SSA-200

ISA Security Compliance Institute – System Security Assurance –

ISASecure® SSA chartered laboratory operations and accreditation

Version 2.9

February 2022

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	2014.02.09	Initial version published to http://www.ISASecure.org
1.9	2015.02.24	Change from Guide 65 to 17065, incorporate ASCI 2009 requirements directly, add figure 1, change SDLA to SDLPA when used for assessment, permit GICSP in qualifications, full software version required on CRT reports SSA.R19, CRT tool calibration not required SSA.R28
2.5	2018.02.02	Alignment with approved ANSI/ISA-62443-4-1: update references, background section, replace section 5.3 with discussion of transition to SSA 2.1.0; explicitly support scalable systems: add definitions of layout, reference layout, reference system, scalable system, modify 4.1 scope, add scalability topics to technical readiness assessment; add CACE and CACS as certifications for auditors and permit any bachelor-level degree with sufficient industry experience; incorporate errata from SSA-102 v1.6
2.6	2018.08.10	Alignment with ISA-62443-4-2: update normative references; in 4.1 modify sentence about FSA-E
2.8	2019.08.18	Update along with transition from EDSA to CSA: change device to component in 4.1 and elsewhere; remove certifier CRT, CRT lab, and tools; remove certifier NST; remove FSA-E; remove figure 1; update material related to maintenance of certification; 17025 scope includes FSA-S testing; discuss transition to SSA 4.0.0; add latest version of 17011
2.9	2022.02.01	Revisions to 6.4.3.1 personnel qualifications to support substitution of training for some qualifications and increase flexibility of education and experience requirements; add SSA.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 ISASecure® certification for control systems, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). Certifications available include ISASecure Component Security Assurance (CSA) for software applications, embedded devices, host devices and network devices, ISASecure System Security Assurance (SSA) for systems, and ISASecure Security Development Lifecycle Assurance (SDLA) which addresses control system supplier development processes. This specification is one of the series of documents that describes requirements for ISASecure SSA certification. The current list of documents related to ISASecure certification programs can be found on the web site http://www.ISASecure.org.

1 Scope

The ISASecure® certification program has 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 SSA (System Security Assurance) program for control systems is referred to as an *ISASecure SSA 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 SSA system certification operations (Section 7).

ISCI has based its certification program approach on:

- International standards for conformity assessment programs; and
- IACS security standards IEC 62443-3-3 and IEC 62443-4-1 (also published as ANSI/ISA standards); and
- Specifications developed for the ISASecure SSA program.

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

ISCI also has developed certification programs for:

- Software applications, embedded devices, host devices, and network devices, under the ISASecure CSA program (Component Security Assurance); and
- Supplier secure product development lifecycle process for control systems and components, the ISASecure SDLA program (Security Development Lifecycle Assurance).

The separate documents CSA-200 *ISASecure CSA 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 CSA and SDLA certifications, respectively.

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

2 Normative references

2.1 General

NOTE The following is the highest level document that describes the ISASecure SSA certification program for control systems.

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

2.2 Accreditation

2.2.1 Chartered laboratory operations and accreditation

[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

2.3 ISASecure symbol and certificates

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

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

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

2.4 Technical specifications

NOTE This section includes the specifications that define technical criteria for evaluating a system for ISASecure SSA certification.

2.4.1 General technical specifications

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

[SSA-300] *ISCI System Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

[SSA-301] *ISCI System Security Assurance – Maintenance of ISASecure Certification,* as specified at http://www.ISASecure.org

[SSA-303] *ISASecure SSA 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 Functional Security Assessment element of an SSA evaluation.

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

NOTE 2 The following document provides the overall technical evaluation criteria for the Security Development Artifacts element of an SSA product evaluation. [SDLA-312] is referenced by [SSA-312] and also provides the technical evaluation criteria for an ISASecure SDLA assessment of a supplier's development lifecycle process.

