SDLA-200

ISA Security Compliance Institute – Security Development Lifecycle Security Assurance –

ISASecure SDLA chartered laboratory operations and accreditation

Version 1.9

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	2014.05.27	Initial version published to http://www.ISASecure.org
1.5	2018.02.01	Alignment with approved ANSI/ISA 62443-4-1: revise references, replace section 5.3 with discussion of transition to SDLA 2.1.0; incorporate errata from SDLA-102 v1.4
1.8	2020.06.19	Add option for shorter certification expiration if not all artifacts available; remove recognition for certification pending; replace EDSA by CSA; remove references to “withdraw certification” except where quoted from 17065
1.9	2022.02.01	Revise 6.4.3.1 personnel qualifications to support substitution of training for some qualifications and increase flexibility of education and experience requirements; add SDLA.R9A regarding timeline for chartered lab to have personnel with full professional certifications

Contents

List of SDLA specific 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 control system components, ISASecure System Security Assurance (SSA) for control 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 SDLA 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 SDLA (Security Development Lifecycle Assurance) program for control system security development processes, is referred to as an *ISASecure SDLA 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 may begin and continue ISASecure SDLA process certification operations (Section 7).

ISCI has based its certification program approach on:

- International standards for conformity assessment programs
- IACS security standard IEC 62443-4-1 (also published as an ANSI/ISA standard)
- Specifications developed for the ISASecure SDLA program.

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

The ISASecure SDLA program certifies a supplier's development lifecycle *process*. ISCI also has developed *product* certification programs for:

- Control system components, the ISASecure CSA program (Component Security Assurance)
- Control systems, the ISASecure SSA program (System Security Assurance).

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

ISASecure programs support and align with the standards ANSI/ISA/IEC 62443 for IACS security. ISASecure SDLA is a conformance program for the approved standard [IEC 62443-4-1]. [SDLA-100] discusses the relationship between ISASecure SDLA and the ANSI/ISA/IEC 62443 effort.

2 Normative references

2.1 General

NOTE 1 The following is the highest level document that describes the ISASecure SDLA certification program for security development process.

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

NOTE 2 The following lists all document titles and versions that define SDLA 3.0.0. It is reissued to list any errata subsequently issued for the baseline documents.

[SDLA-102] *SDLA-102 ISCI Security Development Lifecycle Assurance – Baseline document versions and errata for SDLA 3.0.0 specifications,* as specified at http://www.ISASecure.org

2.2 Accreditation/recognition

2.2.1 Chartered laboratory operations and accreditation

[ISASecure-118] *ISASecure-118 ISCI ISASecure Certification Programs - Policy for transition to SDLA 3.0.0*, 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 SDLA program.

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

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

2.4 Technical specifications

NOTE 1 This section includes the specifications that define technical criteria for evaluating a supplier's development lifecycle process for ISASecure SDLA certification.

NOTE 2 The following document is the overarching technical specification for ISASecure SDLA certification.

[SDLA-300] *ISCI Security Development Lifecycle Assurance – Requirements for ISASecure Certification and Maintenance of Certification,* as specified at http://www.ISASecure.org

[SDLA-303] *ISCI Security Development Lifecycle Assurance - Sample Report*, available on request to ISCI

NOTE 3 The following document provides the detailed technical evaluation criteria for an ISASecure SDLA certification of a supplier's development lifecycle process against the standard [IEC 62443-4-1]. It also provides the technical evaluation criteria for the Security Development Artifacts element (SDA) of an ISASecure CSA or SSA product certification.

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

2.5 External references

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

2.5.1 IACS security standards

NOTE 1 [SDLA-100] describes the relationship of ISASecure SDLA to the 62443 series 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*

2.5.2 International standards for certification programs

NOTE The following international standard applies to the ISASecure certification and testing processes.

[ISO/IEC 17065] ISO/IEC 17065.2012, "*Conformity assessment—requirements for bodies certifying products, processes and services*", October 2012

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

3.1.6
client
organization or person responsible to a certification body for ensuring that certification requirements are fulfilled

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
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.10
development organization
part of a supplier's organization that develops products, components, and systems, and defines and employs a secure development process that encompasses all IEC 62443-4-1 practices

NOTE Some suppliers have a separate organization that defines and maintains their development process. The above definition implies that for the purposes of the present document, such an organization is considered to be a part of all development organizations which employ that process.

3.1.11
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.

3.1.12
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.).

