
| 4 | Intermediate artifacts, paperwork and final evaluation report for a sample component covering SDA-C, FSA-C, and VIT-C. | • SDA-C artifacts were obtained as required by specifications<br><br>• Results of FSA-C indicate compliance with procedures and specifications<br><br>• Report from VIT-C evaluation indicates use of tool version and set of known vulnerabilities specified by [SSA-420]<br><br>• Report from VIT-C evaluation indicates compliance with pass/fail criteria in VIT-C.R5<br><br>• Evaluation report and detailed VIT-C report meet requirements CSA.R21 - R22 in this document<br><br>• Evidence meets CSA.R31 in this document |
| 5 | Evidence demonstrating that the vulnerability identification test result can be reproduced based on information in evaluation report; document steps used to reproduce these | • Verify that steps for creation of reproduced result required only information in the evaluation report; and that results are same as initial results |