[SSA-312] *ISCI System Security Assurance – Security development artifacts for systems,* 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 3 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier secure product development lifecycle processes. [SDLA-100] also lists all other documentation for the SDLA program.

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

2.4.3 Vulnerability identification testing specification

NOTE The following document describes the procedures and the policy parameter values used to perform Vulnerability Identification Testing (VIT-S) for a system.

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

2.5 External references

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

2.5.1 IACS security standards

NOTE [SSA-100] describes the relationship of ISASecure 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-62443-3-3] 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*

[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*

2.5.2 International standards for certification programs

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

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

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

[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 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 ISASecure certification programs, accreditation is an assessment and recognition process via which an organization is granted chartered 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

security level that a component or system can provide when properly configured and integrated

NOTE This type of security level states that a particular component or system is capable of meeting a target security level natively without additional compensating countermeasures when properly configured and integrated.

3.1.6
certification body

third-party conformity assessment body operating certification schemes

3.1.7
certification level

capability security level for which conformance is demonstrated by a certification

NOTE An SSA certification for a particular security zone may be SSA capability security level 1, 2, 3, or 4. A zone certified to SSA capability security level *n* meets requirements for capability security level *n* as defined in the standard [IEC 62443-3-3].

3.1.8
certification scheme

certification system related to specific products, processes, or services, to which the same specified requirements, specific rules and procedures apply

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 certification body for the ISASecure certification programs.

3.1.10
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

3.1.11
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.

3.1.12
control system

hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.13
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.

3.1.14
evidence impact assessment

identification of that portion of the evidence from the certification evaluation of a product, which may be applied toward the certification of a modified version of the product, and of those aspects of the evaluation which must be performed on the modified product and new evidence created

3.1.15
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.).

3.1.16
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

3.1.17
layout

description of a specific instance of a scalable control system, that defines quantities of zones and resident components, and internal and external interfaces

3.1.18
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.

3.1.19
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

3.1.20
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.

3.1.21
reference layout

specific layout for scalable control system, that represents security characteristics found in any layout to be SSA certified, in a manner suitable to support security testing that provides assurance for all such layouts

NOTE A reference layout may be neither the minimum nor the maximum layout for a scalable system. Its properties are specified in requirements found in [SSA-300]. In overview, the reference layout for a control system includes all zones, resident components in these zones, interfaces and protocols present in any layout in scope for a certification.

3.1.22
reference system

physical instance of a control system, that adheres to a reference layout

NOTE A reference system is used for some types of security testing performed by the system supplier and certifier.

3.1.23
scalable control system

control system which supports replication of zones and/or components to support small and large installations

3.1.24
significant financing

financing that is material to the operations of the recipient

3.1.25
significant financial interest

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

3.1.26
significant sales

sales that are material to the operations of the seller

3.1.27
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.

3.1.28
security zone

grouping of logical or physical assets that share common security requirements

NOTE A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

3.1.29
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.

3.1.30
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is "mark."

3.1.31
system
control system

NOTE In the ISASecure SSA documentation, this shorter term is used for convenience to refer to a control system product that may fall under the scope of ISASecure SSA certification. Per the definition above, control systems include safety systems.

3.1.32
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues

3.1.33
upgrade
incremental hardware or software change in order to add new features

3.1.34
zone
security zone

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
CSA	Component Security Assurance
CE	computer engineering
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CS	computer science
CSSLP	Certified Secure Software Lifecycle Professional
DCS	distributed control system
CSA	component security assurance
FSA-S	functional security assessment for systems
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
NA	not applicable
OS	operating system
PLC	programmable logic controller
SDA-S	security development artifacts for systems
SDLA	security development lifecycle assurance
SIS	safety instrumented system
SSA	system security assurance
SY	system
VIT-S	vulnerability identification testing for systems

4 Background

4.1 Technical ISASecure SSA certification elements

ISASecure SSA is a certification program for control systems, where a control system product is considered to be within the scope of this program if it satisfies all of the following criteria:

- The control system consists of an integrated set of components and includes more than one component.