3.1.13
ISASecure version
ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a 3-place number such as SDLA 2.6.1

3.1.14
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

3.1.15
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.

3.1.16
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

3.1.17
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.

3.1.18
significant financing
financing that is material to the operations of the recipient

3.1.19
significant financial interest
financial interest where the value of this interest is material to the financial position of the entity that has the interest

3.1.20
significant sales
sales that are material to the operations of the seller

3.1.21
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.

3.1.22
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is “mark.”

3.1.23
termination
discontinuation of certified status upon request by the certified client

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
CS	computer science
CSA	Component Security Assurance
CSSLP	Certified Secure Software Lifecycle Professional
DCS	distributed control system
GICSP	Global Industrial Cyber Security Professional
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ILAC	International Laboratory Accreditation Cooperation
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
OWASP SAMM	Open Web Application Security Project Software Assurance Maturity Model
PLC	programmable logic controller
SDL	security development lifecycle
SDLA	security development lifecycle assurance, security development lifecycle assessment
SIS	safety instrumented system
SSA	system security assurance

4 Background

4.1 Technical ISASecure SDLA certification criteria

Development organizations for critical systems that specify compliance to the ANSI/ISA/IEC 62443 standards may apply for ISASecure SDLA certification.

In order to obtain ISASecure SDLA certification, a supplier development organization must maintain a documented secure development lifecycle process under change control that meets SDLA criteria specified in [SDLA-312], and demonstrate adherence to this process. If some aspects of the process are fully in place but have not yet been executed, the certifier can grant certification for a limited time period based upon a review of the supplier's readiness to execute them, as specified in [SDLA-300].

[SDLA-300] specifies procedures for granting SDLA certification status, expiration of certification, and maintenance of certification.

4.2 ISASecure SDLA 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 SDLA chartered laboratories are organizations that are accredited to evaluate the development lifecycle for an organization under the ISASecure SDLA program. ASCI grants accredited laboratories the right to process ISASecure SDLA certifications for development organizations on its behalf. A chartered laboratory will issue an ISASecure SDLA certificate for development organizations that meet SDLA program certification requirements. Certificate expiration and certificate maintenance are also managed by the chartered laboratory.

The lists of ASCI ISASecure SDLA chartered laboratories are posted on the ISCI website at http://www.ISASecure.org. At the request of suppliers, development organizations that have achieved certification are registered on this same ISCI website.

5 Summary of operations and accreditation requirements

5.1 Overview

ISASecure SDLA 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 certification programs.

The operations of ISASecure SDLA chartered test 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.

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

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

5.2 Accreditation process

Accreditation of a chartered laboratory consists of an assessment of the organization against the general requirements [ISO/IEC 17065] and the specific requirements in Section 6 of this document. To be recognized as a chartered laboratory for the ISASecure SDLA program, a laboratory shall attain the following accreditation, performed by an IAF/ILAC accreditation body:

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

The laboratory accreditation process consists of two steps. In the first step, an assessor who is qualified with respect to the above accreditation 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 defined in 7.1 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 process evaluations and grant ISASecure SDLA certifications. These rights continue as long as the laboratory receives formal accreditation from an SDLA accreditation body in a timely manner (the second step), and maintains this status.

5.3 Transition to SDLA 3.0.0

SDLA 3.0.0 adds to SDLA 2.0.0, the option for certification when some aspects of a supplier's SDL have not yet been executed on any product. As defined in [SDLA-300], such a certification will have a shorter expiration time. SDLA 3.0.0 also strengthens certifier validation for IEC 62443-4-1 requirement SM-12. SM-12 requires that a supplier employ a process to verify that their documented SDL has been carried out.

ISCI has defined a policy for chartered labs to follow in transitioning certification activities from SDLA 2.0.0 to SDLA 3.0.0. This policy is defined in the document [ISASecure-118].

6 Requirements on operations of chartered laboratories

6.1 Overview

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

Clause 6 is organized as follows:

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

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure SDLA reference
4.1.2 *Certification agreement*	4.2.1.1 h	Certification scheme requirements regarding client references to their certification	Sub clause 5.1 in [SDLA-300], and [SDLA-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	[SDLA-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	Requirements on mechanisms are in [SDLA-204]

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure SDLA reference
		indicating a process is certified	
4.2 *Management of impartiality*	4.2.10	Period of time between performing consultancy and certification services	[SDLA-200] Requirement SDLA.R4
4.6 *Publicly available information*	4.6c)	Certification scheme requirements regarding client references to their process certification	Sub clause 5.1 in [SDLA-300], and [SDLA-204]
4.6 *Publicly available information*	4.6a)	Certification scheme requirements related to granting certification	[SDLA-300]

6.2.3 ISASecure SDLA specific requirements

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

Requirement SDLA.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 oversight ISCI's role as scheme owner.