- The control system is available from and supported as a whole by a single supplier, although it may include hardware and software components from several manufacturers.

- The control system may have a fixed component and zone layout, or may be scalable, that is, may permit replication of components and of zones in order to scale for small and large installations.

- The system product is under configuration control and version management.

In order to obtain ISASecure SSA certification, a supplier must hold an ISASecure SDLA development process certification, as described in [SDLA-100], such that the system to be evaluated is in the scope of that process.

A supplier may apply for ISASecure SSA and SDLA certifications in parallel.

ISASecure SSA certification for systems has three additional elements:

- Security Development Artifacts for systems (SDA-S);

- Functional Security Assessment for systems (FSA-S); and

- Vulnerability Identification Testing for systems (VIT-S).

Both the SDLA certification evaluation and SDA-S assess development process. SDLA certification demonstrates that the supplier has a documented secure product software development lifecycle process, that it is compliant with [IEC 62443-4-1], and that there is evidence the process is followed. SDA-S examines the artifacts that are the outputs of the supplier's development lifecycle processes as they apply to the system to be certified. FSA-S examines the security capabilities of the system. Vulnerability Identification Testing (VIT-S), scans all components of a system for the presence of known vulnerabilities.

A system submitted for certification is comprised of one or more security zones. The supplier identifies a certification level for each zone, which will be the desired capability security level to be demonstrated for that zone by the certification. The SDLA certification does not have an associated level. The SDA-S and VIT-S assessments are the same for all capability security levels with the exception of allowable residual risk for known security issues. The FSA-S evaluation is applied to each security zone; required security capabilities will differ based upon the zone capability security level. The ISASecure SSA certificate for a system will name its security zones and the capability security levels to which they have been certified.

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

For scalable systems, tests performed by the certifier as part of FSA-S or VIT-S will be performed on a reference system, whose layout meets criteria specified in [SSA-300]. Analyses performed by the certifier will take into account all layouts to be evaluated under the certification. In addition to requirements for initial certification, ISASecure SSA specifies requirements for maintaining certification when a certified system and/or ISASecure criteria are modified, as described in [SSA-301].

4.2 ISASecure SSA 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 ISASecure SSA chartered laboratories are organizations that are accredited to evaluate systems under the ISASecure SSA program. ASCI grants accredited laboratories the right to process ISASecure SSA certifications for systems on its behalf and issue certificates for systems meeting the SSA certification requirements. System certification is determined based upon tests, functional audits and process audits, which measure adherence to the ISASecure SSA requirements. Evaluations for all SSA certification elements described in 4.1 are conducted directly by the chartered laboratory or its subcontractors.

The list of ASCI ISASecure SSA chartered laboratories is posted on the ISCI website at http://www.ISASecure.org. At the request of system suppliers, systems that are issued certifications are registered on this same ISCI website.

The ISASecure SSA program requires chartered laboratories to use the Nessus® tool (http://www.tenable.com/products/nessus) for performing the VIT-S element of SSA certification. Nessus may also be used by suppliers in preparation for certification.

5 Summary of operations and accreditation requirements

5.1 Overview

ISASecure SSA 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 SSA 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], the international standard that applies to test organizations.

The present document is organized using the outline of [ISO/IEC 17065]. Where required, it interprets requirements in that document for ISASecure SSA 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 organizations (6.5.3.3);
- Appeals for client complaints (6.5.3.7); and
- Managing complaints to suppliers of 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 SSA evaluations, described in Section 7.3. Technical readiness assessment is based upon review of laboratory processes and procedures as well as review of artifacts from evaluation activities. To be recognized as a chartered laboratory for the ISASecure SSA 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 SSA certification; and
- Accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure SSA FSA-S and VIT-S 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 listed in 7.2 of the present document that may be verified based upon process and procedure documentation evidence. 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 system evaluations and grant ISASecure SSA certifications. These rights continue as long as the laboratory receives formal accreditation from an SSA accreditation body in a timely manner (the second step) and maintains this status.

5.3 Transition to SSA 4.0.0

As of the publication of this document, the current version of the SSA program is 4.0.0. SSA 4.0.0 requires deeper and broader technical audit of supplier robustness testing practices, and removes the requirements for FSA-E (functional security assessment based upon [IEC 62443-4-2]) for each embedded device that is a system component, as well as certifier-performed testing previously known as SSA CRT (communication robustness testing) and NST (network stress testing). Accordingly, ISCI has defined a policy for chartered laboratories to follow in transitioning certification activities from SSA 3.0.0 to SSA 4.0.0. This policy is defined in the document [ISASecure-117].

SSA 4.0.0 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 the SDLA program is needed or described in [ISASecure-117]. This is because the update to [SDLA-312] required for the SSA 4.0.0 program, modifies material in [SDLA-312] that defines certifier validations for the element Security Development Artifacts for systems (SDA-S) of SSA 4.0.0, 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 SSA chartered laboratories. It provides specific interpretations for ISO/IEC 17065 requirements, and defines further requirements that are specific to the ISASecure SSA 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:

  - *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 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 SSA scheme where the relevant scheme requirements are found. These references may refer to ISASecure SSA 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.

- *ISASecure SSA 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 SSA 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 SSA reference
4.1.2 *Certification agreement*	4.1.2.2 h	Certification scheme requirements regarding client references to their certification	[SSA-300] 5.2 requirement SY.R5, and [SSA-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	[SSA-200] 6.6.3.6

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure SSA reference
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 product is certified	Requirements on mechanisms are in [SSA-204]
4.2 *Management of impartiality*	4.2.10	Period of time between performing consultancy and certification services	[SSA-200] Requirement SSA.R5
4.6 *Publicly available information*	4.6c)	Certification scheme requirements regarding client references to their certification	[SSA-300] 5.2 requirement SY.R5, and [SSA-204]
4.6 *Publicly available information*	4.6a)	Certification scheme requirements related to granting certification	[SSA-300] for initial certification, and [SSA-301] for maintenance of certification

6.2.3 ISASecure SSA 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 SSA certification scheme.

Requirement SSA.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 SSA.R2 – Deleted

Requirement SSA.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 SSA.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 SSA.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 SSA.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 SSA certification over time, the certification body SHALL inform the holder of an SSA 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 SSA certification criteria, as these changes will affect certification of upgrades (as defined in 3.1.33) of a certified system in accordance with [SSA-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 SSA 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 SSA 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 SSA certification scheme.

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

Requirement SSA.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 SSA.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:
    - provide significant financing to a supplier or to a major user of auditable products;
    - be a major owner of a supplier or of a major user of auditable products;
- A chartered laboratory SHALL NOT:
    - receive significant financing from a supplier or from a major user of auditable products, or their major owners;
    - 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 SSA.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 SSA reference
6.1 *Personnel*	6.1.1.3	Certification scheme requirements to release information created during an evaluation	[SSA-200] Requirement SSA.R1 and SSA.R3
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	[SSA-200] 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	[SSA-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	[SSA-200] 6.4.3.2

6.4.3 ISASecure SSA 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 SSA certification scheme.

6.4.3.1 Personnel qualifications

Requirement SSA.R10 –FSA-S and SDA-S 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-S and SDA-S 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-S and SDA-S auditor qualifications

Category of qualification / experience	FSA –S auditor	SDA –S auditor
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 Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR** • Equivalent science or engineering degree **OR** • Bachelors 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** • Exceed minimum criterion stated below under “Relevant development work experience.” Specifically where a minimum of four or six years experience is specified there, the individual shall have ten or more years.	• BS Electrical Engineering **OR** • BS Computer Engineering (CE) **OR** • BS Computer Science (CS) **OR** • BS Chemical Engineering with CE or CS minor **OR** • BS Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR** • Equivalent science or engineering degree **OR** • Bachelors 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** • Exceed minimum criterion stated below under “Relevant development work experience.” Specifically where a minimum of four or six years experience is specified there, the individual shall have ten or more years.