Requirement SDLA.R2 – Internal distribution for assessment reports
Procedures for report distribution internal to the chartered laboratory SHALL limit copies of the assessment report only to those that the chartered laboratory determines need the information to fulfill their work responsibilities.

Requirement SDLA.R3 – 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 clause 6.5.3.7 of this document.

Requirement SDLA.R4 – 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 SDLA.R5 – Client facility access without prior notification
Appropriate contracts, covenants, or agreements SHALL include provision(s) for unobstructed access to the client's development premises without prior notification, except as required by the client's standard visit procedures.

6.3 Structural requirements

6.3.1 Overview

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

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

6.3.2 Scheme references for standard requirements

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

Table 2 – Scheme references for ISO/IEC 17065 clause 5

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

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

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

Requirement SDLA.R6 – Organizational affiliations

When the separate legal entity as in [ISO/IEC 17065] 4.2.7 is a major user of products from the certified organization, 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 SDLA.R7 – 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 SDLA.R8 – 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 SDLA reference
6.1 *Personnel*	6.1.1.3	Certification scheme requirements to release information created during an evaluation	[SDLA-200] Requirement SDLA.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	[SDLA-200] sub clause 6.4.3.1
6.1.2 *Management of competence for personnel involved in the certification process*	6.1.2.1 b	Certification scheme requirements for training of personnel involved in certification	[SDLA-200] sub clause 6.4.3.1
6.2.1 *Internal resources* 6.2.2 *External resources*	6.2.1, 6.2.2.1	Applicable requirements from other standards	[SDLA-200] sub clause 6.4.3.2

6.4.3 ISASecure SDLA specific requirements

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

6.4.3.1 Personnel qualifications

Requirement SDLA.R9 – 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 are responsible for evaluation to SDLA requirements SHALL include those specified in Table 4.

The level of knowledge required for ISA 62443 as indicated in the last row of Table 4, 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 – SDLA auditor qualifications

Category of qualification / experience	SDLA auditor
Formal education	• BS Electrical Engineering **OR** • BS Computer Engineering **OR** • BS Computer Science **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 4 or 6 years experience is specified there, the individual shall have ten or more years.
Professional certification	• CSSLP, 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.
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
Relevant development work experience	• Min 4 years electronic hardware or software development 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, or in integration, testing, commissioning, or 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 • Demonstrates understanding and experience with documented product development lifecycle process: definition, execution and/or process improvement • Experience includes 2 years with electronic hardware or software security-related responsibilities
Relevant auditing work experience	• Min 1 year experience performing software process audit OR 2 years in position with significant role in interaction with auditors

Category of qualification / experience	SDLA auditor
Relevant industry specific knowledge	• General knowledge of end-end electronic hardware or software development life cycle **AND** • General knowledge of control systems architectures or pass specified ISCI-approved training
Knowledge of security standards and practices	Publicly available approved parts of the IEC 62443 standard plus at least one of the following or an equivalent standard or practice: • OWASP SAMM • DO-178B • IEC 61508 • ISO/IEC 15408-3 • Microsoft Security Development Lifecycle If have not met a cybersecurity experience requirement under professional certification, also pass specified ISCI-approved training.

If the individual meets all qualifications for the SDLA 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 that use the term “control systems,” then GICSP or a similar control-system focused professional certification is recommended.

Requirement SDLA.R9A – Chartered laboratory requirement for personnel with full professional certifications

Two years after a chartered laboratory receives initial SDLA accreditation, all SDLA certification evaluations toward SDLA 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.

NOTE The requirement SDLA.R9 implies 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. SDLA.R9A requires that ultimately, lead auditors must meet these experience requirements and fully achieve one of these professional certifications.

Requirement SDLA.R10 – 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 17025, 17020, 17021.