Category of qualification / experience	FSA –S auditor	SDA –S auditor
Professional certification	• 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.	• CISA, CISSP, GICSP, CSSLP, 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.
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** • Minimum eight years of work experience in computer technology field, if individual has a bachelors 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	• 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** • Minimum eight years of work experience in computer technology field, if individual has a bachelors 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

Category of qualification / experience	FSA –S auditor	SDA –S auditor
Relevant development work experience	- Min 4 years detailed product development involvement for control systems **OR** - Min 4 years of systems integration, commissioning or maintenance experience for control systems **OR** - 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** - 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** - Min 6 years system level product test of control systems **AND** - Experience includes 2 years with security-related responsibilities **OR** - Same minimums for above activities and security responsibilities for electronic hardware/software non-control systems and pass specified ISCI-approved training **OR** - 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, system-level design or integration experience for control systems, or for non-control systems and pass specified ISCI-approved training **OR** - Other experience requiring interaction with electronic hardware or software development, system level design or integration, or in system commissioning or maintenance, for 6 years total, with 2 years of product development responsibilities, and pass specified ISCI-approved training, unless four years involved control systems - Demonstrates understanding and experience with defining and implementing product lifecycle process improvements - Experience includes 2 years with security-related responsibilities
Relevant auditing work experience	- Min 1 year experience performing technical product audit **OR** - 2 years in position with significant role in interaction with auditors **OR** - Min 3 years experience performing cybersecurity audit (organizational) **OR** - Min 3 years in position in organization which has been audited for cybersecurity, with significant role in interaction with auditors **OR** - Industry-recognized training in IT cybersecurity auditing - 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
Relevant industry specific knowledge	- General knowledge of at least two different control systems or pass specified ISCI approved training **AND** - 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**	- General knowledge of end-end electronic hardware or software development life cycle **AND** - General knowledge of control systems architectures or pass

Category of qualification / experience	FSA –S auditor	SDA –S auditor
	• Moderate level knowledge of networking and communication protocols **AND** • 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** • 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** • Knowledge of methods used to protect communications and detect / prevent communication attacks	specified ISCI-approved training
Knowledge of security standards	IEC 62443 Standard plus at least one of: • Common Criteria • ISO/IEC 27001 • IEC 61508 **AND** 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: • Common Criteria • ISO/IEC 27001 • IEC 61508 **AND** 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 SSA. R11 – Chartered laboratory requirement for personnel with full professional certifications

Two years after a chartered laboratory receives initial SSA accreditation, all SSA certification evaluations toward SSA 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 SSA.R10 and SSA.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. SSA.R11 requires that ultimately, lead auditors/evaluators must meet these experience requirements and fully achieve one of these professional certifications.

Requirement SSA.R12 – VIT-S 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 VIT-S testing and interpretation of results shall include those specified in Table 5:

Table 5 – VIT-S lead evaluator qualifications

Category of qualification / experience	VIT-S lead evaluator
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 Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR** • Equivalent science or engineering degree **OR** • 4 years work experience in testing of control systems may be substituted for degree • 4 years work experience in known vulnerability testing may be substituted for degree
Professional certification	• CISA, CISSP, GICSP, CACE, CACS, or equivalent **OR** • 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** • Min 4 years of systems integration, commissioning, or maintenance experience for computer technology systems **OR** • Min 3 years System Level Product Test for computer technology systems **OR** • Experience includes 1 year with software security-related responsibilities • 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** • Moderate level knowledge of networking and communication protocols **AND** • 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: • Common Criteria • ISO/IEC 27001 • IEC 61508

Requirement SSA.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 an SSA 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	SSA-200 requirement
6.1 6c	Continuing training	SSA.R13
7.4.2	Test and assessment records ("Inspection records" in 17020)	SSA.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 SSA reference
7.1 *General*	7.1.1	Certification scheme used by an SSA chartered laboratory	Defined in [SSA-100]
7.1 *General*	7.1.2	Refers to normative documents against which a system is evaluated	For initial certifications, documents are [SSA-300] and its normative references; for products with a version previously certified, documents are [SSA-301] and its normative references; [SSA-200] SSA.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 [SSA-200] requirement SSA.R14

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure SSA reference
7.2 *Application*	7.2	Information that scheme requires for client application	[SSA-300] 5.2 through 5.4 for initial certification; requirements for products with a version previously certified are in [SSA-301]
7.4 *Evaluation*	7.4.4	Evaluation of system to scope of certification and requirements specified in scheme	Certification requirements for initial certification are listed in [SSA-300] requirement SY.R16; certification requirements for products with a version previously certified are in [SSA-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 [SSA-200] 4.2
7.7 *Certification documentation*	7.7.1 f	Information scheme requires on the document signifying certification	Certificate format and content specified in [SSA-204] and [SSA-205]
7.8 *Directory of certified products*	7.8 last paragraph	Information about certified systems made available to a directory	[SSA-200] 6.5.3.3
7.9 *Surveillance*			Not applicable, see [SSA-200] 6.5.3.4
7.10 *Changes affecting certification*	7.10.1	Actions required by scheme for changes to certification criteria	[SSA-200] Inform clients per SSA.R6, update processes per SSA.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 [SSA-200] 6.5.3.6. Other actions are not defined for SSA certification
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 SSA certification

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure SSA reference
7.12 *Records*	7.12.3	Whether scheme requires complete re-evaluation of process on a predetermined cycle	No, as explained in [SSA-200] 6.5.3.4

6.5.3 ISASecure SSA 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 SSA certification scheme.

6.5.3.1 Application

6.5.3.1.1 Process requirements

Requirement SSA.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 SSA.R15 – Determining applicant eligibility
The chartered laboratory SHALL be responsible for determining whether a potential client meets the scope for SSA certification. 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 SSA.R41 and SSA.R42.

6.5.3.1.2 Content of procedures

Requirement SSA.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 SSA.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 SSA.R18 – Current ISASecure specifications

ISO/IEC 17025 7.2.1.3 on selection and verification of methods, specifies using the latest valid version of a method, unless not appropriate or possible. 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 SSA.R19 – Deleted

Requirement SSA.R20 – Deleted

Requirement SSA.R21 – VIT-S report

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

Requirement SSA.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 [SSA-303], the SSA assessment report sample. A report following this template SHALL also be provided to the client.

6.5.3.2.2 Deleted

6.5.3.2.3 Content of procedures

Requirement SSA.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 SSA.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 SSA 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 SSA.R30 – Deleted

Requirement SSA.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 SSA.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 SSA.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 an appropriate specification edition, 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 SSA.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 SSA.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 SSA.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 SSA.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 SSA 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 systems shipped by the supplier that are labeled with the 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 3.1.32 and 3.1.33), and certification to updated ISASecure versions, are covered in [SSA-301]. As required by SSA.R38 and described in [SSA-301], maintaining SSA 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 SSA certification. The following requirements apply to withdrawal and termination.

Requirement SSA.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 SSA.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 SSA.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 SSA.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 SSA.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 SSA 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 SSA 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 SSA.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 SSA.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 SSA.R45 – Housekeeping
Adequate measures SHALL be taken to ensure good housekeeping at the chartered laboratory facilities where evaluation activities are performed.

Requirement SSA.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 SSA.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 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 SSA.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 SSA.R49 – Archival of superseded specifications
Superseded normative specifications SHALL be archived.