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 5 – ISO/IEC 17020 requirements specified

ISO/IEC 17020 requirement	Topic	SDLA-200 requirement
6.1 6c	Continuing training	SDLA.R10
7.1.2	Sampling	SDLA.R17
7.4.2	Assessment records ("Inspection records" in 17020)	SDLA.R18

6.5 Process requirements

6.5.1 Overview

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

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

6.5.2 Scheme reference for standard requirements

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

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

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

Table 6 – Scheme references for ISO/IEC 17065 clause 7

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure SDLA reference
7.1 *General*	7.1.1	Certification scheme used by an SDLA chartered laboratory	Defined in [SDLA-100]
7.1 *General*	7.1.2	Refers to normative documents against which a supplier’s security development lifecycle is evaluated	Documents are [SDLA-300] and [SDLA-312]
7.1 *General*	7.1.3	Person or committee to provide explanations per application of normative documents	ISCI Technical Steering Committee, as stated in [SDLA-200] Requirement SDLA.R11
7.2 *Application*	7.2	Information that scheme requires for client application	[SDLA-300] sub clause 5.2
7.4 *Evaluation*	7.4.4	Evaluation of process to scope of certification and requirements specified in scheme	Scope of an SDLA certification is defined in [SDLA-300] sub clause 5.1. Requirements are in [SDLA-300] and [SDLA-312]

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure SDLA reference
7.4 *Evaluation*	7.4.9 Note 2	Whether certification scheme requires certification body to perform evaluation under its responsibility after application	Yes, per [SDLA-300] clause 5.2
7.7 *Certification documentation*	7.7.1 f	Information scheme requires on the document signifying certification	Certificate format and content specified in [SDLA-204]
7.8 *Directory of certified products*	7.8 last paragraph	Information about certified processes made available to a directory	[SDLA-200] clause 6.5.3.3
7.9 *Surveillance*			Not applicable, see [SDLA-200] 6.5.3.4
7.10 *Changes affecting certification*	7.10.1	Actions required by scheme for changes to certification criteria	[SDLA-200] clause 6.5.3.5
7.11 *Termination, reduction, suspension or withdrawal of certification*	7.11.3	Actions required when a certification is terminated, suspended or withdrawn	For termination, see [SDLA-200] 6.5.3.6. Suspension and withdrawal are not defined for SDLA 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 SDLA certification
7.12 *Records*	7.12.3	Whether scheme requires complete re-evaluation of process on a predetermined cycle	Yes, in accordance with [SDLA-300] clause 5.3 regarding expiration and recertification

6.5.3 ISASecure SDLA specific requirements

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

6.5.3.1 Application

6.5.3.1.1 Process requirements

Requirement SDLA.R11 – 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 SDLA.R12 – Determining applicant eligibility
The chartered laboratory SHALL be responsible for determining whether a potential client meets the scope for SDLA 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 SDLA.R28 and SDLA.R29.

6.5.3.1.2 Content of procedures

Requirement SDLA.R13 – 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 SDLA.R14 – 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 Process requirements

Requirement SDLA.R15 – 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 [SDLA-303], the SDLA assessment report sample. A report following this template SHALL also be provided to the client.

6.5.3.2.2 Content of procedures

Requirement SDLA.R16 – Content of assessment methods or procedures
Each assessment method or procedure SHALL have sufficient detail instructions that assure reasonable repeatability of assessments and include or address the: title, effective date, assessment data to be obtained and recorded, objective acceptance criteria for results, assessment techniques, where additional information to that in [SDLA-312] is required to meet these goals.

Requirement SDLA.R17 – Sampling
The chartered laboratory SHALL have and shall use adequate documented instructions on sampling techniques, where the absence of such instructions could jeopardize the effectiveness of the assessment process.

NOTE Consideration should be given to sampling approaches for product development artifacts to be inspected during a recertification audit.

Requirement SDLA.R18 – Content of assessment data sheet
Assessment data sheets or similar documents SHALL include the assessment procedure and specification used, date of the assessment, assessment report number, signature of the personnel performing the assessment, and assessment results.

Requirement SDLA.R19 – Content of procedure maintenance procedures
Procedures for developing and maintaining 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 process conforms with the specification, and ensure modifications are reviewed by personnel who are familiar with the specification.

Requirement SDLA.R20 – Content of procedures for evaluating assessment data
Procedures for evaluating assessment data SHALL require the investigator to: verify and use the latest specification edition, provide written justification of how a process complies with each section of the specification (including a reference to an assessment procedure).

Requirement SDLA.R21 – Content of policy for evaluation of assessment data
Policies on evaluation of assessment data SHALL identify personnel responsible for technical decisions on the specification, how to decide which applicable 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 process discrepancies without the laboratory engaging in the redesign of the process, except to explain the failures in regard to the ISASecure specification.