6.6.3.3 Control of records

Requirement SSA.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 SSA.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 SSA.R52 – Basis for internal audits
Internal quality audit policies and procedures SHALL specify the basis for conducting audits.

Requirement SSA.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 SSA.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 SSA.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 SSA certified products

Requirement SSA.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 SSA.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 requirements.

Requirement SSA.R58 – Disclosure to ISCI of complaints related to ISASecure certified product
The chartered laboratory process for handling a report under Requirement SSA.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], published in 2017 as an update of [ISO/IEC 17025 2005]
- Section 6 of 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 produced by the chartered laboratory from sample SDA-S, FSA-S, and VIT-S audits carried out by the laboratory on a system, as described in Section 7.3. The review of artifacts may take place during the pilot phase of the ISASecure SSA program and be related to an early certification performed by the laboratory.

To be recognized as a chartered laboratory for the ISASecure SSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC recognized accreditation body:

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

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

These internationally recognized accreditations shall be obtained by a laboratory within 18 months of obtaining a provisional chartered laboratory status, as described in Section 5.2. 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 the 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 SSA 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 a qualified assessor for the ISO/IEC 17025 and ISO/IEC 17065 accreditations listed in Section 7.1. Provisional chartered status is granted if the evaluation shows that the laboratory complies with all of the requirements in the documents listed in Section 7.1, as well as 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 of Table 8. All ISASecure specific requirements in Section 6 of this document are also mandatory to receive provisional chartered status.

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. [ISASecure-202] provides the ASCI application process and forms for provisional chartered laboratory status based on the evaluation by the accreditation body. “Provisional” chartered laboratory status is a term applied by ASCI/ISCI within the ISASecure SSA 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 reviews technical criteria required for competent performance of the various ISASecure SSA certification elements. The evaluation consists of assessment of evidence supplied by the candidate laboratory per the evaluation criteria in Table 8. The requirements numbered VIT-S.Rnn or VIT.Rnn are from [SSA-420].

Table 8 - Technical readiness criteria for SSA chartered laboratory

ID	Evidence supplied by candidate laboratory	Evaluation criteria
1	Vendor statement of test tool and version in use for VIT-S	• ISCI-specified tool is in place for VIT-S per VIT-S.R6

ID	Evidence supplied by candidate laboratory	Evaluation criteria
2	VIT-S processes/procedures	- Comply with VIT-S.R7 on VIT-S testing configuration - Comply with VIT-S.R8 regarding the Nessus policy to be used and modes of the system components to be tested - Comply with VIT-S.R9 on interfaces to test under VIT-S - Comply with VIT-S.R10 on criteria for VIT-S pass - Instructions for VIT evaluation report creation comply with VIT.R14-23
3	Application form and instructions to be given to supplier submitting the system	- Application requests all items required per [SSA-300] Sections 5.2 through 5.4
4	Intermediate artifacts, paperwork and final evaluation report for a sample system covering SDA-S, FSA-S, and VIT-S	- Scope and results of FSA-S evaluation are consistent with zone capability security levels and cover system layouts to be certified - Scope, artifacts and results from SDA-S are consistent with zone capability security levels and validation activities in [SDLA-312], where these differ by level - Scope, artifacts and results from SDA-S take into account all system layouts in scope for the certification - Report from VIT-S evaluation indicates use of tool version and set of known vulnerabilities specified by [SSA-420] - Report from VIT-S evaluation indicates compliance with pass/fail criteria in VIT-S.R10 - Evaluation report and detailed VIT-S report meet requirements SSA.R21-SSA.R22 in this document - Evidence meets SSA.R31 in this document
5	Evidence demonstrating that VIT-S result for sample system can be reproduced based on information in evaluation report; document steps used to reproduce these	- Verify that steps for creation of reproduced results required only information in the evaluation report; and that results are same as initial results

— — — — — —