Requirement SDLA.R22 – 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 [processes]

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 SDLA.R23 – Input to scheme directory
With permission of the certification client, the chartered lab SHALL inform ISCI of each certification granted and provide a copy of the certificate, to support ISCI's central directory of ISASecure certifications.

Requirement SDLA.R24 – 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 SDLA certification scheme does not require surveillance. Certifications expire, and recertification is required before that time in order to maintain certification, as specified in [SDLA-300] clause 5.3.

6.5.3.5 Changes affecting certification

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

Requirement SDLA.R25 – Intermediate audit for changed certification criteria
Upon request of the client, the chartered laboratory SHALL audit compliance to a changed requirement, prior to its next recertification cycle. The outcome SHALL NOT negatively impact certification status. However it MAY support the update of the client's current certification, to a more recent ISASecure SDLA version.

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, suspension and withdrawal are not defined for SDLA certification. The following requirements apply to termination.

Requirement SDLA.R26 – Termination of certification
Termination before expiration of a certification SHALL be supported by the chartered laboratory.

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 SDLA.R27 – Notification of termination of certification
The chartered laboratory SHALL inform ISCI of any termination of an SDLA certification at the time it occurs.

6.5.3.7 Complaints and appeals

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

Requirement SDLA.R28 – 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 ASCI board of directors.

Requirement SDLA.R29 – 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 organization that has applied for certification;
- Whether or not a certification was granted; or
- Adequacy of the SDL evaluation process by the chartered laboratory.

NOTE ISCI or ASCI does not 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 SDLA 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 SDLA specific requirements

This sub clause lists additional scheme specific requirements related to clause 8 *Management system requirements* in [ISO/IEC 17065], beyond those derived from [ISO/IEC 17065] together with the other documents of the ISASecure SDLA 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 SDLA.R30 – 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 SDLA.R31 – 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 SDLA.R32 – Housekeeping
Adequate measures SHALL be taken to ensure good housekeeping at the chartered laboratory facilities where evaluation activities are performed.

Requirement SDLA.R33 – Artifact inventory
Laboratory procedures for handling of artifact samples SHALL address item inventory.

Requirement SDLA.R34 – 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 SDLA.R35 – 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 SDLA.R36 – Archival of superseded specifications
Superseded normative specifications SHALL be archived.

6.6.3.3 Control of records

Requirement SDLA.R37 – 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 SDLA.R38 – 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 SDLA.R39 – Basis for internal audits
Internal quality audit policies and procedures SHALL specify the basis for conducting audits.

Requirement SDLA.R40 – 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 SDLA.R41 – 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 SDLA.R42 – 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 SDLA certified clients

Requirement SDLA.R43 – 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 SDLA requirements, that are found in ISO/IEC 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 SDLA program.

Requirement SDLA.R44 – Supplier process for disclosure of complaints related to security development process effectiveness
The signed agreement between the chartered laboratory and the client SHALL include the following provision. Any complaint regarding its SDL that is known to the certified organization that is determined to affect product security shall be brought to the attention of the chartered laboratory that granted a certification for the organization's SDL. The laboratory shall evaluate the impact on the organization conformance to the ISASecure SDLA requirements.

Requirement SDLA.R45 – Disclosure to ISCI of complaints related to security development lifecycle effectiveness
The chartered laboratory process for handling a report under Requirement SDLA.R44 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 SDL, whether or not it is attributed to their SDL.

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]
- Section 6 this document, all ISASecure specific requirements subsections.

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

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

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 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 SDLA 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 ISO/IEC 17065. Provisional chartered status is granted if the evaluation shows that the laboratory complies with all of ISO/IEC 17065 requirements. All ISASecure specific requirements in the present document are part of the ISASecure SDLA scheme, and are therefore 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 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.

BIBLIOGRAPHY

[DO-178B] RTCA Inc., RTCA/DO-178B: Software considerations in airborne systems and equipment certification, 1992

[IEC-61508-1] IEC Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, 2010

[IEC-61508-3] IEC Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 2010

[ISO/IEC 15408-3] ISO/IEC 15408 Information technology - security techniques - evaluation criteria for IT security - Part 3: Security assurance components, 2008

[Microsoft] Microsoft Security Development Lifecycle https://www.microsoft.com/en-us/securityengineering/sdl/

[OWASP SAMM] Open Web Application Security Project Software Assurance Maturity Model *https://owasp.org/www-project-samm/*